Council of the European Union

Brussels, 21 May 2024
(OR. en)

10133/24

CYBER 169
TELECOM 187
COSI 87
COPEN 260
CSDP/PSDC 376
DATAPROTECT 212
IND 273
RECH 241
PROCIV 40
HYBRID 83
IPCR 38
JAI 839
RELEX 688
POLMIL 182

OUTCOME OF PROCEEDINGS

From:	General Secretariat of the Council
To:	Delegations
No. prev. doc.:	9252/24
Subject:	Council Conclusions on the Future of Cybersecurity: implement and protect together

Delegations will find in the annex the Council conclusions on the the future of cybersecurity

- Implement and protect together, as approved by the Council at its meeting held on 21 May 2024.

ANNEX

Council Conclusions on the future of cybersecurity

- Implement and protect together -

THE COUNCIL OF THE EUROPEAN UNION,

RECALLING its conclusions and actions on:

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

– EU Cyber Defence Policy Framework[2],

– Internet Governance[3],

– Cyber Diplomacy[4],

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

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

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

1 12109/13
2 15585/14
3 16200/14
4 6122/15+COR 1
5 14540/16
6 14435/17 + COR 1
7 10474/17

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

– EU External Cyber Capacity Building Guidelines[9],

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

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

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

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

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

– Shaping Europe's Digital Future[15],

– The Cybersecurity of connected devices[16],

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

---

8 10086/18
9 10496/18
10 OJ L 320, 17.12.2018, p.28-34
11 7737/19
12 14517/19
13 9596/19
14 14972/19
15 8711/20
16 13629/20
17 7290/21

– Security and Defence[18],

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

– A Strategic Compass for Security and Defence[20],

– the development of the European Union's cyber posture[21],

– ICT Supply Chain Security[22],

– EU Policy on Cyber Defence[23],

– The EU Space Strategy for Security and Defence[24],

– Cyber Crisis Management Roadmap[25],

– The Communication from the Commission "Implementation of the 5G cybersecurity Toolbox"[26],

– The future of EU digital policy.

18 8396/21
19 13048/21
20 7371/22
21 9364/22
22 13664/22
23 15721/22 and 9618/23
24 14512/23
25 15423/22
26 C(2023) 4049 Final

1. NOTES the ever-increasing interconnectivity and importance of the digital domain for the functioning of our society and economy. UNDERLINES the crucial role of cybersecurity as a cornerstone of a successful digital society by maintaining public trust of the systems on which it relies. HIGHLIGHTS the significantly increasing level, complexity and scale of cybersecurity threats, in particular in the wake of the COVID pandemic, Russia's war of aggression against Ukraine, growing global geopolitical tensions, as well as technological developments such as Artificial Intelligence and quantum technology. RECOGNISES the European Union (EU) 's commitment to uphold the international rules-based order to further shape and safeguard the benefits of a free, global, open, and secure cyberspace for future generations.

2. While NOTING that the infrastructure of the internet is mostly privately owned, and digital services are often offered by private providers, ACKNOWLEDGES the public impact, cross-border nature and spill-over risk of cybersecurity threats, as well as the sole responsibility of each Member State on national security and their responsibility for the response to large-scale cyber security incidents and crises affecting them. Therefore EMPHASISES the key role and shared responsibility of Member States, and the EU to set and implement a clear and agile regulatory and policy framework laying down our collective ability to protect, detect, deter and defend against, cyberattacks and recover from them. The implementation of the framework should build on the multi-stakeholder approach of the cybersecurity ecosystem and cooperation with international organisations and partners.

FOCUS AREAS FOR POLICY-MAKING

3. WELCOMES the significant legislative and non-legislative progress achieved within the EU's cybersecurity policy framework during the last five years, which contributes to strengthening the resilience and competitiveness of the EU economy and society, while also contributing to international rule setting and implementing the UN Framework of Responsible State Behaviour in Cyberspace. Increasing the cyber resilience of entities and the cybersecurity of products with digital elements should be a continued focus for policy makers, including steps such as vulnerability management, supply chain security, the development of the necessary skills throughout the workforce and increased international dialogues on standards and cooperation. Yet, ACKNOWLEDGES the significant human, financial and operational resources required from society, businesses and governments for their implementation.

