



Council of the European Union
General Secretariat

Brussels, 08 February 2021

Interinstitutional files:
2018/0328(COD)

WK 1754/2021 INIT

LIMITE

CYBER
TELECOM
CODEC
COPEN
COPS
COSI
CSC

CSCI
IND
JAI
RECH
ESPACE
RELEX
ENFOPOL
DATAPROTECT

WORKING PAPER

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:	General Secretariat of the Council
To:	Delegations
Subject:	Draft Council conclusions on the EU's Cybersecurity Strategy for the Digital Decade - Comments by AT, BG, CZ, DK, EE, FI, FR, DE, HU, IE, IT, LV, LT, MT, NL, RO, ES and SE

Delegations will find in Annex comments by AT, BG, CZ, DK, EE, FI, FR, DE, HU, IE, IT, LV, LT, MT, NL, RO, ES and SE on the above-mentioned subject.

TABLE OF CONTENT

	Page
AUSTRIA	2
BULGARIA	10
CZECH REPUBLIC	11
DENMARK	19
ESTONIA	27
FINLAND	35
FRANCE	44
GERMANY	52
HUNGARY	60
IRELAND	68
ITALY	77
LATVIA	85
LITHUANIA	93
MALTA	101
NETHERLANDS	102
ROMANIA	110
SPAIN	118
SWEDEN	126

ANNEX

AUSTRIA

The Council of the European Union,

RECALLING its conclusions on:

- the Joint Communication to the European Parliament and the Council on the Cybersecurity Strategy for the European Union: "An Open, Safe and Secure Cyberspace",
- on Internet Governance,
- the Joint Communication to the European Parliament and the Council: "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU",
- cybersecurity capability and cyber capacity building in the EU,
- the significance of 5G to the European Economy and the need to mitigate security risks linked to 5G [The 5G cybersecurity Toolbox],
- the future of a highly digitised Europe beyond 2020: "Boosting digital and economic competitiveness across the Union and digital cohesion",
- shaping Europe's Digital Future,
- complementary efforts to enhance resilience and counter hybrid threats,
- strengthening resilience and countering hybrid threats, including countering disinformation in the context of the COVID-19 pandemic,
- Cyber Diplomacy,
- on EU Coordinated Response to Large-Scale Cybersecurity Incidents and Crises
- a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox"),
- EU External Cyber Capacity Building Guidelines,
- the cybersecurity of connected devices,
- and its Council Resolution on Encryption - Security through encryption and security despite encryption.

RECALLING the European Council Conclusions on COVID-19, the Single Market, industry policy, digital and external relations and those on disinformation and hybrid threats,

RECALLING the Global Strategy for the European Union's Foreign and Security Policy,

RECALLING the Communications of the European Commission on shaping Europe's Digital Future and on the EU Security Union Strategy,

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 to protect its people, businesses and institutions from cyber threats while enhancing the trust of citizens and organisations in the EU's ability to promote secure and reliable digital tools and connectivity, and to promote and protect a global, stable, secure, free and open cyberspace, grounded in the rule of law, human rights, fundamental freedoms and democratic values.
2. RECOGNISING that the COVID-19 pandemic has brought trust and security in Information and Communication Technology (ICT) tools and systems to the forefront of our daily lives, stresses that cybersecurity and the global and open Internet are vital for tele-education, social and political participation, the functioning of our public administrations and institutions at both national and EU level, for teleworking, ~~tele-education~~ and doing business online and for society as a whole.
3. CALLS FOR the promotion and protection of the core EU values of democracy, human rights, fundamental freedoms including the freedom of expression, the right to free and equal access to information, the freedom of assembly and association, the right to privacy and the protection against mass surveillance and of the rule of law 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 its efforts to prevent the misuse of emerging technologies, notably through the use of diplomatic measures where necessary, as well as the export control of such technologies.
4. HIGHLIGHTS the importance of strengthening the EU's strategic autonomy, particularly its digital and technological leadership sovereignty in the field of cybersecurity, while preserving an open economy. In this respect, COMMITTS itself to promoting the Union's autonomy on the basis of the development of a dynamic Industrial Strategy that supports EU value chains and secures the supply chains in particular in the most strategic domains, while ensuring that access to the single market is gained on fair and equitable terms and with respect for the Union's values.
5. Bearing in mind the shortage of cybersecurity skills in the workforce, STRESSES the importance of meeting the demand of trained workforce in the field of cybersecurity, in particular by developing, but also by retaining and attracting the best cybersecurity talent, for instance through education and training, and ENCOURAGES women's increased participation in science, technology, engineering, mathematics ('STEM') education and ICT jobs upskilling and reskilling in digital skills.

Commented [A1]: Proposal to include this aspect in order to acknowledge that cybersecurity and the global and open Internet are detrimental for the social and political life of citizens during the COVID-19 pandemic.

Commented [A2]: Austria proposes to align language with the Joint Communication. Technological sovereignty is mentioned a few times.

Commented [A3]: It is not only about attracting the best talents, but assuring the supply of sufficient workforce. This thought could be better reflected in the paragraph.

6. RECALLS that the common and comprehensive EU approach to cyber diplomacy aims to contribute to conflict prevention, the 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 confidence-building measures on the regional and international levels, such as the pioneering Cyber CBMs of the OSCE. REITERATES the United Nations General Assembly's call that UN Member States be guided by the UNGGE reports' recommendations in their use of ICT and notably the application of international law, in particular the UN Charter, in cyberspace. RECALLS that International Humanitarian Law and International Human Rights Law fully apply in cyberspace.

Commented [A4]: In an EU document we could be more ambitious on the application of international law.

7. REAFFIRMS that the further development of standards within the Union is essential and COMMITTS to engage actively in -with a view to- shaping international standards in the areas of emerging technologies and core internet architecture so that these are in line with EU values and-through a multi-stakeholder approach, the further development of standards within the Union is essential: this will ensure that the Internet remains global, stable, secure, free and open and that digital technologies are human-centric, privacy-preserving, and that their use is lawful, safe and ethical. LOOKS FORWARD to the upcoming Standardisation Strategy and COMMITTS itself to proactive and coordinated outreach to promote the EU's objectives at international level, including through cooperation with like-minded partners, civil society and the private sector, and active participation in international technical standard-setting bodies.

