Brussels, 14 February 2025

WK 2061/2025 INIT

LIMITE

CYBER	**PROCIV**	**DISINFO**
TELECOM	**HYBRID**	**COTER**
COSI	**IPCR**	**CFSP/PESC**
COPEN	**JAI**	**CIVCOM**
CSDP/PSDC	**JAIEX**	**CSC**
DATAPROTECT	**RELEX**	**CODEC**
IND	**POLMIL**	**CSCI**
RECH	**EUMC**	**ESPACE**

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

WORKING DOCUMENT

From: To:	Presidency Horizontal Working Party on Cyber Issues
N° prev. doc.:	5165/25
Subject:	Stocktaking exercise on the implementation of recent Council conclusions on cyber issues

The Presidency has launched 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 six 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),
- Council conclusions on the cybersecurity of connected devices (13629/20), and
- Council conclusions on ICT supply chain security (13664/22)

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) *[finalised]*

The Presidency invited 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. The stakeholders had the opportunity to share their thoughts, suggestions, and identify possible missing elements which helped in refining the approach.

Step 2: State of play (February) *[ongoing]*

Following the feedback received from all stakeholders, the table was amended early February. The Presidency invites 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.

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]

Council conclusions on ICT supply chain security – [SCS]

I. Implementation, Simplification, and Lessening of Administrative Burden

Measures [Conclusions, paragraph]	Action words used	Responsible Entity(s)	Timeline	State of play / Comments
1. Develop a clear **overview of horizontal and sectoral legislative frameworks** and their interplay to avoid overlaps. [FC,8]	Calls on	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,6] **3.** **Prepare a mapping of relevant reporting obligations** set out in the respective EU legislative acts in cyber and digital matters. [ENISA,8]	2. Invites 3. Recalls its invitation	Commission with support of ENISA and other relevant EU entities	Deliver by 2025 Q1	
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]	Calls on	Commission, High Representative	Deliver by 2025 Q1	

Measures [Conclusions, paragraph]	Action words used	Responsible Entity(s)	Timeline	State of play / Comments
5. Promote and implement **a single entry point** for incident notifications at the national level. [FC,6]	Encourages	Member States		
6. Continue to exchange with Member States on the practicalities, simplification and **streamlining of the reporting procedure**. [ENISA,8]	Calls	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]	Urges	ENISA		
8. **Adopt delegated and implementing acts** mandatory for implementing the NIS2 Directive and Cyber Resilience Act. [FC,7]	Calls	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]	Encourages	ENISA	Ongoing	
10. **Ensure coherence and avoid overlap** between cybersecurity and digital regulations. [FC,8]	Urges	Commission	Ongoing	
11. **Reduce complexity** in the field of cyber, avoid unnecessary **duplication** and **ensure cooperation and synergies** with existing initiatives. [CD,5]	Encourages	High Representative and Commission	Ongoing	
12. Promote actions facilitating and supporting **compliance and reducing administrative burden**, especially for micro, small and medium enterprises. [FC,5]	Calls	Commission	Ongoing	
13. Ensure that **ENISA's mandate** to support Member States and EUIBAs is **focused and clearly-defined** in addition to a more	Calls	Commission	Ongoing	

Measures [Conclusions, paragraph]	Action words used	Responsible Entity(s)	Timeline	State of play / Comments
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]				
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]	Invites	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]	Invites, encourages	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]	Calls	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]	Encourages	Commission		
18. **Ensure that the supply chain security requirements are, to the extent possible, aligned throughout all relevant sectors, especially those covered by the future NIS 2 Directive**, in order to avoid discrepancies between the obligations imposed on suppliers as well as to ease the burden on operators of critical sectors of	Stresses importance	General	N/A	

