Council of the European Union

Brussels, 9 March 2021
(OR. en)

6722/21

CYBER 55	RECH 86
JAI 227	COMPET 151
JAIEX 23	IND 52
EJUSTICE 25	COTER 25
COSI 39	ENFOPOL 80
DATAPROTECT 54	COPS 79
COPEN 103	MI 136
TELECOM 88	IXIM 43
PROCIV 21	POLMIL 25
CSC 85	HYBRID 10
CIS 35	CSCI 34
RELEX 168	POLGEN 33

'I/A' ITEM NOTE

From:	General Secretariat of the Council
To:	Permanent Representatives Committee/Council
Subject:	Draft Council conclusions on the EU's Cybersecurity Strategy for the Digital Decade

1. On 16 December 2020, the Commission and the High Representative of the Union for Foreign Affairs and Security Policy published its Joint communication to the European Parliament and the Council "The EU's Cybersecurity Strategy for the Digital Decade"[1]. The new Cybersecurity Strategy aims to bolster Europe's collective resilience against cyber threats and ensure that all citizens and businesses can fully benefit from trustworthy and reliable services and digital tools.

[1] 14133/20

2. The Commission and the EEAS presented the Joint communication at the informal videoconference of the Horizontal Working Party on cyber issues (HWPCI) on 17 December 2020 and on 12 January 2021. At the informal videoconference of the HWPCI on 17 December 2020, the incoming Portuguese Presidency announced its intention to prepare draft Council conclusions on the EU's Cybersecurity Strategy for the Digital Decade.

3. The Presidency presented a first draft of the Council conclusions at the informal videoconference of the HWPCI on 2 February 2021. These conclusions were subsequently discussed at informal videoconference meetings of the HWP CI on 9 February 2021, on 19 February 2021 and on 1 and 9 March 2021.

4. Since the draft conclusions also contain a reference to the EU's defence policies (paragraph 30) the Politico-Military Group (PMG) discussed the relevant paragraph at its meeting on 10 February 2021.

5. Various paragraphs relate to the Common Foreign and Security Policy (paragraphs 1, 4, 7, 8, 9, 20, 23, 24, 26, 27, 28, 29, 30, 31, 32 and 33) and were therefore submitted to the Political and Security Committee which endorsed these paragraphs at its meeting on 4 March 2021.

6. At its informal videoconference on 9 March 2021, the HWPCI reached agreement on the draft Council conclusions as set out in 6722/21.

7. In view of the above, the Permanent Representatives Committee is invited to submit the draft Council Conclusions, as set out in annex to the Council and to suggest that it adopts the draft conclusions as an 'A' item on its agenda.

ANNEX

Draft Council Conclusions on the EU's Cybersecurity Strategy for the Digital Decade

THE COUNCIL OF THE EUROPEAN UNION,

RECALLING its conclusions on:

- the Joint Communication of 25 June 2013 to the European Parliament and the Council on the Cybersecurity Strategy for the European Union: "An Open, Safe and Secure Cyberspace"[2],

- Internet Governance[3],

- the Joint Communication of 20 November 2017 to the European Parliament and the Council: "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU"[4],

- cybersecurity capacity and capabilities building in the EU[5],

- the significance of 5G to the European Economy and the need to mitigate security risks linked to 5G[6]

- the future of a highly digitised Europe beyond 2020: "Boosting digital and economic competitiveness across the Union and digital cohesion"[7],

- complementary efforts to Enhance Resilience and Counter Hybrid Threats[8],

- shaping Europe's Digital Future[9],

---

2 12109/13
3 16200/14
4 14435/17 + COR 1
5 7737/19
6 14517/19
7 9596/19
8 14972/20
9 8711/20

- Digital Diplomacy[10],

- strengthening resilience and countering hybrid threats, including disinformation in the context of the COVID-19 pandemic[11],

- Cyber Diplomacy[12],

- EU Coordinated Response to Large-Scale Cybersecurity Incidents and Crises[13],

- a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox")[14],

- EU External Cyber Capacity Building Guidelines[15],

- A recovery advancing the transition towards a more dynamic, resilient and competitive European industry[16],

- the cybersecurity of connected devices[17],

- Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry[18],

- and its Council Resolution on Encryption - Security through encryption and security despite encryption[19],

---

10 12804/20
11 14064/20
12 6122/15 + COR 1
13 10086/18
14 10474/17
15 10496/18
16 13004/20
17 13629/20
18 14540/16
19 13084/1/20 REV 1