Commented [A5]: Previous placement of this phrase would have implied that norms inside EU would automatically ensure a positive outcome at the international level.

Commented [A6]: More background is needed to look forward and commit to the mentioned strategy.

8. STRONGLY SUPPORTS the multi-stakeholder model for Internet governance and commits itself to reinforcing regular and structured exchanges with stakeholders including the private sector, academia and civil society, in particular within the context of the Paris Call and in international fora. PROMOTES universal, affordable and equal access to the Internet and, in particular, the empowerment of persons in vulnerable situations or marginalised groups, in both policy development and in the use of the Internet and SUPPORTS efforts at building the required capacities.

9. EMPHASISES the need to include cybersecurity in all digital-investments in digital technology in the coming years and SUPPORTS the Commission's plan to increase public spending and leverage private investment in the cybersecurity domain, taking into account note of the prospective-possible increase in the number of sectors to which the Directive on measures for a high common level of cybersecurity across the Union (NIS Directive 2.0) will-would apply. HIGHLIGHTS the importance of Small and Medium Sized Enterprises (SMEs) in the cybersecurity ecosystem and RECOGNISES the relevant financial instruments available to support a cybersecurity digital transformation over the 2021-2027 Multiannual Financial Framework (MFF) as well as in the Recovery and Resilience Facility.

Commented [A7]: Unclear formulation.

Commented [A8]: As a matter of principle, Austria would like to avoid prejudging outcomes of ongoing negotiations.

10. LOOKS FORWARD to the ~~rapid~~ implementation of the Regulation on Cybersecurity Industrial, Technology and Research Competence Centre and Network of Coordination Centres (CCCN) with a view to swiftly allow for targeted and needs-based investments maximising the effects of investments to ~~strengthen enable~~ the Union's leadership in the field of cybersecurity, to support technological capacities and skills and to increase the Union's global competitiveness with input from industry and academic communities in cybersecurity, which should be brought into a more systematic collaboration.

Commented [A9]: The proposal specifies in more detail how effects can be maximised.

11. REITERATES the need to explore the scope of a possible horizontal Union legal act, including for market access, which the Commission may be invited to propose in order to address all relevant aspects of cybersecurity of connected objects and its links with the cybersecurity certification framework under the Cybersecurity Act (CSA), as well as any other product specific instruments, in order to ensure adequate synergies, while avoiding inconsistencies or duplication.

Commented [A10]: Austria supports the inclusion in the CC and is of the opinion that agreed language should be used in this regard (see CC on the cybersecurity of connected devices).

12. ACKNOWLEDGES the importance of a harmonised approach on cybersecurity in the Union, while fully respecting Member States' competences, and WELCOMES the new proposal for a Directive on measures for a high common level of cybersecurity across the Union (NIS Directive 2.0) that builds upon the NIS Directive as an evolution of the efforts undertaken and which has contributed to strengthening and harmonising national cybersecurity frameworks and promoted cooperation between Member States. Furthermore, RECOGNISES that the NIS Directive sets the reference framework for the need for close alignment with other sectorial legislation in this domain.

Commented [A11]: Sectorial legislation should align with the NIS directive, not the other way around.

13. TAKES NOTE of the Commission's proposal to support Member States in strengthening their national Security Operation Centres (SOCs) and to build a network of SOCs across the EU, to detect signals of attacks on networks and enable responses before harm is done. LOOKS FORWARD to exploring this network's potential to strengthen SOCs as well as their complementarity and coordination with existing networks and actors (for instance CSIRTs Network, ENISA and CERT-EU), including within the scope of the EU's cyber crisis management framework, in order to promote an efficient, secure and reliable information-sharing culture. Within this process, the best use should be made of the work carried out in the context of Artificial Intelligence and High Performance Computing initiatives and by European Digital Innovation Hubs, as well as the entire electronic communications infrastructure such as land and submarine network systems.

14. TAKES NOTE of the planned implementation possible development of an the ultra-secure connectivity system, building on the Euro quantum communication infrastructure (QCI), building on existing telecommunication infrastructures and new Space components including and EUGOVSAATCOM, and COMMENDS that it be based on a robust cybersecurity framework.

Commented [A12]: With the aim of a quantum computing system, QCI is the only system which will make ultra-secure communication available in this context.

The proposed changes in the paragraph should reflect a more forward looking implementation of projects in the pilot phase in this regard.

15. 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 its operators in guaranteeing that the Internet remains globally accessible and non-fragmented. RECOGNISES that an alternative European service for accessing the global internet ("DNS4EU" initiative), based on a transparent model which conforms to the latest security and data protection and privacy by design and by default standards and rules, can contribute to increased resilience.
16. 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 to increase the overall level of security, resilience and openness of the global internet, while increasing the competitiveness of the EU industry and in particular of the internet infrastructure operators.
17. 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 Cybersecurity Strategy and as based on the review 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. URGES Member States to continue 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 its strong commitment to applying the EU 5G Toolbox, including if necessary relevant restrictions on high-risk suppliers for key assets defined as critical and sensitive in the EU coordinated risk assessments and to continuing efforts made to guarantee the cybersecurity of 5G networks.
18. RECOGNISES the relevance of integrating cybersecurity into EU crisis response mechanisms and STRESSES the importance of enhancing cooperation and information-sharing amongst the various cybersecurity communities within the EU and of linking the existing initiatives, structures and procedures (such as the Blueprint, the CSIRT Network, the NIS Cooperation Group, CyCLONe, the European Cybercrime Centre, EU INCEN and the IPCR) in case of large-scale cyber incidents and threats. TAKING INTO ACCOUNT the progress already achieved in this domain, LOOKS FORWARD to the Commission's proposal on the process, milestones and timeline for defining and implementing the Joint Cyber Unit (JCU) with a view to providing added value and streamlining the EU cybersecurity crisis management framework, including through preparedness, shared situational awareness, coordinated response and exercises, in a transparent and incremental manner while avoiding duplication and overlap and respecting the competences of the Member States.