4. CALLS on the Member States, Commission and involved European entities to focus on facilitating a structured, efficient, comprehensive and timely implementation of these newly set rules, including with practical guidance. In this regard, CALLS on the Commission, the European Union Agency for Cybersecurity (ENISA), the European Cybersecurity Competence Centre (ECCC), as well as the EU's Computer Emergency Response Team (CERT-EU), the European Cybercrime Centre Europol (EC3), the NIS Cooperation Group (NIS CG), the CSIRTs Network, EU-CyCLONe (European Union- Cyber Crises Liaison Organisation Network) and national CSIRTs, competent authorities and National Coordination Centres (NCC) to support all stakeholders with this implementation, in line with their respective roles and responsibilities.

5. CALLS for actions facilitating and supporting compliance and reducing administrative burden, especially for micro, small and medium enterprises (SMEs).

6. As streamlining incident notification obligations across relevant legislative acts is a particular challenge, ACKNOWLEDGES the potential of the concept of a single entry point for incident notification and ENCOURAGES Member States to reflect on the possibilities to implement it at the national level. INVITES the Commission to prepare, with the support of ENISA and other relevant EU entities, a mapping of relevant reporting obligations set out in the respective EU legislative acts in cyber and digital matters in order to identify opportunities to reduce the administrative burden.

7. CALLS on the Commission to swiftly move forward with the adoption of delegated and implementing acts, especially those that are mandatory for the implementation of the NIS2 Directive and the Cyber Resilience Act. CALLS as well to continue the work on harmonised standards in cooperation with Member States, in order to support the implementation of EU cybersecurity legislation building on relevant work of European and International Standardisation bodies. INVITES the Commission, in cooperation with ENISA and the Member States, to closely collaborate with international partners on this subject, in order to safeguard the human-centric approach within such standards.

8. STRONGLY CAUTIONS against fragmentation, duplication or overlap of cybersecurity regulation across the Union by sector specific initiatives or *lex specialis*. Cybersecurity is not only a sector but also a horizontal domain. UNDERLINES the inherent coherence between digital and cybersecurity policy. Therefore, URGES the Commission to ensure a coherent approach in future initiatives, which should strengthen or complement existing structures, avoiding unnecessary complexity and duplication. STRESSES in this regard the importance of thorough impact assessments for all new legislative initiatives which is a key part of the Better Regulation Agenda. CALLS on the Commission to develop a clear overview of the relevant horizontal and sectoral legislative frameworks and their interplay. UNDERLINES the importance of horizontal coordination within the EU on cyber issues across sectors and domains and LOOKS FORWARD to continue to strengthen this coordination.

9. INVITES the Commission to collaborate with relevant national experts and policy makers, including at strategic level, as well as with all relevant EU entities and networks before launching new initiatives. Similarly INVITES Member States to exchange lessons learned on new national proposals through existing structures.

10. WELCOMES the European Common Criteria-based cybersecurity certification scheme (EUCC) as the first adopted scheme under the Cybersecurity Act, yet EXPRESSES concern on the slow and challenging development of the European cybersecurity certification schemes, and calls for the smooth adoption of high quality schemes. EMPHASISES the need for a thorough, comprehensive and transparent review of the European cybersecurity certification framework, to enable a faster and more transparent adoption of certification schemes with full involvement of Member States. In this regard, CALLS on the Commission to take into account the key role of the European Cybersecurity Certification Group.

