Council of the European Union

Brussels, 9 January 2025
(OR. en)

5165/25

LIMITE

CYBER 8
TELECOM 5
COSI 1
COPEN 3
CSDP/PSDC 11
DATAPROTECT 4
IND 6
RECH 8
PROCIV 3
HYBRID 1
IPCR 1
JAI 26
JAIEX 1
RELEX 16
POLMIL 2
EUMC 12
DISINFO 1
COTER 1
CFSP/PESC 43
CIVCOM 7
CSC 14
CODEC 15
CSCI 4
ESPACE 3

NOTE

From:	Presidency
To:	Delegations
Subject:	Stocktaking exercise on the implementation of recent Council conclusions on cyber issues - Mapping of actionable measures

The Presidency will be launching a stocktaking exercise on the implementation of recent Council conclusions on cyber issues. The main goal of the table set out in the annex is to take stock of the implementation of five sets of Council conclusions:

- Council conclusions on the future of cybersecurity – Implement and protect together- (10133/24),
- Council conclusions on ENISA (16527/24),
- Council conclusions on the development of the European Union's cyber posture (9364/22),
- Council conclusions on the EU Policy on Cyber Defence (9618/23), and
- Council conclusions on the cybersecurity of connected devices (13629/23).

This process is designed to be collaborative, and the Presidency will ensure that all stakeholders will have the opportunity to contribute and shape the final outcome. The steps outlined below provide the roadmap for this process:

Step 1: Initial feedback (End of January)

The Presidency invites stakeholders (Member States, Commission, EEAS) for feedback on the table and the envisaged process by the end of January following the presentation of the table at the HWPCI meeting on 13 January 2025. This will give stakeholders the opportunity to share their thoughts, suggestions, and identify possible missing elements which will help in refining the approach.

Step 2: State of play (February)

Following the feedback received from all stakeholders, the table might be amended early February. The Presidency will then invite all stakeholders to complete the 'state of play' section and send this information by the end of February.

Step 3: Table (March)

The Presidency will consolidate the input received and produce a new version of the table, incorporating all information by the end of March.

Step 4: Presentation of the new table and possibility to comment (April)

The new table will be presented in the HWPCI and delegations will have two weeks to review and provide comments.

Step 5: Finalisation of the table (mid-May)

By mid-May, the Presidency will aim to have a final version of the table, incorporating all stakeholder feedback and input.

Step 6: Debate and prioritisation (May/June)

The Presidency will launch another debate on the table, focusing on the identification of key areas and actions that Member States intend to prioritise.

The Presidency looks forward to delegations' active participation and engagement throughout this process and hopes that this stocktaking exercise will continue under future Presidencies.

ANNEX

Stocktaking exercise on the implementation of recent Council conclusions on cyber issues – Mapping of actionable measures

Council Conclusions on the future of cybersecurity – [FC]

Council Conclusions on ENISA – [ENISA]

Council Conclusions on the development of the European Union's cyber posture – [CP]

Council Conclusions on the EU Policy on Cyber Defence – [CD]

Council Conclusions on the cybersecurity of connected devices – [IoT]

I. Implementation, Simplification, and Lessening of Administrative Burden

Measures	Paragraph(s)	Responsible Entity(s)	Timeline	State of play
1. Develop a clear **overview of horizontal and sectoral legislative frameworks** and their interplay to avoid overlaps. [FC]	8	Commission	Deliver by 2025 Q1	
2. Prepare a **mapping of relevant reporting obligations** in EU legislative acts in cyber and digital matters to reduce administrative burden. [FC] **3.** **Prepare a mapping of relevant reporting obligations** set out in the respective EU legislative acts in cyber and digital matters. [ENISA]	6 [FC] 8 [ENISA]	Commission, ENISA, other relevant EU entities	Deliver by 2025 Q1	