Measures [Conclusions, paragraph]	Action words used	Responsible Entity(s)	Timeline	State of play / Comments
assessing the compliance of suppliers with those obligations, while taking into account sector specificities. [SCS,15]				
19. Required to issue the **interoperability guidelines for the Cross-Border Cyber Hubs** [ENISA,11]	Recalls	ENISA	Without undue delay	
20. To implement **solutions within the European Digital Identity Framework** and to timely develop European cybersecurity certification schemes to be adopted pursuant to Regulation (EU) 2019/881 for the certification of the European Digital Identity Wallet. [FC,15]	Calls, Encourages	Commission, Member States	Ongoing	
21. To swiftly complete the actions needed for the **ECCC to gain financial autonomy and finalise its institutional set up**. [FC,21]	Calls	ECCC, Commission		Done, ECCC has gained financial autonomy

II. Crisis Management and Cyber Resilience

Measures [Conclusions, paragraph]	Action words used	Responsible Entity(s)	Timeline	State of play / Comments
1. Evaluate and update the EU cybersecurity crisis management framework, including integration of new developments such as the Cyber Crisis Management Roadmap. [FC,26]	Stresses the need	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]	Calls	Commission, High Representative	Draft revised blueprint by 2025 Q1	

Measures [Conclusions, paragraph]	Action words used	Responsible Entity(s)	Timeline	State of play / Comments
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]	Invites	Commission, High Representative		
4. Conduct regular **joint cybersecurity exercises** at technical, operational, and political levels to test readiness. [FC,28]	Emphasises	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]	Invites	ENISA, the CSIRTs Network and EU-CyCLONe	Ongoing	
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]	Acknowledges the need	General	Ongoing	
7. Present a proposal on a new **Emergency Response Fund for Cybersecurity.** [CP,13]	Invites	Commission	End of Q3 2022	
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]	Invites	ENISA	immediately upon the entry into force of the Cyber Solidarity Act	

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

Measures [Conclusions, paragraph]	Action words used	Responsible Entity(s)	Timeline	State of play / Comments
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]	Invites	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]	Invites	Commission	Ongoing	
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]	Underlines the need	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]	Calls	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]	Calls	Commission	Ongoing	
14. Work in close co-operation with the Member States, in contributing to the development of **EU-level situational awareness**. [ENISA,14]	Encourages	ENISA, Member States, High Representative	Ongoing	

Measures [Conclusions, paragraph]	Action words used	Responsible Entity(s)	Timeline	State of play / Comments
15. Propose EU common cybersecurity requirements for connected devices and associated processes and services through the Cyber Resilience Act. [CP,4]	Calls	Commission		Done by the Cyber Resilience Act
16. Establish a **Cyber capacity building board** and to hold regular exchanges in the Horizontal Working Party on Cyber Issues. [CP,20]	Calls	High Representative, Commission	Board has been established, the exchanges with HWP CI ongoing	
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]	Invites	Member States, through their competent authorities	Ongoing	
18. Establishing mutual beneficial **cooperation between the Commission's cyber situation and analysis centre and other EU-IBAs, in particular ENISA and CERT-EU**. Ensuring close cooperation with EU cooperation networks when developing situational awareness. [CD,14]	Emphasises the importance, underlines the importance	COM's cyber situation and analysis centre, ENISA, CERT-EU,EU-CyCLONe, CNW, NIS CG	ongoing	
19. Carry out a **mapping of existing tools for secure communication** in the cyber field to be discussed in relevant Council bodies and with relevant cooperation groups. [CP,15]	Invites	Commission and other relevant EU-IBAs; CNW, EU-CyCLONe	By the end of 2022	Not yet available
20. Recommendations based on the mapping of existing tools for secure communication in the cyber domain, to be developed swiftly. [CD,22]	Calls for	Commission and relevant institutions		
21. 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**	Invites	relevant authorities, such as the Body of European Regulators for Electronic	Ongoing	