- and the Member States' declaration of 15 October 2020 on building the next generation cloud for business and the public sector in the EU,

RECALLING the European Council Conclusions on COVID-19, the Single Market, industrial policy, digital and external relations of 1-2 October 2020[20] and those on disinformation and hybrid threats and on a new strategic agenda 2019-2024 of 20 June 2019[21],

RECALLING the Global Strategy for the European Union's Foreign and Security Policy - Shared vision, Common Action: a Stronger Europe of 28 June 2016,

RECALLING the Communications of the European Commission on shaping Europe's Digital Future of 19 December 2020[22] and on the EU Security Union Strategy of 24 July 2020[23],

RECALLING the joint Communication of the European Commission and the High Representative on a new EU-US agenda for global change of 2 December 2020[24],

1. HIGHLIGHTS the fact that cybersecurity is essential for building a resilient, green and digital Europe and WELCOMES the Joint Communication to the European Parliament and the Council entitled "The EU's Cybersecurity Strategy for the Digital Decade", which outlines the new framework for the EU action in the area of "resilience, technological sovereignty and leadership" as well as to protect its people, businesses and institutions from cyber incidents and threats while enhancing the trust of individuals and organisations in the EU's ability to promote secure and reliable network and information systems, infrastructure and connectivity, and to promote and protect a global, open, free, stable and secure cyberspace grounded in human rights, fundamental freedoms, democracy and the rule of law.

---

20 EUCO 13/20
21 EUCO 9/19
22 19.2.2020 COM(2020) 67 final
23 24.7.2020 COM(2020) 605 final
24 2.12.2020 JOIN(2020) 22 final

2. RECOGNISES that the COVID-19 pandemic has brought the increased need for trust in Information and Communication Technology (ICT) tools and systems and their security to the forefront of our daily lives. STRESSES that cybersecurity and the global and open Internet are vital for the functioning of public administration and institutions at both national and EU level and for our society and the economy as a whole.

3. STRESSES the need to raise more awareness on cyber issues at the political and strategic decision-making levels by providing decision-makers with relevant knowledge and information and UNDERLINES the need to enhance the awareness of general public and promote cyber hygiene.

4. CALLS FOR the promotion and protection of the core EU values of democracy, the rule of law, human rights and fundamental freedoms, including the right to freedom of expression and information, the right to freedom of assembly and association and the right to privacy in cyberspace. WELCOMES, in this regard, further sustained efforts to protect human rights defenders, civil society and academia working on issues such as cybersecurity, data privacy, surveillance and online censorship by providing further practical guidance, promoting best practices and stepping-up the EU's efforts to prevent violations and abuses of human rights and the misuse of emerging technologies, notably through the use of diplomatic measures where necessary, as well as the export control of such technologies. EMPHASISES, in this context, the importance of the EU's Action Plan on Human Rights and Democracy 2020-2024 and its Human Rights Guidelines on Freedom of Expression Online and Offline.

5. HIGHLIGHTS that achieving strategic autonomy while preserving an open economy is a key objective of the Union in order to self-determine its economic path and interests. This includes reinforcing the ability to make autonomous choices in the area of cybersecurity with the aim to strengthen the EU´s digital leadership and its strategic capacities. RECALLS that this includes identifying and reducing strategic dependencies and increasing resilience in the most sensitive industrial ecosystems and specific areas. UNDERLINES that this can include diversifying production and supply chains, fostering and attracting investments and production in Europe, exploring alternative solutions and circular models, and promoting broad industrial cooperation across Member States.

6. Bearing in mind the shortage of digital and cybersecurity skills in the workforce, STRESSES the importance of meeting the demand of a trained workforce in the field of digital and cybersecurity in particular by developing, retaining and attracting the best talent, for instance through education and training to be able to digitize our society in a cyber-secure manner. ENCOURAGES women's and girls' increased participation in science, technology, engineering, mathematics ('STEM') education and ICT jobs upskilling and reskilling in digital skills as one of the means to bridge the gender digital divide.