Measures	Paragraph(s)	Responsible Entity(s)	Timeline	State of play
4. Develop a comprehensive **overview of the roles and responsibilities** of EU entities, networks, and structures in cybersecurity (e.g., ENISA, CERT-EU, CSIRTs, ECCC). [FC]	18	Commission, High Representative	Deliver by 2025 Q1	
5. Promote and implement **a single entry point** for incident notifications at the national level. [FC]	6	Member States		
6. Continue to exchange with Member States on the practicalities, simplification and **streamlining of the reporting procedure**. [ENISA]	8	ENISA in cooperation with the Commission and Member States	Ongoing	
7. Establish and maintain the **single reporting platform under the Cyber Resilience Act**. [ENISA]	9	ENISA		
8. **Adopt delegated and implementing acts** mandatory for implementing the NIS2 Directive and Cyber Resilience Act. [FC]	7	Commission	Ongoing	
9. Share and actively promote **technical guidance and best practices** in a regular and structured manner assisting the Member States in implementing cybersecurity policy and legislations. [ENISA]	6	ENISA	Ongoing	
10. **Ensure coherence and avoid overlap** between cybersecurity and digital regulations. [FC]	8	Commission	Ongoing	
11. **Reduce complexity** in the field of cyber, avoid unnecessary **duplication** and **ensure cooperation and synergies** with existing initiatives. [CD]	5	High Representative and Commission	Ongoing	

Measures	Paragraph(s)	Responsible Entity(s)	Timeline	State of play
12. Promote actions facilitating and supporting **compliance and reducing administrative burden**, especially for micro, small and medium enterprises. [FC]	5	Commission	Ongoing	
13. Ensure that **ENISA's mandate** to support Member States and EUIBAs is **focused and clearly-defined** in addition to a more precise division of tasks and competences with respect to other actors, reinforce ENISA's advisory role, consider streamlining ENISA's role in respect of tasks that are not at the core of its mission. [ENISA]	4, 5	Commission	Ongoing	
14. Use the evaluation of the Cybersecurity Act as an opportunity to examine how it can contribute to the simplification of the complex cyber ecosystem. [ENISA]	4	Commission	Ongoing	
15. Streamline the tasks of the Cyber Situation and Analysis Centre of the Commission and ENISA's related tasks. Avoid unnecessary duplication. [ENISA]	15	Commission	Ongoing	
16. Present a concept and roadmap for the establishment of the EUCDCC, drawing lessons from similar international entities, identifying resources required, avoiding unnecessary duplication and **seeking complementarity with the wider EU cybersecurity framework**. [CD]	12	High Representative	Ongoing	
17. Assess, where necessary, complementary sector specific regulations that should define which level of cybersecurity should be met by the connected device to ensure that specific security and privacy requirements are put in place for such devices with higher security risks. **[IoT]**	14	Commission		

II. Crisis Management and Cyber Resilience

Measures	Paragraph(s)	Responsible Entity(s)	Timeline	State of play
1. **Evaluate and update the EU cybersecurity crisis management framework**, including integration of new developments such as the Cyber Crisis Management Roadmap. [FC]	26	Commission, High Representative, ENISA, Member States	Complete evaluation and updates by 2025 Q1	
2. **Propose a revised Cybersecurity Blueprint**, ensuring compatibility with existing frameworks like the EU Cyber Diplomacy Toolbox and IPCR. [FC]	27	Commission, High Representative	Draft revised blueprint by 2025 Q1	
3. Use the **evaluation of the Cyber Blueprint** to properly reflect the additional tasks and responsibilities for contributing to **developing a cooperative response to large-scale cross-border cyber incidents or crises**, as well the role attributed to ENISA as the secretariat of CSIRT Network and EU-CyCLONe and by the recent cybersecurity legislation. [ENISA]	16	Commission, High Representative		
4. Conduct regular **joint cybersecurity exercises** at technical, operational, and political levels to test readiness. [FC]	28	ENISA, High Representative, Member States, ECCC	Ongoing	
5. **Make most efficient use of existing regular exercises** to test and improve the EU-crisis response framework, and to assure maximum uptake of the lessons learned. [ENISA]	17	ENISA, the CSIRTs Network and EU-CyCLONe	Ongoing	

Measures	Paragraph(s)	Responsible Entity(s)	Timeline	State of play
6. **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 an exercise focusing on crisis cooperation amongst EUIBAs[1]. [CP]	11	General	Ongoing	
7. Present a proposal on a new **Emergency Response Fund for Cybersecurity.** [CP]	13	Commission	Done in the Cybersolidarity Act	
8. **Commence the mapping** of the services needed and their availability immediately upon the entry into force of the Cyber Solidarity Act, **in order to make the EU Cybersecurity Reserve** as useful and tailored to users' needs as possible in all Member States. [ENISA]	11	ENISA	immediately upon the entry into force of the Cyber Solidarity Act	
9. **Involve Member States, in particular by gathering input** on the required criteria and informing about upcoming tenders, early **in the process of establishing the EU Cybersecurity Reserve**. [ENISA]	11	ENISA	Ongoing	
10. Examine and further strengthen **ENISA's role in supporting operational cooperation at the EU level and among Member States** in enhancing cyber resilience, taking into account Member States' competences in this field. [ENISA]	4	Commission	Ongoing	