11. REITERATES that the European cybersecurity certification schemes may decrease fragmentation and ensure harmonisation in the Union, while strengthening resilience and trust in an enhanced digital and cybersecurity ecosystem. NOTES that in certain cases additional requirements going beyond certification may be necessary to ensure trust. WELCOMES the political agreement on the amendment to the Cyber Security Act that introduce the certification of managed security services. ACKNOWLEDGES the opportunity for certification to stimulate higher levels of cybersecurity, including by seeking to make cybersecurity measures standard practice for organisations. RECOGNISES the potential for EU certification to support the implementation of existing legislation and support the actions of competent national authorities within the context of NIS2, the Cyber Resilience Act and other cybersecurity regulations.

12. EMPHASISES the need for sufficient skilled experts for all the relevant national and EU entities in the cybersecurity domain. ENCOURAGES cooperation among all stakeholders, including the private sector, academia and public sector to close this skills gap and STRESSES the importance of paying particular attention to closing the digital gender gap as well, taking into account the innovative potential and expansion of the talent pool that a diverse workforce offers. CALLS for the further development of the Cybersecurity Skills Academy and implementation of its actions to strengthen the EU cybersecurity workforce. INVITES ENISA and the ECCC together with the NCCs to continue their involvement and clarify roles, and CALLS to consider exploring the synergies with any future EDIC (European Digital Infrastructure Consortium) on this topic as well as potentially with the European Security and Defence College and the European Union Agency for Law Enforcement Training (CEPOL) Cybercrime Academy. Recognising that workforce skills are highly mobile in a global marketplace, CALLS for international cooperation in particular on the potential for mutual recognition of skills frameworks.

13. Without pre-empting the negotiations of the Multiannual Financial Framework, EMPHASISES the need for adequate funding for EU entities active in the cybersecurity domain in light of the significantly increasing cybersecurity threats across the EU; and. CALLS on the Commission to prioritise between actions when preparing the draft general budget of the Union. ACKNOWLEDGES the need for financial and other incentives to foster innovation in cybersecurity across the EU and secure the digital single market. To this end, CALLS on the Commission, the ECCC and relevant national authorities to stimulate and support use by, in particular, European businesses, research institutions and academia of EU cyber security funding. In light of the scale and complexity of the cybersecurity threats, ACKNOWLEDGES that European funding alone is not sufficient and therefore STRESSES the importance of attracting and investing private capital.

14. NOTES how during the last five years, notable attention has been directed towards imposing obligations upon potential targets of cyber-attacks, to strengthen their cyber resilience. POINTS out that Member States' CSIRTs, in line with their respective roles, possess the capacity to undertake proactive measures aimed at safeguarding individual users and organisations on a much larger scale, including the possibility of pre-emptive incident prevention or the provision of centralised assistance for self-protection. WELCOMES the integration of Active Cyber Protection (ACP) as a concept within the NIS2 Directive, as well as Coordinated Vulnerability Disclosures, and SUPPORTS their active promotion. CALLS ON Union entities and Member States to place greater emphasis on concrete and scalable preventive and protective measures and, where appropriate, to collaborate in a cross-border manner and with private entities. CALLS ON ENISA and the ECCC to stimulate such collaborative projects at national and EU level. Such centralised provision of support and protection not only helps achieve cost-effectiveness, but also holds the potential to address the substantial deficit of cybersecurity experts, which might otherwise necessitate individual recruitment by each organisation.

15. REITERATES the potential of digital identity to bolster online security and trust in a proactive and inclusive manner. With the Regulation for a European Digital Identity Framework, the EU holds a unique prospect to use digital identity in the ongoing battle against phishing or social engineering, which remain persistent and pervasive vectors of cyberattacks. Against the backdrop of increased misuse of emerging and disruptive technologies (such as AI, for example for the creation of deepfakes), the role of authenticated digital identity assumes augmented importance in strengthening digital trust and confidence. UNDERLINES at the same time the importance of preserving the option of anonymity within the digital world and support of the principle of data minimisation, including the use of pseudonyms, asking users to share only the minimum data necessary for the specific purpose. CALLS on the Union to swiftly implement solutions within the European Digital Identity Framework, to allow businesses, organisations, and individuals to voluntarily identify themselves online in a trusted manner, and STRESSES the crucial importance of the cybersecurity of these solutions. ENCOURAGES the timely development of European cybersecurity certification schemes adopted pursuant to Regulation (EU) 2019/881 for the certification of the European Digital Identity Wallets.