7. RECALLS that the common and comprehensive EU approach to cyber diplomacy aims at contributing to conflict prevention, mitigation of cybersecurity threats and greater stability in international relations. In this context, REAFFIRMS its commitment to the settlement of international disputes in cyberspace by peaceful means, and that all of the EU's diplomatic efforts should, as a priority, be aimed at promoting security and stability in cyberspace through increased international cooperation, and at reducing the risk of misperception, escalation and conflict that may stem from ICT incidents and SUPPORTS further development and operationalisation of confidence-building measures (CBMs) at regional and international level. REITERATES the United Nations General Assembly's call, agreed by consensus, that UN Member States be guided by the UNGGE reports' recommendations in their use of ICT and REAFFIRMS the application of international law, in particular of the UN Charter in its entirety, in cyberspace.

8. REAFFIRMS that, with a view to substantially shaping international norms and standards in the areas of emerging technologies and the technical and logical infrastructure essential to the general availability and integrity of the public core of the Internet, so that these are in line with universal and EU values and through a multi-stakeholder approach, the further development of norms and standards within the Union is essential. This will ensure that the Internet remains global, open, free, stable and secure and that the use and development of digital technologies are human rights respecting, and that their use is lawful, safe and ethical. TAKES NOTE of the upcoming Standardisation Strategy and COMMITS itself to proactive and coordinated outreach to promote EU leadership and the EU's objectives at international level, including in various international standardisation bodies and through cooperation with like-minded partners, civil society, academia and the private sector.

9. STRONGLY SUPPORTS the multi-stakeholder model for Internet governance and cybersecurity and commits itself to reinforcing regular and structured exchanges with stakeholders including the private sector, academia and civil society in international fora, including within the context of the Paris Call for Trust and Security in Cyberspace. PROMOTES universal, affordable and equal access to the Internet bridging the digital divides and, in particular, the empowerment of women and girls and persons in vulnerable or marginalised situations, in both policy development and in the use of the Internet.

10. EMPHASISES the need to include cybersecurity in digital investments and initiatives in the coming years and the need to progressively contribute to a level playing field in cybersecurity and NOTES the Commission's plan to increase public spending and leverage private investment in the cybersecurity domain. HIGHLIGHTS the importance of Small and Medium Sized Enterprises (SMEs) in the cybersecurity ecosystem and RECOGNISES the relevant financial instruments available to support a strong cybersecurity focus within digital transformation over the 2021-2027 Multiannual Financial Framework (MFF) as well as in the Recovery and Resilience Facility (RRF).

11. LOOKS FORWARD to the swift implementation of the Regulation on the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres (CCCN), including the rapid set up and operationalisation of the European Cybersecurity Competence Centre in Bucharest. A prompt adoption of its agenda will contribute to maximising the effects of investments to strengthen the Union's leadership and strategic autonomy in the field of cybersecurity and support technological capacities and skills and to increase the Union's global competitiveness with input from industry and academic communities in cybersecurity, including SMEs and research centres, which will benefit from a more systematic, inclusive and strategic collaboration, having regard to the cohesion of the Union and all of its Member States.

12. WELCOMES the ongoing work led by ENISA, along with Member States and interested stakeholders, to provide the EU with certification schemes for ICT products, services and processes that should contribute to raising the overall level of cybersecurity within the Digital Single Market. In this context, LOOKS FORWARD to the Union Rolling Work Programme (URWP) with a view to develop EU cybersecurity certification schemes within the Cybersecurity Act (CSA). RECOGNISES, in this context, the pivotal role of the EU to develop standards that can shape the cybersecurity landscape and that contribute to ensuring fair competition within the EU and on the global stage, promoting market access as well as addressing security risks while ensuring the applicability of the EU legislative framework.

13. REITERATES the importance of assessing the need for horizontal legislation, also specifying the necessary conditions for the placement on the market, in the long-term to address all relevant aspects of cybersecurity of connected devices, such as availability, integrity and confidentiality. WELCOMES in this regard a discussion to explore the scope of such a legislation and its links with the cybersecurity certification framework as defined under the CSA, with the aim of raising the level of security within the Digital Single Market. STRESSES that cybersecurity requirements should be defined in line with the relevant Union legislation, including the CSA, the New Legislative Framework (NLF), the Regulation on European Standardisation and a possible future horizontal legislation, to avoid ambiguity and fragmentation in legislation.

14. ACKNOWLEDGES the importance of a comprehensive and horizontal approach on cybersecurity in the Union, while fully respecting Member States' competences and needs as well as the importance of ongoing support for technical assistance and cooperation to build the capacity of Member States. Taking into account the evolution of the cyber threat landscape, TAKES NOTE of the new proposal for a Directive on measures for a high common level of cybersecurity across the Union that builds upon the NIS Directive and reiterates its support to strengthening and harmonising national cybersecurity frameworks and sustained cooperation between Member States. Furthermore, STRESSES the need for alignment and articulation of sectoral legislation in this domain.