[1] Relevant as well for the chapter on civilian- military cooperation

Measures	Paragraph(s)	Responsible Entity(s)	Timeline	State of play
11. Further test and reinforce **operational cooperation and shared situational awareness** among Member States, including through established networks such as the CSIRTs Network and the Cyber Crisis Liaison Organisation Network (EU CyCLONe) in order to advance EU preparedness to face large-scale cyber incidents. [CP]	12	general	Ongoing	
12. Reinforce efforts to raise the overall level of cybersecurity, for example by **facilitating the emergence of trusted cybersecurity service providers**. [CP]	6	EU, Member States	Ongoing	
13. Prioritise actions and assign priority to tasks related to **supporting Member States in enhancing their cyber resilience,** their operational cooperation and the development and implementation of Union Law **when preparing the draft general budget of the Union.** [ENISA]	5	Commission	N/A	
14. Work in close co-operation with the Member States, in contributing to the development of **EU-level situational awareness**. [ENISA]	14	ENISA, Member States, High Representative	Ongoing	
15. Propose EU common cybersecurity requirements for connected devices and associated processes and services through the Cyber Resilience Act. [CP]	4	Commission	Done by the Cyberresilience Act	
16. Establish a **Cyber capacity building board** and to hold regular exchanges in the Horizontal Working Party on Cyber Issues. [CP]	20	High Representative, Commission	Board has been established, the exchanges with HWP CI ongoing	

Measures	Paragraph(s)	Responsible Entity(s)	Timeline	State of play
17. Continue to contribute to EU INTCEN's, EUMS Intelligence Directorate's and Member States work under the Single Intelligence Analysis Capacity (**SIAC**). [CD]	13	Member States, through their competent authorities	Ongoing	
18. 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. [CP]	5	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 and in consultation with the High Representative	Ongoing	

Measures	Paragraph(s)	Responsible Entity(s)	Timeline	State of play
19. Actively participate in this initiative of strengthening the Digital Single Market and enhancing the trust in ICT products, services and processes for connected devices by ensuring privacy and cybersecurity and to facilitate the increased global competitiveness of the Union's IoT industry **through ensuring the highest standards of resilience, safety and security**. [IoT]	16	the Commission, the EU Agency for Cybersecurity (ENISA), the Telecommunication Conformity Assessment and Market Surveillance Committee, and the European Cybersecurity Certification Group (ECCG)	Ongoing	
20. Need to build a **comprehensive threat picture** from various sources, including the private sector[2]. [ENISA]	14	General, with emphasis on ENISA, CERT-EU, Europol, Council, EEAS / INTCEN	Ongoing	
21. Inform the public about cyber threats and the measures taken nationally and at EU level against these threats by **involving civil society, the private sector, and academia, with a view to raising awareness** and encouraging an appropriate level of cyber protection and cyber hygiene[3]. [CP]	10	Member States	Ongoing	

[2] Relevant also for the chapter on the cooperation with private sector.

[3] Relevant also for the chapter on the cooperation with private sector.

Measures	Paragraph(s)	Responsible Entity(s)	Timeline	State of play
22. **Establishing a programme of regular cross-community and multi-level cyber exercises** in order to test and develop the EU's 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 EU's general exercise policy[4]. [CP]	11	Member States, High Representative, Commission, ENISA	Ongoing	

III. Cyber Defence & Strengthening Cooperation Between Civilian and Military Domains

Measures	Paragraph(s)	Responsible Entity(s)	Timeline	State of play
1. Deepen **collaboration with NATO** on emerging and disruptive technologies and cybersecurity policies to avoid duplication and create synergies. [FC]	29	Member States, High Representative	Review progress by 2025 Q1	
2. **Engage with the EEAS and the Commission**, in those cases where ENISA has a role in **supporting the implementation of the EU Policy on Cyber Defence, in close cooperation with the EDA, the ECCC and the cyber defence community**. [ENISA]	22	ENISA, EEAS, EDA, ECCC	Ongoing	
3. **Enhance civilian-military cooperation in cyber training and joint exercises.** [CP]	11	Member States		

[4] Relevant also for the chapter on the cooperation with private sector.