Measures [Conclusions, paragraph]	Action words used	Responsible Entity(s)	Timeline	State of play / Comments
within the European Union, including the continued implementation of the EU 5G Toolbox. [CP,5]		Communications (BEREC), ENISA and NIS CG, Commission, High Representative		
22. **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]	Invites	Commission, ENISA, the Telecommunication Conformity Assessment and Market Surveillance Committee, and ECCG	Ongoing	
23. Consider ways to **enhance the collaboration between ENISA and European standardisation bodies**. [ENISA,26]	Calls	Commission, ENISA	Ongoing	
24. Strengthen efforts to **establish cybersecurity norms, standards or technical specifications for connected devices** undertaken by European Standards Organisations in this matter. [IoT,11]	Recommends, emphasises need to establish	European Standards Organisations, Commission	Ongoing	
25. Need to build a **comprehensive threat picture** from various sources, including the private sector[2], including situational briefings within the context of Cyber Diplomacy Toolbox complementing the situational awareness provided by Single Intelligence Analysis Capacity (SIAC). [ENISA,14]	Stresses the need	General, with emphasis on ENISA, CERT-EU, Europol, Council, EEAS / INTCEN	Ongoing	
26. 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**	Reiterates its commitment	Member States	Ongoing	

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

Measures [Conclusions, paragraph]	Action words used	Responsible Entity(s)	Timeline	State of play / Comments
awareness and encouraging an appropriate level of cyber protection and cyber hygiene[3]. [CP,10]				
27. 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]	Stresses the importance	Member States, High Representative, Commission, ENISA	Ongoing	
28. Strengthen the overall resilience and security of ICT supply chains against the whole variety of threat factors, such as natural events, system failures, insider threats, or human errors. [SCS,3] **29. Enhance the security and resilience of ICT supply chains** for the functioning of the Single Market together with the need to ensure the availability, security and diversity of ICT products and services in the Single Market. [SCS,6]	Emphasises that it is important	General	Ongoing	
30. Work towards **avoiding situations of unwanted strategic external dependencies** in relation to ICT products and services. [SCS,4]	Encourages	Member States	Ongoing	
31. Diversify suppliers of critical ICT in order to avoid or limit the creation of major dependencies on single suppliers, and in particular high-risk suppliers, as it increases the exposure to the consequences of potential disruptions. [SCS,8]	Reaffirms the importance	Member States	Ongoing	

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

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

Measures [Conclusions, paragraph]	Action words used	Responsible Entity(s)	Timeline	State of play / Comments
32. **Develop methodological guidelines** by the third quarter of 2023 in order to encourage the contracting authorities to put appropriate focus on the cybersecurity practices of tenderers and their subcontractors, and to assess and, if needed, make proposals to revise or complement relevant public procurement legislation. [SCS,9]	Invites	Commission	by the third quarter of 2023	
33. **Further exchange information on best practices and methodologies regarding the implementation of measures recommended in the EU 5G Toolbox** and in particular to **apply the relevant restrictions on high-risk suppliers** for key assets defined as critical and sensitive in the EU coordinated risk assessment. [SCS,11]	Calls on	Member States	Ongoing	
34. **Formulate recommendations**, based on risk assessments, to Member States and the Commission in order **to reinforce the resilience communications networks and infrastructures within the European Union**, including the continued implementation of the **EU 5G Toolbox**. [SCS,13]	Recalls the invitation	Relevant authorities		
35. **Perform a stock-taking of best practices available for supply chain risk management and compile them into methodological guidelines.** [SCS,18]	Encourages	ENISA with the assistance of NIS CG		
36. Integrating aspects related to the **prevention of vendor lock-in** into EU legislation. [SCS,8]	Encourages	Commission (drive)		
37. Explore options for **including ICT supply chain security aspects in the upcoming calls within the Cybersecurity Work Programmes**	Calls as matter of priority	ECCC, Commission	Ongoing	

Measures [Conclusions, paragraph]	Action words used	Responsible Entity(s)	Timeline	State of play / Comments
under the Digital Europe Programme and Horizon Europe Programme, or any other relevant funding opportunities. [SCS, 23]				
38. **Assess the results and gaps of the EU Cybersecurity Strategy** from December 2020 and its impact, and to present on this basis a revised strategy reflecting these Council conclusions. [FC,37]	Concludes, invites	Commission, High Representative	without undue delay	