Commented [A13]: The present text implies that "relevant restrictions" are already mandatory to implement. Even if a manufacturer is considered a "high-risk supplier", there must be room for flexibility and proportionality.

Commented [A14]: This inclusion gives merit to the mentioning of Blueprint which is neither a structure nor a procedure.

Commented [A15]: CC should not prejudge the outcome of the proposals mentioned.

19. As highlighted by the impact of the COVID-19 pandemic, STRESSES the importance of promoting cooperation and exchange between cybersecurity actors and law enforcement and judicial authorities and the need to expand and improve the capacity of these authorities to investigate cybercrime, while fully respecting fundamental rights and striving to ensure the requisite balance between various rights and interests, in particular privacy and security.
20. 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 citizens, governments, industry and society and, at the same time, the need to ensure the ability of the competent law enforcement and judicial authorities to exercise their lawful powers, both online and offline, to protect our societies and citizens.
21. CONTINUES to support and promote the Budapest Convention on Cybercrime, and the ongoing work on the Second Additional Protocol to that Convention. ~~Furthermore, will~~COMMITTS to continue to engage in multilateral exchanges on cybercrime, including the intergovernmental Expert Group to Conduct a Comprehensive Study on Cybercrime as well as the Ad Hoc Committee to elaborate a comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes to ensure an enhanced international cooperation to counter cybercrime, while the respect of respecting, promoting and protecting human rights and fundamental freedoms.
22. 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 INCEN's work, including by exploring the establishment of an EU Cyber Intelligence Working Group.
23. HIGHLIGHTS the importance of a robust and consistent security framework to better protect all EU personnel, data, information, communication networks 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 classified and non-classified EU networks while ensuring that sufficient resources are available. WELCOMES, in this context, the ongoing interinstitutional discussions on the establishment of common rules on information security and cybersecurity for all EU institutions, bodies, offices and agencies.
24. BUILDING ON the EU's cyber diplomacy efforts, COMMITTS itself to increasing the effectiveness and the efficiency of the EU Cyber Diplomacy Toolbox and LOOKS FORWARD to deepening discussions building on lessons learned from the application of this instrument to date. These discussions should aim at building a notion of shared security at international level by strengthening prevention, cooperation and advancing confidence and capacity building and, where necessary, impose restrictions, thereby contributing to the EU's security and integrity and consolidating the EU's cyber posture, in full respect of national competences and prerogatives. In particular, special attention should be given to countering cyberattacks affecting our critical infrastructure, democratic institutions and processes, as well as to countering cyberattacks on supply chain-attacks with systemic effects and cyber-enabled theft of intellectual property.

25. In order to contribute to a global, secure, stable, free and open 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, contributing to the respect for international law in cyberspace and adherence to the norms, rules and principles of responsible state behaviour in cyberspace, especially for instance 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 outcome of both the current UN GGE and OEWG processes.
26. RECALLS its strong commitment to multilateralism aimed at strengthening cooperation and coordination with international and regional organisations, namely the United Nations, the Council of Europe, the OSCE, the OECD, NATO, 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 the UN Secretary General's Roadmap on digital cooperation. WELCOMES the establishment of 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 EU delegations and MS embassies on international cyber issues in order to strengthen coordinated outreach.
27. ACKNOWLEDGES the importance of strengthening cooperation with international partners, including with NATO, in order to advance the shared understanding of the cyber threat landscape, to develop cooperation mechanisms, to identify, where appropriate, cooperative diplomatic responses as well as to improve information-sharing, including through education, training and exercises. In particular, REAFFIRMS that a strong transatlantic partnership is vital to ensure and to contribute to our common security, stability and prosperity.
28. LOOK 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 security, crisis management and defence agenda, for instance 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 on setting up the Military CERT-Network by the European Defence Agency (EDA) and SUPPORTS efforts made to enhance synergies and coordination between the cybersecurity civilian, defence and space spheres, including through the dedicated PESCO projects.

Commented [A16]: After the announcement by the Chair, input might be given in PMG.

29. TAKES NOTE of the development of an EU External Cyber Capacity Building Agenda and the creation of an EU Cyber Capacity Building Board in order to increase cyber resilience and capacities worldwide. In this context, ENCOURAGES cooperation with Member States, as well as with public and private sector partners 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 Neighbourhood.

30. 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 partners 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.

31. WELCOMES the ~~comprehensive~~ proposals presented in the Cybersecurity Strategy and ~~ACKNOWLEDGES that all of the initiatives presented therein are important. In order to ensure their seamless implementation, and~~ taking into account the multiannual character of some of these, CONSIDERS it is necessary to set the priorities with an accompanying and detailed implementation plan.

Commented [A17]: With the adoption of these Council Conclusions the Council articulates its priorities in regard to the Joint Communication. This paragraph should not prejudice discussions.

32. MONITORS the progress in the implementation of these Conclusions by the means of an Action Plan to be adopted by the Council by The action plan would be regularly reviewed and updated by the Council in cooperation with the European Commission and the High Representative.

Commented [A18]: The Action plan up to date proved to be a useful tool and should be continued in the same manner.

BULGARIA

11. REITERATES the need to explore the scope of a possible horizontal Union legal act, ~~including for market access~~ specifying the necessary conditions for the placement on the market, which the Commission may be invited to propose in order to address all relevant aspects of cybersecurity of connected objects and its links with the cybersecurity certification framework under the Cybersecurity Act (CSA), as well as any other product specific instruments, in order to ensure adequate synergies, while avoiding inconsistencies or duplication.

The reason for this proposal is to align with the agreed language in Council Conclusions on the cybersecurity of the connected devices (13629/20), paragraph 7.

CZECH REPUBLIC

ANNEX

The Council of the European Union,

RECALLING its ~~e~~CConclusions on:

- the Joint Communication to the European Parliament and the Council on the Cybersecurity Strategy for the European Union: "An Open, Safe and Secure Cyberspace",
- on Internet Governance,
- the Joint Communication to the European Parliament and the Council: "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU",
- cybersecurity capability and cyber capacity building in the EU,
 - the significance of 5G to the European Economy and the need to mitigate security risks linked to 5G [The 5G cybersecurity Toolbox],
- the future of a highly digitised Europe beyond 2020: "Boosting digital and economic competitiveness across the Union and digital cohesion",
- shaping Europe's Digital Future,
- complementary efforts to enhance resilience and counter hybrid threats,
- strengthening resilience and countering hybrid threats, including countering disinformation in the context of the COVID-19 pandemic,
- Cyber Diplomacy,
- on EU Coordinated Response to Large-Scale Cybersecurity Incidents and Crises
- a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox"),
- EU External Cyber Capacity Building Guidelines,
- the cybersecurity of connected devices,
- and its Council Resolution on Encryption - Security through encryption and security despite encryption.