Measures	Paragraph(s)	Responsible Entity(s)	Timeline	State of play
4. Create, building on the work of the EDA, a MilCERT network 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 military cyber commanders in order to strengthen strategic cooperation between EU Member States' cyber commands or other corresponding authorities. [CP]	28	Member States, EDA		
5. Further explore and strengthen civil-military national coordination mechanisms, facilitate common voluntary information sharing, share lessons learned, contribute to the development of interoperable standards and conduct risk evaluations and risk scenario-building, as well as joint exercises particularly at the European level, in full respect of the provisions of the Directive on measures for a high common level of cybersecurity across the Union (NIS2). [CD]	5	Member States, High Representative	N/A	
6. Encourage all Member States to take part in **[the EU Cyber Commanders Conference].** [CD]	7	Member States	Ongoing	
7. Identify possible ways to cooperate and benefit from a joint military and civilian perspective. [CD]	7	EU Cyber Crises Liaison Organisation Network (EU-CyCLONe) and the EU Cyber Commanders Conference	N/A	

Measures	Paragraph(s)	Responsible Entity(s)	Timeline	State of play
8. Explore, in close cooperation with Member States and the EEAS, **how CyDef-X could further support exercises such as CYBER PHALANX**, including on mutual assistance under Article 42(7) TEU and solidarity clause under Article 222 TFEU, **as well as with the Commission and ENISA as regards civilian exercises**. [CD]	15	EDA with Member States and the EEAS, Commission and ENISA	Ongoing	
9. Explore options to increase cybersecurity across the whole supply chain of the **EU's Defence Technological and Industrial Base (EDTIB).** [CP]	8	Commission	Ongoing	
10. 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. [CP]	27	Member States		
11. Complement the development of an EU cyber posture by tabling an ambitious **proposal for an EU Cyber Defence Policy in 2022.** [CP]	27	High Representative together with Commission	Done	
12. Further develop their own capabilities to conduct cyber defence operations, including when appropriate proactive defensive measures to protect, detect, defend and deter against cyberattacks. [CD]	18	Member States	Ongoing	
13. Closely cooperate to create synergies with the aim to develop and deliver full-spectrum cyber defence capabilities[5]. [CD]	19	the cybersecurity and the cyber defence industries	N/A	

[5] Relevant also for the chapter on the cooperation with private sector.

Measures	Paragraph(s)	Responsible Entity(s)	Timeline	State of play
14. Further support the development of a strong, agile, globally competitive and **innovative European cyber defence industrial and technological base**, including small- and medium-sized enterprises (**SMEs**), through further investments, and policy actions[6]**.** [CD]	19	Commission, in close collaboration with the ECCC	N/A	

IV. Risk Assessment

Measures	Paragraph(s)	Responsible Entity(s)	Timeline	State of play
1. Implement strategic and technical recommendations from the NIS Cooperation Group's risk assessments on communications infrastructures. [FC]	16	Member States, ENISA, Commission	Ongoing	
2. Use the opportunity of **the Cyber Security Act evaluation** to find ways to have a leaner, risk-based as well as more transparent and faster approach to the **development of EU cybersecurity certification schemes**. [ENISA]	7	Commission, Member States	Ongoing	
3. Consider ways to **enhance the collaboration between ENISA and European standardisation bodies**. [ENISA]	26	Commission, ENISA	Ongoing	
4. Strengthen efforts to **establish cybersecurity norms, standards or technical specifications for connected devices** undertaken by European Standards Organisations in this matter. [IoT]	11	European Standards Organisations	Ongoing	

[6] Relevant also for the chapter on the cooperation with private sector.

Measures	Paragraph(s)	Responsible Entity(s)	Timeline	State of play
5. Develop a **coherent and comprehensive approach across sectors** to risk assessment and scenario building, based on a common methodology. [FC]	16	Commission, High Representative, ENISA, NIS Cooperation Group	Deliver by 2025 Q2	
6. Strengthen ICT supply chain security by advancing the **ICT Supply Chain Toolbox.** [FC]	17	NIS Cooperation Group, Commission	Updates to toolbox during 2025	
7. Further **publicise guidance, policies and procedures on vulnerability disclosure.** [ENISA]	10	NIS CG with the assistance of ENISA	Ongoing	
8. **Conduct a risk evaluation and build risk scenarios** from a cybersecurity perspective in a situation of threat or possible attack against Member States or partner countries and present them to the relevant Council bodies. [CP]	12	Commission, High Representative and the NIS Cooperation group, in coordination with relevant civilian and military bodies and agencies and established networks, including the EU CyCLONe	Partially done	