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

Measures [Conclusions, paragraph]	Action words used	Responsible Entity(s)	Timeline	State of play / Comments
1. Deepen **collaboration with NATO** on emerging and disruptive technologies and cybersecurity policies to avoid duplication and create synergies. [FC,29]	Emphasises the importance	Member States, High Representative	Review progress by 2025 Q1	
2. Continue to pursue working arrangement **with NATO Communications and Information Agency** [ENISA,22]	Encourages	ENISA	Ongoing	
3. **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]	Highlights the need	ENISA, EEAS, EDA, ECCC	Ongoing	
4. **Enhance civilian-military cooperation in cyber training and joint exercises.** [CP,11]	Invites	Member States		
5. **Create, building on the work of the EDA, a MilCERT network to develop cooperation and facilitate the exchange of information,**	Invites	Member States, EDA		

Measures [Conclusions, paragraph]	Action words used	Responsible Entity(s)	Timeline	State of play / Comments
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]				
6. 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]	Encourage	Member States, High Representative	N/A	
1. Identify possible ways to cooperate and benefit from a joint military and civilian perspective. [CD,7]	Invites	EU-CyCLONe and the EU Cyber Commanders Conference, EU CDCC (represented by EEAS and Member States)	N/A	
2. To **participate in MICNET** in order to ensure the network's effectiveness and to build on lessons learned from the CSIRTs Network, and to create effective cooperation and coordination between the two networks. [CD,8]	Encourages, strongly encourages	Member States	At an appropriate time	
3. 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	Encourages	EDA with Member States and the EEAS, Commission and ENISA	Ongoing	

Measures [Conclusions, paragraph]	Action words used	Responsible Entity(s)	Timeline	State of play / Comments
and solidarity clause under Article 222 TFEU, **as well as with the Commission and ENISA as regards civilian exercises**. [CD,15]				
4. Strengthen and advance its cooperation and explore mutually beneficial and tailored partnerships on cyber defence policies, including on cyber defence capacity building through the European Peace Facility (EPF). [CD,31]	Calls	High Representative, Commission	Ongoing	
5. 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]	Encourages	Member States		
6. 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[5]**.** [CD,19]	Invites	Commission, in close collaboration with the ECCC	N/A	
7. Develop a working arrangement to facilitate information sharing among respective staffs on respectively civil, dual use and defence technology priorities. [CD,26]	Encourages	ECCC, EDA		
8. Boost research and innovation, invest more in civilian and defence areas to strengthen the EU's Defence Technological and Industrial Base (EDTIB). [CP,7]	Underlines the need	Commission		

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

IV. Risk Assessment

Measures [Conclusions, paragraph]	Action words used	Responsible Entity(s)	Timeline	State of play / Comments
1. Implement strategic and technical recommendations from the NIS Cooperation Group's risk assessments on communications infrastructures. [FC,16]	Calls	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]	Urges	Commission, Member States	Ongoing	
3. Participate in the preparatory work on individual European certification schemes in order to build trust in secure ICT products, processes, and services and to strengthen their resilience[6]. [SCS,17]	Encourages	Commission, ENISA, all relevant stakeholders	Ongoing	
4. Swiftly prepare implementing acts on the European certification schemes after the completion of preparatory work, notably the Common Criteria-based European cybersecurity certification scheme. [SCS,17]	Calls	Commission		
5. Develop a **coherent and comprehensive approach across sectors** to risk assessment and scenario building, based on a common methodology. [FC,16]	Calls	Commission, High Representative, ENISA, NIS CG	Deliver by 2025 Q2	
6. Strengthen ICT supply chain security by advancing the **ICT Supply Chain Toolbox.** [FC,17]	Calls	NIS CG, Commission	Updates to toolbox during 2025	
7. Further **publicise guidance, policies and procedures on vulnerability disclosure**,step up all the necessary work to ensure	Invites	NIS CG with the assistance of ENISA	Ongoing	

[6] Relevant also for the chapter on crisis management & cyber resilience.