RECALLING the European Council Conclusions on COVID-19, the Single Market, industry policy, digital and external relations and those on disinformation and hybrid threats,

RECALLING the Global Strategy for the European Union's Foreign and Security Policy,

RECALLING the Communications of the European Commission on shaping Europe's Digital Future and on the EU Security Union Strategy,

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 to protect its people, businesses and institutions from cyber threats while enhancing the trust of citizens and organisations in the EU's ability to promote secure and reliable digital tools and connectivity, and to promote and protect a global, stable, secure, free and open cyberspace, grounded in the rule of law, human rights, fundamental freedoms and democratic values.
2. RECOGNISING that the COVID-19 pandemic has brought trust and security in Information and Communication Technology (ICT) tools and systems to the forefront of our daily lives, ~~stresses~~ **STRESSES** that cybersecurity and the global and open Internet are vital for the functioning of our public administrations and institutions at both national and EU level, for teleworking, tele-education and doing business online and for society as a whole.
3. CALLS FOR the promotion and protection of the core EU values of democracy, human rights, fundamental freedoms including the freedom of expression, the right to free and equal access to information, the freedom of assembly and association, the right to privacy and the protection against mass surveillance and of the rule of law 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 its efforts to prevent the misuse of emerging technologies, notably through the use of diplomatic measures where necessary, as well as the export control of such technologies.
4. HIGHLIGHTS the importance of strengthening the EU's strategic autonomy, particularly its digital and technological leadership in the field of cybersecurity, while preserving an open economy. In this respect, COMMITTS itself to promoting the Union's autonomy on the basis of the development of a dynamic Industrial Strategy that supports EU value chains and secures the supply chains in particular in the most strategic domains, while ensuring that access to the single market is gained on fair and equitable terms and with respect for the Union's values.
5. Bearing in mind the shortage of cybersecurity skills in the workforce, STRESSES the importance of developing, retaining and attracting the best cybersecurity talent, for instance through education and training, and ENCOURAGES women's increased participation in science, technology, engineering, mathematics ('STEM') education and ICT jobs upskilling and reskilling in digital skills.

Commented [A19]: We agree with the current wording to the strategic autonomy. In this respect, it is necessary to fully take into consideration the Council Conclusions on Climate and Energy Diplomacy (from 25/01/2021) whose text reflects the intensive discussion before their approval.

6. RECALLS that the common and comprehensive EU approach to cyber diplomacy aims to contribute to conflict prevention, the mitigation of cybersecurity threats and greater stability in international relations. In this context, REAFFIRMS its commitment to the settlement of international disputes arising from ICT activities 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. REITERATES the United Nations General Assembly's ~~call~~ agreement by consensus that UN Member States should be guided by the UNGGE reports' recommendations in their use of ICT and notably the application of international law, in particular the UN Charter, in cyberspace.

Commented [A20]: We recommend to use rather this formulation, which, in our opinion, better reflects commonly used language as the term "*international dispute in cyberspace*" is not used in current relevant agreed wordings. Disputes do not take place between states "in cyberspace" but in real space as a result of the activities of states in cyberspace.

7. REAFFIRMS that, with a view to shaping international standards in the areas of emerging technologies and core internet architecture so that these are in line with EU values and a multi-stakeholder approach, the further development of standards within the Union is essential: this will ensure that the Internet remains global, stable, secure, free and open and that digital technologies are human-centric, privacy-preserving, and that their use is lawful, safe and ethical. LOOKS FORWARD to the upcoming Standardisation Strategy and COMMITS itself to proactive and coordinated outreach to promote the EU's objectives at international level, including through cooperation with like-minded partners, civil society and the private sector.

Commented [A21]: The fact that those norms were agreed unanimously should be emphasized.

Commented [A22]: We welcome this reference and it is important for us to preserve it in the final text

Commented [A23]: We would recommend to broaden this statement, if possible (e.g. with any indication of expected views what this Strategy should bring or of expected further Council's action in this regard).

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

9. EMPHASISES the need to include cybersecurity in all digital investments in the coming years and SUPPORTS the Commission's plan to increase public spending and leverage private investment in the cybersecurity domain, taking into account the prospective increase in the number of sectors to which the Directive on measures for a high common level of cybersecurity across the Union (NIS Directive 2.0) will apply. HIGHLIGHTS the importance of Small and Medium Sized Enterprises (SMEs) in the cybersecurity ecosystem and RECOGNISES the relevant financial instruments available to support a cybersecurity digital transformation over the 2021-2027 Multiannual Financial Framework (MFF) as well as in the Recovery and Resilience Facility.

Commented [A24]: As the outcome of the legislative process is anticipated here, we would prefer to use more careful language in this regard and recommend adding something like: "*Without prejudice to the outcome of the (future) legislative process....*"

10. LOOKS FORWARD to the rapid implementation of the Regulation on Cybersecurity Industrial, Technology and Research Competence Centre and Network of Coordination Centres (CCCN) with a view to maximising the effects of investments to strengthen the Union's leadership in the field of cybersecurity, to support technological capacities and skills and to increase the Union's global competitiveness with input from industry and academic communities in cybersecurity, which should be brought into a more systematic collaboration.

11. REITERATES the importance of assessing the need to explore the scope of a possible horizontal Union legal act, including conditions for the placement on for-market access, which the Commission may be invited to propose in order to address all relevant aspects of cybersecurity of connected objects-devices and its links with the cybersecurity certification framework under the Cybersecurity Act (CSA), as well as any other product specific instruments, in order to ensure adequate synergies, while avoiding inconsistencies or duplication.