15. TAKES NOTE of the Commission's proposal to support Member States in establishing and strengthening Security Operation Centres (SOCs) in order to build a network of SOCs across the EU, to further monitor and anticipate signals of attacks on networks. In this context, AWAITS the Commission's detailed plans concerning the network of SOCs, while respecting the competences of the Member States. RECALLS the efforts undertaken by Member States, supported by the EU, to set up sectoral, national and regional CSIRTs and national or European Information Sharing and Analysis Centres (ISACs) as part of an effective network of cybersecurity partnerships in the Union. LOOKS FORWARD to exploring this network's potential to strengthen SOCs as well as their complementarity and coordination with existing networks and actors (most notably the CSIRTs Network), in order to promote an efficient, secure and reliable information-sharing culture. EMPHASISES that this process will build on the work carried out in the context of Artificial Intelligence and High Performance Computing initiatives and by European Digital Innovation Hubs.

16. TAKES NOTE of the possible development of a secure connectivity system, building on the European quantum communication infrastructure (EuroQCI) and the European Union Governmental Satellite Communication (GOVSATCOM), and RECOGNISES that any future possible development should be based on a robust cybersecurity framework and take into account the entire electronic communications infrastructure such as space, land and submarine network systems.

17. LOOKS FORWARD to discussions with the Commission, ENISA, the two EU DNS Root Server Operators and the multi-stakeholder community to assess the role of the two EU DNS Root Server Operators when it comes to guaranteeing that the Internet remains globally accessible and non-fragmented. WELCOMES further discussion on the Commission's intention to develop an alternative European service for accessing the global internet ("DNS4EU" initiative), based on a transparent model which conforms to the latest security, data protection and privacy by design and by default standards and rules, in order to contribute to increased resilience, while maintaining and enhancing international connectivity for all Member States.

18. RECOGNISES the need for a joint effort from the Commission and the Member States to accelerate the uptake of key internet standards, including IPv6, and well-established internet security standards as they are instrumental in increasing the overall level of security, resilience, openness and interoperability of the global internet, while increasing the competitiveness of the EU industry and in particular of the internet infrastructure operators.

19. STRESSES the importance of a coordinated approach as well as the development and implementation of effective measures at national level to reinforce the cybersecurity of 5G networks. SUPPORTS the next steps to be taken on the cybersecurity of 5G networks, as presented in the appendix to the EU's Cybersecurity Strategy and as based on the results of the report on the impacts of the Commission's recommendation on the security of 5G networks, for instance with regard to the definition of a long-term and comprehensive approach looking at the entire 5G value chain and ecosystem. With a view to further strengthen the coordinated approach to the security of 5G networks, URGES Member States, EU Institutions and other relevant stakeholders to continue their periodic stocktaking, together with the exchange of information and best practice within the dedicated NIS Cooperation Group Work Stream on 5G Cybersecurity, and report regularly on the progress made to the Council. HIGHLIGHTS, while emphasising Member States' responsibility for the protection of national security, its strong commitment to applying and swiftly completing the implementation of the EU 5G Toolbox measures and to continuing efforts made to guarantee the security of 5G networks and the development of future network generations. The close cooperation between Member States, the Commission and ENISA on security of 5G networks could serve as an example for other issues in the field of cybersecurity while respecting the competences of the Member States and the principles of subsidiarity and proportionality.

20. RECOGNISES the relevance of further integrating cybersecurity into EU crisis response mechanisms and testing these in relevant exercises and HIGHLIGHTS the importance of enhancing cooperation and information-sharing amongst the various cyber communities within the EU and of linking the existing initiatives, structures and procedures (such as the IPCR, the CSIRT Network, the NIS Cooperation Group, the CyCLONe, the European Cybercrime Centre, EU INTCEN, and other relevant EU bodies) in case of large-scale and cross-border cyber incidents and threats. TAKING INTO ACCOUNT the progress already achieved in this domain, AWAITS the Commission's proposal on the process, milestones and timeline for defining the Joint Cyber Unit (JCU) with a view to providing added value, clear focus and streamlining the EU cybersecurity crisis management framework, including through preparedness, shared situational awareness, reinforcing coordinated response and exercises, in a transparent and incremental manner while avoiding duplication and overlap and while respecting the competences of the Member States.