16. WELCOMES the risk assessment on the cybersecurity and resilience of Europe's communications infrastructures and networks carried out by the NIS Cooperation Group, and CALLS UPON Member States, Commission and ENISA to work on the implementation of the strategic and technical recommendations to mitigate the threats and risks that may have been identified. CALLS on the Commission, the High Representative and ENISA, together with NIS Cooperation Group, within their respective mandates, to swiftly develop a coherent and comprehensive approach across sectors to risk assessment and scenario building, based on a common methodology. This should include prioritisation, minimising duplication, ensuring the quality of these assessments and building synergies, that pursue an all-hazards approach and that the Commission, the High Representative and relevant working parties and networks within the Council take into account the ongoing efforts to counter hybrid threats, such as physical sabotage and foreign information manipulation and interference.

17. REITERATES its commitment towards ensuring the security of the ICT supply chains as indicated in the Council Conclusions on ICT supply chain security, while noting the relevance of non-technical risk factors in this context, such as undue influence by a third State on suppliers and service provider. CALLS on the NIS Cooperation Group to continue working on the ICT Supply Chain toolbox and the risk assessments and evaluations with the focus on the ICT supply chain security, in particular in relation to technologies necessary for the green and digital transition.

STRENGTHENING THE INSTITUTIONAL FRAMEWORK

18. WELCOMES, over the course of the last five years, the necessary further enhancement of already existing cybersecurity cooperation structures and entities (notably the CSIRTs Network, NIS Cooperation Group, CERT-EU, ENISA) and the creation of new structures (ECCG, EU-CyCLONe, ECCC and network of NCCs and Military CERT operational Network -MICNET-). CALLS upon these structures and entities to fully implement their mandate and, in the context of an increasing complexity of the European cybersecurity ecosystem, to strengthen cooperation and avoid possible duplication of efforts. INVITES Member States driven cooperation networks such as the NIS Cooperation Group, and, supported by ENISA, the CSIRTs Network and EU-CyCLONe to establish a multi-annual strategic perspective, in full respect of their legal mandate. CALLS on the Commission and the High Representative, working closely with relevant EU entities, to develop across policy domains a clear overview of the roles and responsibilities of all relevant EU entities, stakeholders and networks, both civilian and military, active in the cybersecurity domain, including in their interaction.

19. RECOGNISES ENISA's key supportive role to improve the level of cybersecurity in the Union and the Member States. ENCOURAGES ENISA to continue its efforts to support the implementation of relevant Union law and policy, to contribute to common situational awareness through close cooperation with Member States, EU entities, and the private sector, to assess the cyber threat landscape, and to support operational cooperation and the building of capacity. CALLS on the Commission to take duly into account the development of ENISA’s role reviewing the Cybersecurity Act. CALLS upon ENISA to establish clear priorities, including focusing on supporting the Member States through existing structures.

20. UNDERLINES the importance of fortifying the cybersecurity of EU entities to protect information and safeguard a strong EU cyber posture. ENCOURAGES the swift implementation of the Act on a high level of cybersecurity of EU institutions, bodies and agencies, accompanied by a decisive Interinstitutional Cybersecurity Board, enhancement of the security culture within EU entities and an allocation of adequate resources for ICT security. ENCOURAGES CERT-EU to develop its role further in line with this Regulation, and in this regard pay particular attention to the close cooperation with relevant networks such as the CSIRTs Network.