Measures [Conclusions, paragraph]	Action words used	Responsible Entity(s)	Timeline	State of play / Comments
the smooth functionality of the European vulnerability database. [ENISA,10]				
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]	Invites	Commission, High Representative and the NIS CG, in coordination with relevant civilian and military bodies and agencies and established networks, including the EU CyCLONe	Partially done	
9. **Assess the risks for supply chains of critical infrastructure** in various domains, including the digital domain, related to the EU's security and defence interests as well as to explore options to increase cybersecurity across the whole supply chain of the EU's Defence Technological and Industrial Base. [SCS,11]	Reaffirms its invitation	Commission, together with Member States	In 2023	
10. **Reflect on ICT supply chain security in the implementation of the commitments and actions of the Strategic Compass**.[SCS,11]	Invites	Member States, Commission		
11. **Monitor investments in the ICT supply chain** security of the entities regulated under the forthcoming NIS 2 Directive. [SCS,18]	Encourages	ENISA		
12. **Identify the specific ICT services, systems or products that might** be subjected to the coordinated supply chain risk assessments with priority. [SCS,20]	Invites	Commission, after consulting the NIS CG and ENISA	by the second quarter of 2023	

Measures [Conclusions, paragraph]	Action words used	Responsible Entity(s)	Timeline	State of play / Comments
13. Develop a toolbox of measures for reducing critical ICT supply chain risks (**ICT Supply Chain Toolbox**). [SCS,21]	Invites	NIS CG, in cooperation with the Commission and ENISA	Expected by end of Q1 2025	

V. Cybercrime

Measures [Conclusions, paragraph]	Action words used	Responsible Entity(s)	Timeline	State of play / Comments
1. Strengthen **collaboration on cybercrime through EMPACT** and enhance processes for investigating and disrupting ransomware operations. [FC,24,30] **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,10]	1. Calls 2. Emphasises the need	Commission, Europol, Eurojust, Member States,	Ongoing	
3. Facilitate **information exchange between CSIRTs and law enforcement** to improve victim notification and threat mitigation. [FC,24]	Invites	ENISA, CERT-EU, Europol	Ongoing	
4. Promote **lawful access to data for law enforcement** in compliance with data protection and privacy laws. [FC,24]	Invites	Member States, Europol, Commission	Commission to propose roadmap by 2025 Q2	
5. Strengthen their capabilities to defend and secure CSDP missions and operations in light of the increase of malicious cyber activities	Invites	Commission, EEAS, Member States	Ongoing	

Measures [Conclusions, paragraph]	Action words used	Responsible Entity(s)	Timeline	State of play / Comments
from State and non-State actors on EU CSDP missions and operations [CD,9]				

VI. Skills

Measures [Conclusions, paragraph]	Action words used	Responsible Entity(s)	Timeline	State of play / Comments
1. Further develop the **Cybersecurity Skills Academy**. [FC,12]	Calls	Commission, ENISA, ECCC	Updates by 2025	
2. Promote **international cooperation on mutual recognition of cybersecurity skills frameworks**. [FC,12]	Calls	ENISA, Member States	Ongoing	
3. Enhance **cybersecurity workforce development** through partnerships with academia, public, and private sector. [FC,12]	Calls	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]	Invites, calls on	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]	Encourages	ENISA, ECCC	Ongoing	

Measures [Conclusions, paragraph]	Action words used	Responsible Entity(s)	Timeline	State of play / Comments
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]	Invites	Commission	Ongoing	
7. Liaise with Member States interested in **setting up a EDIC**. [ENISA,24]	Invites	Commission	Ongoing	
8. Prioritise supporting Member States' **skills** and education efforts, **strengthening general public awareness** and collaborate with the ECCC where appropriate. [ENISA,24]	Invites	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]	Calls	Commission		Done, ECCC gained financial autonomy
10. Exchange **information on best practices to develop skilled cybersecurity professionals,** leveraging the synergies between military, civilian and law enforcement initiatives. [CD,29]	Invites	Member States, Commission, ENISA, EDA, ESDC	Ongoing	