V. Cybercrime

Measures	Paragraph(s)	Responsible Entity(s)	Timeline	State of play
1. Strengthen **collaboration on cybercrime through EMPACT** and enhance processes for investigating and disrupting ransomware operations. [FC] 2. Strengthen 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 law enforcement capabilities in investigating and prosecuting cybercrime. [CP]	1. 24, 30 2. 10	1. Europol, Eurojust, Member States, 2. General	Ongoing	
3. Facilitate **information exchange between CSIRTs and law enforcement** to improve victim notification and threat mitigation. [FC]	24	ENISA, CERT-EU, Europol	Ongoing	
4. Promote **lawful access to data for law enforcement** in compliance with data protection and privacy laws. [FC]	24	Member States, Europol, Commission	Commission to propose roadmap by 2025 Q2	

VI. Skills

Measures	Paragraph(s)	Responsible Entity(s)	Timeline	State of play
1. Further develop the **Cybersecurity Skills Academy**. [FC]	12	Commission, ENISA, ECCC	Updates by 2025	

Measures	Paragraph(s)	Responsible Entity(s)	Timeline	State of play
2. Promote **international cooperation on mutual recognition of cybersecurity skills frameworks**. [FC]	12	ENISA, Member States	Ongoing	
3. Enhance **cybersecurity workforce development** through partnerships with academia, public, and private sector. [FC]	12	Commission, Member States	Ongoing	
4. Clarify roles regarding **development of skills** and exploring synergies with any future European Digital Infrastructure Consortium on this topic as well as with the European Security and Defence College and CEPOL. [FC]	12	ENISA, ECCC	Ongoing	
5. **Continue their close cooperation**, especially in relation to research and innovation needs and priorities, as well as cyber skills, to increase the competitiveness of the Union's cybersecurity industry [ENISA]	20	ENISA, ECCC	Ongoing	
6. Examine how **synergies in the working of ENISA and the ECCC** can be further optimised and how to better streamline activities according to their respective mandates. [ENISA]	20	Commission	Ongoing	
7. Liaise with Member States interested in **setting up a EDIC**. [ENISA]	24	Commission	Ongoing	
8. Prioritise supporting Member States' **skills** and education efforts, **strengthening general public awareness** and collaborate with the ECCC where appropriate. [ENISA]	24	ENISA and ECCC	Ongoing	
9. Swiftly **operationalise the European Cybersecurity Competence Centre** to develop a strong European cyber research, industrial and technological ecosystem. [CP]	7	Commission	Done, ECCC gained financial autonomy	

Measures	Paragraph(s)	Responsible Entity(s)	Timeline	State of play
10. Exchange **information on best practices to develop skilled cybersecurity professionals,** leveraging the synergies between military, civilian and law enforcement initiatives. [CD]	29	Member States, Commission, ENISA, EDA, ESDC	Ongoing	

VII. Cooperation with Private Sector

Measures	Paragraph(s)	Responsible Entity(s)	Timeline	State of play
1. Engage with **private sector stakeholders** to strengthen cybersecurity measures and foster collaborative initiatives. [FC] **2. Bolster cooperation** with the private sector. [ENISA]	1. 22 2. 25	1. Commission, ENISA, ECCC, Member States 2. ENISA, in close cooperation with the Member States and across EU entities, High Representative	Ongoing	
3. Encourage **voluntary information sharing** between private entities and public authorities. [FC]	23	ENISA, CERT-EU, Member States	Ongoing	
4. Ensure adequate financial and human **resources for cybersecurity and measures aiming at creating a conducive environment for the private sector to be competitive.** Design and implement a horizontal mechanism combining multiple sources of financing, including the cost of highly qualified human resources. Explore options for such a mechanism. [CP]	9	Commission		

VIII. Future Threats and Emerging Technologies

Measures	Paragraph(s)	Responsible Entity(s)	Timeline	State of play
1. Establish and implement the **roadmap for the transition to Post-Quantum Cryptography (PQC)**. [FC]	35	Commission, Member States	Publish roadmap by 2026 Q2	
2. Consider **non-legislative risk-based initiatives for emerging and disruptive technologies**, including AI, quantum, and 6G. [FC]	34	Commission, ENISA, Member States, NIS Cooperation Group, High Representative	Ongoing	
3. Contribute further to **drawing the public's attention to the risks and possibilities** of technologies such as artificial intelligence and quantum computing. [ENISA]	12	ENISA	Ongoing	