Commented [A25]: We recommend to stick to the agreed language from the Council Conclusions on the cybersecurity of connected devices

12. ACKNOWLEDGES the importance of a harmonised approach on cybersecurity in the Union, while fully respecting Member States' competences, and WELCOMES the new proposal for a Directive on measures for a high common level of cybersecurity across the Union (NIS Directive 2.0) that builds upon the NIS Directive as an evolution of the efforts undertaken and which has-should contributed to strengthening and harmonising national cybersecurity frameworks and promoted cooperation between Member States. Furthermore, RECOGNISES-EMPHASISES the need for close alignment with -other sectorial legislation in this domain.

Commented [A26]: We understand that this is linked to NIS 2.0.

Commented [A27]: This is an extremely important aspect from our point of view in order to ensure coherence

13. TAKES NOTE of the Commission's proposal to support Member States in establishing new and strengthening -their existing national Security Operation Centres (SOCs) and to build a network of SOCs across the EU, to detect signals of attacks on networks and enable responses before harm is done. LOOKS FORWARD to exploring this network's potential to strengthen SOCs as well as their complementarity and coordination with existing networks and actors (for instance CSIRTs Network, ENISA and CERT-EU), including within the scope of the EU's cyber crisis management framework, in order to promote an efficient, secure and reliable information-sharing culture. Within this process, the best use should be made of the work carried out by in the context of Artificial Intelligence and High Performance Computing initiatives and by European Digital Innovation Hubs, as well as the entire electronic communications infrastructure such as space, land and submarine network systems, should be made.

Commented [A28]: From our point of view, the support in establishing new national SOCs is very desirable and welcomed and therefore it should be included as well

Commented [A29]: Or another formulation, like: "COMMENDS the work carried out by AI, HPC initiatives and EDIH..., which should be best used", etc.

14. TAKES NOTE of the possible development of an ultra-secure connectivity system, building on the Euro quantum communication infrastructure (QCI) and EUGOVSATCOM, and COMMENDS that it should be based on a robust cybersecurity framework.

15. 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 its operators in guaranteeing that the Internet remains globally accessible and non-fragmented. RECOGNISES that an alternative European service for accessing the global internet (“DNS4EU” initiative), based on a transparent model which conforms to the latest security, ~~and~~ data protection and privacy by design and by default standards and rules, can contribute to increased resilience.

16. 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, ~~and~~ openness ~~and interoperability~~ of the global internet, while increasing the competitiveness of the EU industry and in particular of the internet infrastructure operators.

Commented [A30]: Or “instruments to increase”

Commented [A31]: The emphasis on the interoperability is an important aspect for us because it counteracts the efforts to build an alternative internet infrastructure and to close some countries

17. 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 Cybersecurity Strategy and as based on the review 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. ~~URGES-STRONGLY ENCOURAGES~~ Member States to continue 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 its strong commitment to applying the EU 5G Toolbox, including relevant restrictions on high-risk suppliers for key assets defined as critical and sensitive in the EU coordinated risk assessments and to continuing efforts made to guarantee the cybersecurity of 5G networks.

18. RECOGNISES the relevance of integrating cybersecurity into EU crisis response mechanisms and STRESSES the importance of enhancing cooperation and information-sharing amongst the various cybersecurity communities within the EU and of linking the existing structures and procedures (such as the Blueprint, the CSIRT Network, the NIS Cooperation Group, CyCLONe, the European Cybercrime Centre, EU INCEN and the IPCR) in case of large-scale cyber incidents and threats. TAKING INTO ACCOUNT the progress already achieved in this domain, LOOKS FORWARD to the Commission’s proposal on the process, milestones and timeline for ~~defining and implementing-deploying~~ the Joint Cyber Unit (JCU) with a view to providing added value 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.

Commented [A32]: The Strategy itself states: “defining, preparing, deploying and expanding”

19. As highlighted by the impact of the COVID-19 pandemic, STRESSES the importance of promoting cooperation and exchange between cybersecurity actors and law enforcement and judicial authorities and the need to expand and improve the capacity of these authorities to investigate cybercrime, while fully respecting fundamental rights and striving to ensure the requisite balance between various rights and interests, in particular privacy and security.

20. 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 citizens, governments, industry and society and, at the same time, the need to ensure the ability of the competent law enforcement and judicial authorities to exercise their lawful powers, both online and offline, to protect our societies and citizens. EMPHASISES that any actions taken have to balance these interests carefully against the principles of necessity, proportionality and subsidiarity

Commented [A33]: This is an important aspect stated in the referred Council resolution, that should be mentioned and emphasised.

21. CONTINUES to support and promote the Budapest Convention on Cybercrime, and the ongoing work on the Second Additional Protocol to that Convention. Furthermore, will continue to engage in multilateral exchanges on cybercrime to ensure the respect of human rights and fundamental freedoms.

22. 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 INCEN's work, including by exploring the establishment of an EU Cyber Intelligence Working Group.

23. HIGHLIGHTS the importance of a robust and consistent security framework to better protect all EU personnel, data, ~~information~~, 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 classified and non-classified EU networks while ensuring that sufficient resources are available. WELCOMES, in this context, the ongoing interinstitutional discussions on the establishment of common rules on information security and cybersecurity for all EU institutions, bodies, offices and agencies.

24. BUILDING ON the EU's cyber diplomacy efforts, COMMITTS itself to increasing the effectiveness and the efficiency of the ~~EU~~-Cyber Diplomacy Toolbox and LOOKS FORWARD to deepening discussions building on lessons learned from the application of this instrument to date. These discussions should aim at building a notion of shared security at international level by strengthening prevention, stability, cooperation and advancing confidence and capacity building and, where necessary, impose restrictions, thereby contributing to the EU's security and integrity and consolidating the EU's cyber posture, in full respect of national competences and prerogatives. In particular, special attention should be given to countering cyberattacks affecting our critical infrastructure, essential services, democratic institutions and processes, as well as to countering cyberattacks on supply chain-attacks with systemic effects and cyber-enabled theft of intellectual property.

Commented [A34]: We suggest to add "stability" to cover all the categories of the measures from the Cyber Diplomacy Toolbox

25. In order to contribute to a global, secure, stable, free and open 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, contributing to the respect for international law in cyberspace and adherence to the norms, rules and principles of responsible state behaviour in cyberspace, for instance 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 outcome of both the current UN GGE and OEWG processes.