21. STRESSES both the importance of promoting cooperation and information exchange between relevant cybersecurity actors and competent authorities in the area of security and criminal justice, e.g. law enforcement and judicial authorities as well as the need to expand and improve the capacity of these authorities to investigate and prosecute cybercrime and to foster international negotiations and EU rules on cross-border access to electronic evidence. Independently of the technological environment of the day, it is essential to preserve the powers of competent authorities in the area of security and criminal justice through lawful access to carry out their tasks, as prescribed and authorised by law. Such laws providing for the enforcement powers must always fully respect due process and other safeguards, as well as fundamental rights, in particular the right to respect for private life and communications and the right to the protection of personal data.

22. 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 and, at the same time, ACKNOWLEDGES the need to ensure the ability of the competent authorities in the area of security and criminal justice, e.g. law enforcement and judicial authorities to exercise their lawful powers, both online and offline, to protect our societies and citizens. 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. EMPHASISES that any actions taken have to balance these interests carefully against the principles of necessity, proportionality and subsidiarity.

23. SUPPORTS and PROMOTES the Budapest Convention on Cybercrime and the ongoing work on the Second Additional Protocol to that Convention. Furthermore, continues to engage in multilateral exchanges on cybercrime, including in processes related to the Council of Europe, United Nations Office on Drugs and Crime (UNODC) and the Commission on Crime Prevention and Criminal Justice (CCPCJ), to ensure an enhanced international cooperation to counter cybercrime, including the exchange of best practices and technical knowledge and support capacity building, while respecting, promoting and protecting human rights and fundamental freedoms.

24. While national security remains the sole responsibility of each Member State, ACKNOWLEDGES the importance of strategic intelligence cooperation on cyber threats and activities, and INVITES Member States, through their competent authorities, to continue to contribute to EU INTCEN's work as the hub for situational awareness and threat assessments on cyber issues to the EU and to explore the proposal on the possible establishment of a Member States' cyber Intelligence working group in order to strengthen INTCEN's dedicated capacity in this domain, based on voluntary Intelligence contributions from the Member States and without prejudice to their competences.

25. HIGHLIGHTS the importance of a robust and consistent security framework to protect all EU personnel, data, communication networks and information systems and decision-making processes based on comprehensive, consistent and homogeneous rules. In particular, this should be done by enhancing the resilience and improving the security culture of the EU against cyber threats and by strengthening the security of classified and non-classified EU networks while ensuring an adequate governance and that sufficient resources and capabilities are made available, including in the context of the reinforcement of the mandate of CERT-EU. WELCOMES, in this context, the ongoing discussions on the establishment of common rules on information security taking due account of the Council's security rules for the protection of EU classified information, as well as the definition of common binding rules on cybersecurity for all EU institutions, bodies and agencies.

26. BUILDING ON the EU's cyber diplomacy efforts, COMMITS itself to increasing the effectiveness and the efficiency of the Cyber Diplomacy Toolbox and LOOKS FORWARD to deepening discussions on its scope and use building on lessons learned from the application of this instrument to date. These discussions should contribute to promoting security at international level by fostering dialogue and nurturing a shared vision of cybersecurity matters, strengthening prevention, stability, cooperation and advancing confidence and capacity building and, where necessary applying restrictive measures, in order to prevent, discourage, deter and respond to malicious cyber activities targeting the integrity and security of the EU and its Member States, thereby contributing to international security and stability and consolidating the EU´s cyber posture, in full respect of national competences and prerogatives. In particular, special attention should be given to preventing and countering cyberattacks with systemic effects that might affect our supply chains, critical infrastructure and essential services, democratic institutions and processes and undermine our economic security, including cyber-enabled theft of Intellectual Property. The Member States and the EU Institutions should also further reflect on the articulation between the EU cybersecurity crisis management framework, the cyber diplomacy toolbox and the provisions of Article 42(7) TEU and Article 222 TFEU, notably through scenario based work to build a common understanding of the practical modalities for the implementation of Article 42(7) TEU.