21. ACKNOWLEDGES the increasingly important role of the ECCC within the developing cyber framework of the EU. CALLS on the ECCC and the Commission to swiftly complete the actions needed for the ECCC to gain financial autonomy and finalise its institutional set up. ENCOURAGES the National Coordination Centres and the ECCC to swiftly activate the Cybersecurity Competence Community in a streamlined manner, as a bottom-up, inclusive and key forum for collaboration with industry, academic and research organisations, other relevant civil society associations, public entities and other entities dealing with cybersecurity. CALLS on all Union entities and Member States to support this effort and to preserve the central role of the ECCC in coordinating the EU cybersecurity investment strategy, boosting the EU cybersecurity industry and fostering skilled experts to enhance the EU's cybersecurity resilience, as well as to increase consistency and synergies with the ECCC's agenda. INVITES policy makers at European and national level to contemplate a more efficient use of investment as an enabler or a complement to legislation in increasing cybersecurity.

22. Given the crucial role and expertise of the private sector in the security of our digital infrastructure and the protection of entities and citizens that depend on it, CALLS on Member States, the Commission, the High Representative, ENISA, ECCC, the CSIRTs Network and Europol to thoroughly, openly and in a coordinated manner engage with all relevant private sector stakeholders to fortify cybersecurity measures, foster collaborative initiatives, and formulate robust strategies to mitigate the risks posed by cyber threats, including regarding business continuity. Such engagement could include communities of information sharing, support to SMEs, or cooperation agreements on operational projects.

23. CALLS on Member States and the Commission, in cooperation with all relevant networks and entities on the Union level to increase voluntary information sharing in view of a common situational awareness, including, for Member States, through the EU Intelligence Analysis Centre (EU INTCEN). STRESSES the need to prevent any duplication of efforts in this regard and UNDERLINES the importance of cooperation with the private sector, at national and Union level and according to the appropriate procedures. WELCOMES in this regard the political agreement on the Cyber Solidarity Act including its future contribution to the common detection and situational awareness of cyber threats and incidents.

24. CALLS on the Commission, relevant Union entities, in particular Europol and Eurojust, and Member States, making best use of the European Multidisciplinary Platform Against Criminal Threats (EMPACT), to strengthen their collaboration on the significant threat posed by cybercrime, including the pressing issue of ransomware, and to enhance processes to investigate cybercrime. Given how law enforcement actions to disrupt cybercriminal activities also contribute to the prevention of further cybersecurity incidents, a structured and mutually beneficial collaboration between the cybersecurity and law enforcement communities is necessary to further enhance the state of cybersecurity in Europe. STRESSES that in the crucial fight against cybercrime, it is equally important to protect data and ensure privacy, including through secure communications. REITERATES that competent authorities must be able to access data in a lawful and targeted manner, in full respect of fundamental rights and the relevant data protection laws, while upholding cybersecurity. REAFFIRMS its support to the development, implementation and use of strong encryption as a necessary means of protecting fundamental rights and the digital security of individuals, governments, industry and society. Therefore, INVITES Member States and the relevant EU entities to stimulate a structured and appropriate information exchange between national CSIRTs and law enforcement, as well as at EU level between Europol, the CSIRTs Network and CERT-EU, including for victim notification purposes.

25. Given the cyber threat landscape and the fast pace of technological development, HIGHLIGHTS the importance of comprehensive cooperation between civilian and military domains, including between EU cooperation networks. WELCOMES the progress made by Member States and relevant Union entities in implementing the EU Cyber Defence Policy.

26. Building on the Commission Recommendation on coordinated response to large-scale cybersecurity incidents and crises, and on the provisions of Directive (EU) 2022/2555, guided by the Cyber Crisis Management Roadmap developed in the Council under the Czech Presidency, and without prejudice to the Member States' sole responsibility for safeguarding national security. STRESSES the need to evaluate and further develop the EU cybersecurity crisis management framework integrating new developments and avoiding fragmented Union procedures.