26. RECALLS its strong commitment to multilateralism aimed at strengthening cooperation and coordination with international and regional organisations, namely the United Nations, the Council of Europe, the OSCE, the OECD, NATO, 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 the UN Secretary General's Roadmap on digital cooperation. WELCOMES the establishment of 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 EU delegations and its Member States embassies on international cyber issues in order to strengthen coordinated outreach.

Commented [A35]: We recommend to formulate this in a more general way which in our opinion better reflects the purpose of the Network.

27. ACKNOWLEDGES the importance of strengthening cooperation with international partners, including with NATO, in order to advance the shared understanding of the cyber threat landscape, to develop cooperation mechanisms, to identify, where appropriate, cooperative diplomatic responses as well as to improve information-sharing, including through education, training and exercises. In particular, REAFFIRMS that a strong transatlantic partnership is vital to ensure and to contribute to our common security, stability and prosperity.

28. LOOK 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 security, crisis management and defence agenda, for instance 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 on setting up the Military CERT-Network by the European Defence Agency (EDA) and SUPPORTS efforts made to enhance synergies and coordination between the cybersecurity civilian, defence and space spheres, including through the dedicated PESCO projects.

29. TAKES NOTE of the development of an EU External Cyber Capacity Building Agenda and the creation of an EU Cyber Capacity Building Board in order to increase cyber resilience and capacities worldwide. In this context, ENCOURAGES cooperation with Member States, as well as with public and private sector partners 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 Neighbourhood.
30. 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 partners 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.
31. WELCOMES the comprehensive proposals presented in the Cybersecurity Strategy and ACKNOWLEDGES that all of the initiatives presented therein are important. In order to ensure their seamless implementation, and taking into account the multiannual character of some of these, CONSIDERS it is necessary to set the priorities with an accompanying and detailed implementation plan.
32. MONITORS the progress in the implementation of these Conclusions by the means of an Action Plan to be adopted by the Council by The action plan would be regularly reviewed and updated by the Council in cooperation with the European Commission and the High Representative.

Commented [A36]: As it was discussed during the HWPCI, we generally suggest to make a clearer distinction between the implementation plan and the Action plan and to take into consideration also the roles of other relevant actors (and their adequate cooperation with the Council) throughout all the initiatives mentioned in this whole draft.

The solution for the latter could be to add something like following paragraph (taken from the 2017 Council Conclusions) to the text:

[The Council]
INVITES the Member States, the EU institutions, agencies and bodies to work together, respecting each other's' areas of competence and the principle of subsidiarity and proportionality, in response to the strategic objectives set out in these Conclusions.

DENMARK

The Council of the European Union,

RECALLING its conclusions on:

- the Joint Communication to the European Parliament and the Council on the Cybersecurity Strategy for the European Union: "An Open, Safe and Secure Cyberspace",
- on Internet Governance,
- the Joint Communication to the European Parliament and the Council: "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU",
- cybersecurity capability and cyber capacity building in the EU,
 - the significance of 5G to the European Economy and the need to mitigate security risks linked to 5G [The 5G cybersecurity Toolbox],
- the future of a highly digitised Europe beyond 2020: "Boosting digital and economic competitiveness across the Union and digital cohesion",
- shaping Europe's Digital Future,
- complementary efforts to enhance resilience and counter hybrid threats,
- strengthening resilience and countering hybrid threats, including countering disinformation in the context of the COVID-19 pandemic,
- Cyber Diplomacy,
- on EU Coordinated Response to Large-Scale Cybersecurity Incidents and Crises
- a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox"),
- EU External Cyber Capacity Building Guidelines,
- the cybersecurity of connected devices,
- and its Council Resolution on Encryption - Security through encryption and security despite encryption.

RECALLING the European Council Conclusions on COVID-19, the Single Market, industry policy, digital and external relations and those on disinformation and hybrid threats,

RECALLING the Global Strategy for the European Union's Foreign and Security Policy,

RECALLING the Communications of the European Commission on shaping Europe's Digital Future and on the EU Security Union Strategy,

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 to protect its people, businesses and institutions from cyber threats while enhancing the trust of citizens and organisations in the EU's ability to promote secure and reliable digital tools and connectivity, and to promote and protect a global, stable, secure, free and open cyberspace, grounded in the rule of law, human rights, fundamental freedoms and democratic values.
2. RECOGNISING that the COVID-19 pandemic has brought trust and security in Information and Communication Technology (ICT) tools and systems to the forefront of our daily lives, stresses that cybersecurity and the global and open Internet are vital for the functioning of our democratic public administrations and institutions at both national and EU level, for teleworking, tele-education and doing business online and for society as a whole.
3. CALLS FOR the promotion and protection of the core EU values of democracy, human rights, fundamental freedoms including the freedom of expression, the right to free and equal access to information, the freedom of assembly and association, the right to privacy and the protection against mass surveillance and of the rule of law 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 its efforts to prevent the misuse of emerging technologies, notably through the use of diplomatic measures where necessary, as well as the export control of such technologies.
4. HIGHLIGHTS the importance of strengthening the EU's strategic autonomy, particularly its digital and technological leadership in the field of cybersecurity, while preserving an open economy. In this respect, COMMITS itself to promoting the Union's autonomy on the basis of strengthening the Single market and the development of a dynamic Industrial Strategy that supports EU value chains and underpins development of capacities critical for the society~~secures the supply chains in particular in the most strategic domains~~, while ensuring that access to the single market is gained on fair and equitable terms and with respect for the Union's values.
5. Bearing in mind the shortage of cybersecurity skills in the workforce, STRESSES the strategic importance of developing, retaining and attracting the best cybersecurity talent, for instance through education and training, and ENCOURAGES women's increased participation in science, technology, engineering, mathematics ('STEM') education and ICT jobs upskilling and reskilling in digital skills.

Commented [A37]: Here, we would like to emphasize the single market's role in the creation of strategic autonomy (as its conditions set the stage for the leadership in the field of cyber security).