27. ACKNOWLEDGES the importance of strengthening cooperation with international organisations and partner countries in order to advance the shared understanding of the cyber threat landscape, to develop dialogues and cooperation mechanisms, to identify, where appropriate, cooperative diplomatic responses as well as to improve information-sharing, including through education, training and exercises. In particular, HIGHLIGHTS that a strong transatlantic partnership in the cybersecurity field contributes to our common security, stability and prosperity and NOTES the provisions on cybersecurity cooperation within the EU-UK Trade and Cooperation Agreement. RECALLING the key achievements of EU-NATO cooperation in the area of cybersecurity in the framework of the implementation of the 2016 Warsaw and 2018 Brussels Joint Declarations, reiterates the importance of enhanced, mutually-reinforcing and beneficial cooperation through education, training, exercises and coordinated response to malicious cyber activities, in full respect of the decision-making autonomy and procedures of both organisations, on the basis of the principles of transparency, reciprocity and inclusiveness

28. In order to contribute to a global, open, free, stable and secure cyberspace, which is of ever-increasing importance for the continued prosperity, growth, security, well-being, connectivity and integrity of our societies, COMMITS itself to continuous engagement in norm-setting processes in international organisations, especially in the UN first committee related processes, promoting and contributing to the recognition of the application of international law in cyberspace and adherence to the norms, rules and principles of responsible state behaviour in cyberspace, including by promoting the swift establishment of a Programme of Action (PoA) for Advancing Responsible States behaviour in cyberspace, as a constructive, inclusive and consensus-based follow-up of both the current UN GGE and OEWG processes.

29. RECALLS its strong commitment to effective multilateralism and a rules-based global order with the United Nations at its core and its determination to strengthen cooperation and coordination with international and regional organisations, namely the UN system, NATO, the CoE, the OSCE, the OECD, the AU, the OAS, ASEAN, the ARF, the GCC and the LAS concerning discussions on cyber-related issues as well as the continuation and expansion of structured EU cyber dialogues and consultations with third countries. STRESSES its active support to the UN, in particular in relation to its Agenda 2030, including the Sustainable Development Goals, and WELCOMES the UN Secretary General's Roadmap on digital cooperation and the UN Secretary General's Agenda for Disarmament fostering accountability and adherence to norms in cyberspace and contributing to the prevention and peaceful settlement of conflict stemming from malicious activity in cyberspace. WELCOMES the proposal to establish an informal EU Cyber Diplomacy Network by the High Representative for Foreign Affairs and Security Policy with a view to developing the engagement and expertise of both the EU and Member States on international cyber issues in order to strengthen coordinated outreach.

30. LOOKS FORWARD to the forthcoming proposal for a review of the Cyber Defence Policy Framework (CDPF), and COMMITS itself to pursuing efforts to strengthen cybersecurity and cyber defence dimensions with a view to ensuring that these are fully integrated into the wider area of security and defence, in particular in the context of the work on the Strategic Compass. CONSIDERS that the upcoming "Military Vision and Strategy on Cyberspace as a Domain of Operations" will contribute to furthering these discussions. WELCOMES the initiative by the European Defence Agency (EDA) to foster cooperation between Military CERTs and SUPPORTS efforts made to enhance civil-military synergies and coordination on cyber defence and cybersecurity, including on space-related aspects, including through the dedicated PESCO projects.

31. WELCOMES the proposal to develop an EU External Cyber Capacity Building Agenda, the proposal to create an EU Cyber Capacity Building Board and the establishment and implementation of EU CyberNet (EU's Cyber Capacity Building Network) in order to increase cyber resilience and capacities worldwide. In this context, WELCOMES cooperation with Member States, as well as with public and private sector partners, notably the Global Forum on Cyber Expertise (GFCE) and other relevant international bodies, to ensure coordination and avoid duplication. In particular, ENCOURAGES cooperation with partners in the Western Balkans and in the EU Eastern and Southern Neighbourhood.

32. To ensure that all countries are able to reap the social, economic and political benefits of the Internet and the use of technologies, COMMITS itself to assisting partner countries in tackling the growing challenge of malicious cyber activities, notably those that harm the development of their economies, societies and the integrity and security of democratic systems, including in line with the efforts under the European Democracy Action Plan.

33. In order to ensure the development, implementation and monitoring of proposals presented in the EU's Cybersecurity Strategy, and taking into account the multiannual character of some of the initiatives, ENCOURAGES the Commission and the High Representative for Foreign Affairs and Security Policy to establish a detailed implementation plan setting the priorities and the schedule of planned actions. Will MONITOR the progress in the implementation of these Conclusions by means of an Action Plan which will be regularly reviewed and updated by the Council in close cooperation with the European Commission and the High Representative.