27. Therefore ENCOURAGES Member States to regularly take stock of progress achieved in the implementation of the Roadmap, CALLS upon the Commission to swiftly evaluate the current cybersecurity Blueprint and, on this basis, propose a revised Cybersecurity Blueprint in the form of a Council recommendation that will address the current challenges and complex cyber threat landscape, strengthen existing networks, enhance cooperation, and break silos between organisations, utilising to this end first and foremost existing structures. Furthermore, the revised Blueprint should rely on time-tested guiding principles of cooperation (proportionality, subsidiarity, complementarity and confidentiality of information) and expand them to the full crisis management lifecycle and should contribute to aligning and enhancing secure communication in the cybersecurity field. The revised Blueprint should ensure its compatibility with existing frameworks such as the IPCR, the EU Cyber Diplomacy Toolbox, the EU Hybrid Toolbox, the Law Enforcement Emergency Response Protocol (LERP), emerging frameworks such as the Critical Infrastructure Blueprint, sectoral procedures, and overall crisis management structures within Union entities, involving also the High Representative and Europol. In this revised Blueprint, the role of the Commission, the High Representative and ENISA, in line with their competences, should focus in particular on supporting horizontal coordination.

28. UNDERLINES that frequent cybersecurity exercises and training, including, possibly, involving the private sector, strengthen resilience and can effectively decrease the costs, duration and severity of cyber security incidents in organisations. EMPHASIZES that upon its adoption, the new revised Blueprint should be tested as early and to the fullest extent possible, at a technical, operational and political level.

THE INTERNAL/EXTERNAL NEXUS FOR CYBERSECURITY POLICY

29. UNDERSCORES that cybersecurity in the European Union cannot be tackled in a vacuum. and that an active international cyber policy, including in the UN, NATO, OSCE, ITU, Council of Europe and other multilateral and multistakeholder organisations, is an essential contribution to European cybersecurity. A strong European cybersecurity is also key for the European diplomatic posture. Synergies between the EU's internal and external cyber initiatives should be captured where possible. STRESSES that a secure cyberspace is not only defined at the nexus between internal and external European policy, but also between the digital and the security domains, as well as between the civilian and the defence domain. In this context, the European efforts regarding cyber capacity building, cyber diplomacy and cyber defence via various Council conclusions and instruments contribute significantly to European cybersecurity. STRESSES the importance of pragmatic cooperation while safeguarding the distinction between civilian and military, as well as national and European roles and responsibilities. In full respect of the agreed guiding principles on EU-NATO cooperation, in particular reciprocity, inclusiveness, decision-making autonomy and full transparency towards all Member States, EMPHASISES the importance of close EU-NATO cooperation on emerging and disruptive technologies in view of creating synergies and avoiding unnecessary duplication.

30. INVITES the Member States and relevant EU entities to engage with countries and actors outside of the Union in order to increase international cooperation against cybercrime. In this regard, WELCOMES the work of the Counter Ransomware Initiative (CRI) and the commitment of the EU, its Member States and entities to the CRI's Joint Statement on Ransomware Payments as well as the work carried out in cooperation with third states including through EMPACT.

31. UNDERLINES the importance of fostering the European market for trusted digital products. HIGHLIGHTS in this context the adoption of the Cyber Resilience Act that will enhance the overall level of security for all products with digital elements and also UNDERLINES the importance of EU cybersecurity certification schemes. WELCOMES in this context the ongoing transatlantic cooperation, including through the agreement of an EU-US Joint Cyber Safe Product Action Plan to prepare the ground to explore mutual recognition on cybersecurity requirements for IoT hardware and software. WELCOMES the contribution of these efforts to a strong international ecosystem.

32. RECALLS that secure, resilient, accessible, available and affordable digital infrastructure and connectivity solutions are a decisive factor for economic and social progress and development opportunities in third countries; ensuring rights and freedoms of citizens and enabling trusted transactions between citizens, businesses and governments. STRESSES that cyber capacity building and its contribution to the cybersecurity of digital infrastructure is a condition for the transition into a safe, secure and responsible digital society, which contributes also to improving the EU's collective cybersecurity. EMPHASISES the importance of the Teams Europe approach and calls on the Member States, Commission and High Representative and to strengthen this in cyber capacity building. STRESSES the need to create awareness on the importance of secure connectivity and trusted suppliers in third countries, including by offering technical assistance and by sustaining investment in secure and trusted connectivity, which incentivises increased alignment with the EU Toolbox on 5G cybersecurity.