6. RECALLS that the common and comprehensive EU approach to cyber diplomacy aims to contribute to conflict prevention, the 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 relevant 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. REITERATES the United Nations General Assembly's call that UN Member States be guided by the UNGGE reports' recommendations in their use of ICT and notably the application of international law, in particular the UN Charter, in cyberspace.
7. REAFFIRMS that, with a view to shaping international standards in the areas of emerging technologies and core internet architecture so that these are in line with EU values and a multi-stakeholder approach, the further development of standards within the Union is essential: this will ensure that the Internet remains global, stable, secure, free and open and that digital technologies are human-centric, privacy-preserving, and that their use is lawful, safe and ethical. ~~LOOKS FORWARD to~~ ANTICIPATES the upcoming Standardisation Strategy and COMMITTS itself to proactive and coordinated outreach to promote the EU's objectives at international level, including through cooperation with like-minded partners, civil society and the private sector.
8. STRONGLY SUPPORTS the multi-stakeholder model for Internet governance and commits itself to reinforcing regular and structured exchanges with stakeholders including the private sector, academia and civil society, in particular within the context of the Paris Call and in international fora. PROMOTES universal, affordable and equal access to the Internet and, in particular, the empowerment of persons in vulnerable situations or marginalised groups, in both policy development and in the use of the Internet.
9. EMPHASISES the need to include cybersecurity in ~~all~~ digital investments in the coming years and SUPPORTS the Commission's plan to increase focus on the cybersecurity domain ~~in~~ public spending and leverage private investment in ~~the cybersecurity domain~~, taking into account the prospective increase in the number of sectors to which the Directive on measures for a high common level of cybersecurity across the Union (NIS Directive 2.0) will apply. HIGHLIGHTS the importance of Small and Medium Sized Enterprises (SMEs) in the cybersecurity ecosystem and RECOGNISES the relevant financial instruments available to support a cybersecurity digital transformation over the 2021-2027 Multiannual Financial Framework (MFF) as well as in the Recovery and Resilience Facility.

Commented [A38]: We would prefer to delete "all" - again cybersecurity should be a general focus point, but not impose demands on digital investments where cyber security might not be completely intertwined with the nature of the project.

10. LOOKS FORWARD to the ~~rapid~~ implementation of the Regulation on Cybersecurity Industrial, Technology and Research Competence Centre and Network of Coordination Centres (CCCN) with a view to maximising the effects of investments to strengthen the Union's leadership in the field of cybersecurity, to support technological capacities and skills and to increase the Union's global competitiveness with input from industry and academic communities in cybersecurity, which should be brought into a more systematic collaboration.
11. REITERATES the need to explore the scope of a possible horizontal Union legal act, including for market access, which the Commission may be invited to propose in order to address all relevant aspects of cybersecurity of connected objects and its links with the cybersecurity certification framework under the Cybersecurity Act (CSA), as well as any other product specific instruments, in order to ensure adequate synergies, while avoiding inconsistencies or duplication.
12. ACKNOWLEDGES the importance of a harmonised approach on cybersecurity in the Union, while fully respecting Member States' competences, and WELCOMES the new proposal for a Directive on measures for a high common level of cybersecurity across the Union (NIS Directive 2.0) that builds upon the NIS Directive as an evolution of the efforts undertaken and which has contributed to strengthening and harmonising national cybersecurity frameworks and promoted cooperation between Member States. Furthermore, RECOGNISES the need for close alignment with other sectorial legislation in this domain.
13. TAKES NOTE of the Commission's proposal to support Member States while fully respecting Member States' competences within security, in strengthening their national Security Operation Centres (SOCs) and to build a network of SOCs across the EU, to detect signals of attacks on networks and enable responses before harm is done. LOOKS FORWARD to exploring this network's potential to strengthen SOCs as well as their complementarity and coordination with existing networks and actors (for instance CSIRTs Network, ENISA and CERT-EU), including within the scope of the EU's cyber crisis management framework, in order to promote an efficient, secure and reliable information-sharing culture. ANTICIPATES the Commission's description on exactly how such a network of SOCs, which shall be shielding the EU, will be brought into realization. It is important that such a network of SOCs will bring added value. In this regard, the Council welcomes an investigation into whether regional instances of such a network of SOCs network should be based on sector, in lieu of geography. Within this process, the best use should be made of the work carried out in the context of Artificial Intelligence and High Performance Computing initiatives and by European Digital Innovation Hubs, as well as the entire electronic communications infrastructure such as land and submarine network systems.
14. TAKES NOTE of the possible development of an ultra-secure connectivity system, building on the Euro quantum communication infrastructure (QCI) and EUGOVSATCOM, and COMMENDS that it be based on a robust cybersecurity framework.

15. 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 its operators in guaranteeing that the Internet remains globally accessible and non-fragmented. RECOGNISES that an alternative European service for accessing the global internet (“DNS4EU” initiative), based on a transparent model which conforms to the latest security and data protection and privacy by design and by default standards and rules, can contribute to increased resilience.
16. 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 to increase the overall level of security, resilience and openness of the global internet, while increasing the competitiveness of the EU industry and in particular of the internet infrastructure operators.
17. 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 Cybersecurity Strategy and as based on the review 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. URGES Member States to continue 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 its strong commitment to applying the EU 5G Toolbox, including relevant restrictions on high-risk suppliers for key assets defined as critical and sensitive in the EU coordinated risk assessments and to continuing efforts made to guarantee the cybersecurity of 5G networks.
18. ~~RECOGNISES~~ ~~STRESSES~~ the relevance of integrating cybersecurity into EU crisis response mechanisms and ~~STRESSES~~ ~~RECOGNISES~~ the importance of enhancing cooperation and information-sharing amongst the various cybersecurity communities within the EU and of linking the existing structures and procedures (such as the Blueprint, the CSIRT Network, the NIS Cooperation Group, CyCLONe, the European Cybercrime Centre, EU INCEN and the IPCR) in case of large-scale cyber incidents and threats. TAKING INTO ACCOUNT the progress already achieved in this domain, LOOKS FORWARD to the Commission’s proposal on the process, milestones and timeline for defining and implementing the Joint Cyber Unit (JCU) with a view to providing added value and streamlining the EU cybersecurity crisis management framework, including through preparedness, shared situational awareness, coordinated response and exercises, in a transparent and incremental manner while avoiding duplication and overlap and respecting the competences of the Member States.