VII. Cooperation with Private Sector

Measures [Conclusions, paragraph]	Action words used	Responsible Entity(s)	Timeline	State of play / Comments
1. Engage with **private sector stakeholders** to strengthen cybersecurity measures and foster collaborative initiatives. [FC,22] **2.** **Bolster cooperation** with the private sector. [ENISA,25]	1. Calls 2. Encourages	1. Commission, ENISA, ECCC, Member States, High Representative, CSIRT's Network, Europol	Ongoing	

Measures [Conclusions, paragraph]	Action words used	Responsible Entity(s)	Timeline	State of play / Comments
		2. ENISA, in close cooperation with the Member States and across EU entities, High Representative		
3. Encourage **voluntary information sharing** between private entities and public authorities. [FC,23]	Calls	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]	Calls	Commission, relevant Council bodies	explore options for such a mechanism before the end of 2022	

VIII. Future Threats and Emerging Technologies

Measures [Conclusions, paragraph]	Action words used	Responsible Entity(s)	Timeline	State of play / Comments
1. Establish and implement the **roadmap for the transition to Post-Quantum Cryptography (PQC), as well as exchange views on the topic**.. [FC,35]	Encourages	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]	Invites	Commission, ENISA, Member States, NIS CG, High Representative	Ongoing	

Measures [Conclusions, paragraph]	Action words used	Responsible Entity(s)	Timeline	State of play / Comments
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]	Encourages	ENISA and where relevant the ECCC	Ongoing	
4. **Pursue in the risk-based approach** to tackle possible security risks of emerging and disruptive technologies[7]. [SCS,6]	Encourages	Member States		
5. Adjust to new threats by **actively and continually monitoring, analysing, and assessing the supply chain threat landscape**, to raise awareness and build knowledge about threats and vulnerabilities, and to **proactively alert relevant entities** in a tailored manner[8]. [SCS,7]	Stresses the necessity to	General		

IX. Cyberdiplomacy and International Cooperation

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

[7] Relevant also for the chapter on risk assessment.

[8] Relevant also for the chapter on risk assessment.

Measures [Conclusions, paragraph]	Action words used	Responsible Entity(s)	Timeline	State of play / Comments
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]	Encourages	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]	Acknowledges	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]	Underlines the need	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]	Calls	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]	Calls	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]	Commits itself	Council via Member States	Ongoing	

Measures [Conclusions, paragraph]	Action words used	Responsible Entity(s)	Timeline	State of play / Comments
10. Establish the Programme of Action for **advancing responsible State behaviour in cyberspace (PoA).** [CP,18]	Underlines that will actively work towards	High Representative, Member States	Ongoing	
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]	Emphasises	EU, Member States	Done	
12. Further **mobilise the NDICI, the IPA III and other financial tools**, such as the EPF and the Global Gateway Initiative, to support strengthening the resilience of our partners. [CP,20]	Calls on	Commission, High Representative		
13. 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]	Requests	High Representative	Ongoing	
14. 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]	Calls	High Representative	Ongoing	

Measures [Conclusions, paragraph]	Action words used	Responsible Entity(s)	Timeline	State of play / Comments
15. 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]	Encourages	High Representative, Commission, Member States	Ongoing	
16. Work towards a **revised version of the implementing guidelines of the EU Cyber Diplomacy Toolbox**, notably by exploring additional response measures. [CP,23]	Invites	Member States, High Representative, with the support of the Commission	Ongoing	
17. 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]	Underlines the need	Member States, High Representative, Commission, ENISA	Ongoing	
18. 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]	Invites	EEAS, EDA, EU Military Staff		
19. 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]	Invites	General		
20. 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	Calls	High Representative, Commission, CERT-EU	N/A	

Measures [Conclusions, paragraph]	Action words used	Responsible Entity(s)	Timeline	State of play / Comments
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]				
21. 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]	Notes the need	Member States, EU INTCEN, EEAS	Ongoing	
22. 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]	Calls	High Representative, in cooperation with the Commission	Ongoing	