33. UNDERLINES that the integration of geopolitical considerations into technical endeavours, such as the EU Toolbox on 5G cybersecurity, coordinated risk assessments or specific certification schemes, can present a challenge. This must be approached with due regard for European market principles, while effectively addressing threats and risks. WELCOMES the progress made by Member States in implementing the measures of the EU Toolbox on 5G cybersecurity. However STRESSES the need to complete its implementation in view of minimising exposure to high-risk suppliers and of avoiding dependency on these suppliers at national and EU level. ACKNOWLEDGES the commitments made by the Commission in its Communication from June 2023 to avoid exposure of its corporate communications to mobile networks using high-risk suppliers as well as to make its assessment available for the design of all relevant EU funding programmes and instruments.

THE CYBERSECURITY DIMENSION OF EMERGING AND DISRUPTIVE TECHNOLOGIES

34. STRESSES the attention needed from an EU cybersecurity policy perspective to the challenges and opportunities presented by emerging and disruptive technologies that are critical to our future development such as AI, quantum and 6G technology. RECOGNISES their potential to introduce game-changing threats to cybersecurity and UNDERSCORES the necessity of addressing these developments with sufficient care and attention. ACKNOWLEDGES at the same time the potential opportunities in the cybersecurity field these technologies offer, including technologies aiming to protect the confidentiality of digital communications such as end-to-end encryption, enhance protection measures and scale-up CSIRT services. Therefore, INVITES Member States, the Commission, ENISA and the NIS Cooperation Group to consider concrete non-legislative risk-based initiatives such as roadmaps and action plans to further guide EU action in this area, incentivising innovation and addressing risks efficiently by leveraging a broad range of existing tools and mechanisms. RECALLING that the use and development of technologies should respect human rights, be privacy-focused and that their use is lawful, safe and ethical.

35. UNDERLINES that the transition to Post-Quantum Cryptography (PQC) has clear priority to protect classified and sensitive information in anticipation of the threats posed by future cryptographically relevant quantum computers. In this regard, ACKNOWLEDGES the Commission Recommendation on a Coordinated Implementation Roadmap for the transition to PQC addressing the current and future cybersecurity needs in Union entities, national public administrations and other critical infrastructure, taking into consideration the rapidly evolving computing power and novel trends in technologies. ENCOURAGES Member States to further engage and exchange views on activities and strategic decisions for the transition to PQC. RECOGNIZES that the transition to PQC may require hybrid schemes that combine this technology with existing cryptographic approaches. In the future, further improvements could allow quantum key distribution to also contribute to secure communications.

36. RECOGNISES the role of free and open-source software as a major public good of the digital age as well as the special nature of many open-source development models. NOTES that, given its prevalence in supply chains, free and open-source software also remains a major cybersecurity challenge in the EU and globally. However, the inherent and unique advantage is that its entirely transparent nature allows for security vulnerabilities to be comprehensively addressed. Therefore, UNDERLINES the need to promote a consistent, coherent and transparent policy approach to free and open-source software including concrete measures aimed at supporting the security of free and open-source software projects that are of public interest or widely used across the European economy.

CONCLUSION

37. CONCLUDES that in light of the changed and rising threat level, the EU Cybersecurity Strategy from December 2020 should be reviewed, updating its objectives and approach, setting a clear framework with roles and responsibilities for all entities involved, straightforward and efficient coordination mechanisms and an enhanced cooperation with the private sector and academia. Therefore INVITES the Commission and the High Representative to assess the results and gaps of the current Strategy and its impact, and to present on this basis a revised strategy without undue delay, which will reflect these Conclusions.