IX. Cyberdiplomacy and International Cooperation

Measures	Paragraph(s)	Responsible Entity(s)	Timeline	State of play
1. Engage third countries to enhance **cooperation against cybercrime and ransomware.** [FC]	30	Member States, Europol, High Representative	Regular updates with review in 2025	
2. Promote **international standards for cybersecurity certification and risk mitigation**. [FC]	14, 31	ENISA, High Representative. Commission	Ongoing	
3. Strengthen the EU's role **in multilateral cyber forums** to shape global norms. [FC]	29	High Representative, Commission		

Measures	Paragraph(s)	Responsible Entity(s)	Timeline	State of play
4. Continue to promote our **common values and joint efforts within global forums** in order to safeguard a free, global, open and secure cyberspace. [ENISA]	23	High Representative, Member States	Ongoing	
5. The necessity of **clarifying**, in accordance with relevant procedures, **ENISA's international involvement**, ensuring in particular that its Management Board is duly and timely informed of the related activities. Involvement in relevant international cybersecurity cooperation frameworks, including organisations such as **NATO and the OSCE.** [ENISA]	23	General		
6. 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 EU INTCEN in the framework of the EU Cyber Diplomacy Toolbox. [CP]	12	EU CyCLONe, High Representative		
7. Review the existing bilateral cyber dialogues and, if necessary, propose to start similar cooperation with additional countries or relevant international organisations. [CP]	16	High Representative	Ongoing	
8. Further strengthen 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** [CP]	17	High Representative, Member States	Ongoing	
9. Engagement in relevant international organisations especially in the **UN First and Third committees related processes**, while emphasising that existing international law applies, without reservation, in and with regard to cyberspace. [CP]	18	Council via Member States	Ongoing	

Measures	Paragraph(s)	Responsible Entity(s)	Timeline	State of play
10. Establish the Programme of Action for **advancing responsible State behaviour in cyberspace (PoA).** [CP]	18	High Representative, Member States	Done	
11. 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. [CP]	18	EU, Member States	Done	
12. Present an outreach plan on how to promote a global common understanding of the application of international law in cyberspace, **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) to the Council. [CP]	21	High Representative	Done	
13. Establish the **EU Cyber Diplomacy Network**, 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. [CP]	21	High Representative	Ongoing	
14. Make full and systematic use of the 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**. [CP]	21	High Representative, Commission, Member States	Ongoing	

Measures	Paragraph(s)	Responsible Entity(s)	Timeline	State of play
15. Work towards a **revised version of the implementing guidelines of the EU Cyber Diplomacy Toolbox**, notably by exploring additional response measures. [CP]	23	Member States and the High Representative, with the support of the Commission	Done	
16. Hold regular exchanges on the cyber threat landscape in the 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 overall awareness and preparedness for further applications of the EU Cyber Diplomacy Toolbox, and develop further tools to support its implementation. [CP]	24	Member States, High Representative, Commission, ENISA	Ongoing	
17. Work on a set of **EU cyber defence interoperability requirements**, which would build on, and be compatible with, existing principles, processes and standards established in particular in the North Atlantic Treaty Organization (**NATO**) framework. [CD]	20	Commission, EEAS, EDA, EU Military Staff		
18. Explore in the **framework of the European Defence Standardisation Committee** whether specific voluntary standards for defence systems could be required, in close cooperation with all relevant stakeholders, including European standardisation organisations and NATO as appropriate. [CD]	20	General		

Measures	Paragraph(s)	Responsible Entity(s)	Timeline	State of play
19. Call for **links on relevant levels to be established between EU-NATO on training, education, situational awareness, exercises and R&D platforms, and to seek potential synergies** between the respective voluntary commitments for the developments of national cyber defence capabilities and the crisis management frameworks, the protection of critical infrastructure, and the enhancement of exchanges of situational awareness, coordinated responses to malicious cyber activities as well as capacity building efforts in third countries. This includes the Technical Arrangement between NATO Computer Incident Response Capability (NCIRC) and the Computer Emergency Response Team – EU (CERT-EU) as well as an enhanced political dialogue on cyber defence issues on all levels**.** [CD]	33	High Representative, Commission, Cert-EU	N/A	
20. 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 decisionmaking process, including on the question of attribution, and thereby enable a swift, effective and substantiated response to malicious cyber activities targeting the EU and its partners. [CP]	24	Member States, EU INTCEN, EEAS	Ongoing	
21. Identify possible EU joint responses to cyberattacks, including sanctions options, across the spectrum in order to be prepared to take swift and effective action when necessary. [CP]	26	High Representative, in cooperation with the Commission	Ongoing	