Commented [A39]: Important wording

Commented [A40]: Important wording

19. As highlighted by the impact of the COVID-19 pandemic, STRESSES the importance of promoting cooperation and exchange between cybersecurity actors and law enforcement and judicial authorities and the need to expand and improve the capacity of these authorities to investigate cybercrime, while fully respecting fundamental rights and striving to ensure the requisite balance between various rights and interests, in particular privacy and security.
20. 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 citizens, governments, industry and society and, at the same time, the need to ensure the ability of the competent law enforcement and judicial authorities to exercise their lawful powers, both online and offline, to protect our societies and citizens.
21. CONTINUES to support and promote the Budapest Convention on Cybercrime, and the ongoing work on the Second Additional Protocol to that Convention. Furthermore, will continue to engage in multilateral exchanges on cybercrime to ensure the respect of human rights and fundamental freedoms.
22. 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, ~~including by exploring the establishment of an EU Cyber Intelligence Working Group.~~
23. HIGHLIGHTS the importance of a robust and consistent security framework to better protect all EU personnel, data, information, communication networks 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 classified and non-classified EU networks while ensuring that sufficient resources are available. WELCOMES, in this context, the ongoing interinstitutional discussions on the establishment of common rules on information security and cybersecurity for all EU institutions, bodies, offices and agencies.
24. BUILDING ON the EU's cyber diplomacy efforts, COMMITTS itself to increasing the effectiveness and the efficiency of the EU Cyber Diplomacy Toolbox and LOOKS FORWARD to deepening discussions building on lessons learned from the application of this instrument to date. These discussions should aim at building a notion of shared security at European and international level by strengthening prevention, cooperation and advancing confidence and capacity building and, ~~where—when~~ necessary, ~~impose restrictions, expediently move to approve restrictive measures thereby imposing cost, and thereby~~ contributing to the EU's security and integrity and consolidating the EU's forward-looking cyber posture, in full respect of national competences and prerogatives. In particular, special attention should be given to countering cyberattacks affecting our critical infrastructure, democratic institutions and processes, as well as to countering cyberattacks on supply chain-attacks with systemic effects and cyber-enabled theft of intellectual property.

Commented [A41]: Please write explicitly if the "lessons learned" are more than just oral discussions in the form of e.g. a report

25. In order to contribute to a global, secure, stable, free and open 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, contributing to the respect for international law in cyberspace and adherence to the norms, rules and principles of responsible state behaviour in cyberspace, for instance 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 outcome of both the current UN GGE and OEWG processes.
26. RECALLS its strong commitment to multilateralism aimed at strengthening cooperation and coordination with international and regional organisations, namely the United Nations, the Council of Europe, the OSCE, the OECD, NATO, 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 the UN Secretary General's Roadmap on digital cooperation. WELCOMES the establishment of 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 EU delegations and MS embassies on international cyber issues in order to strengthen coordinated outreach.
27. ACKNOWLEDGES the importance of strengthening cooperation with international partners, including with NATO, in order to advance the shared understanding of the cyber threat landscape, to develop cooperation mechanisms, to identify, where appropriate, cooperative diplomatic responses as well as to improve information-sharing, including through education, training and exercises. In particular, REAFFIRMS that a strong transatlantic partnership is vital to ensure and to contribute to our common security, stability and prosperity.
28. LOOK 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 security, crisis management and defence agenda, for instance 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 on setting up the Military CERT-Network by the European Defence Agency (EDA) and SUPPORTS efforts made to enhance synergies and coordination between the cybersecurity civilian, defence and space spheres, including through the dedicated PESCO projects.

29. TAKES NOTE of the development of an EU External Cyber Capacity Building Agenda and the creation of an EU Cyber Capacity Building Board in order to increase cyber resilience and capacities worldwide. In this context, ENCOURAGES cooperation with Member States, as well as with public and private sector partners 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 Neighbourhood.

30. To ensure that all likeminded countries are able to reap the social, economic and political benefits of the Internet and the use of technologies, COMMITS itself to assisting partners 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.

31. WELCOMES the comprehensive proposals presented in the Cybersecurity Strategy and ACKNOWLEDGES that all of the initiatives presented therein are important. In order to ensure their seamless implementation, and taking into account the multiannual character of some of these, CONSIDERS it is necessary to set the priorities ~~with, therefore~~ ENCOURAGES an accompanying and detailed implementation plan.

32. MONITORS the progress in the implementation of these Conclusions by the means of an Action Plan to be adopted by the Council by The action plan would be regularly reviewed and updated by the Council in cooperation with the European Commission and the High Representative.

ESTONIA

The Council of the European Union,

RECALLING its conclusions on:

- the Joint Communication to the European Parliament and the Council on the Cybersecurity Strategy for the European Union: "An Open, Safe and Secure Cyberspace",
- on Internet Governance,
- the Joint Communication to the European Parliament and the Council: "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU",
- cybersecurity capability and cyber capacity building in the EU,
 - the significance of 5G to the European Economy and the need to mitigate security risks linked to 5G [The 5G cybersecurity Toolbox],
- the future of a highly digitised Europe beyond 2020: "Boosting digital and economic competitiveness across the Union and digital cohesion",
- shaping Europe's Digital Future,
- complementary efforts to enhance resilience and counter hybrid threats,
- strengthening resilience and countering hybrid threats, including countering disinformation in the context of the COVID-19 pandemic,
- Cyber Diplomacy,
- on EU Coordinated Response to Large-Scale Cybersecurity Incidents and Crises
- a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox"),
- EU External Cyber Capacity Building Guidelines,
- the cybersecurity of connected devices,
- and its Council Resolution on Encryption - Security through encryption and security despite encryption.

RECALLING the European Council Conclusions on COVID-19, the Single Market, industry policy, digital and external relations and those on disinformation and hybrid threats,

RECALLING the Global Strategy for the European Union's Foreign and Security Policy,

RECALLING the Communications of the European Commission on shaping Europe's Digital Future and on the EU Security Union Strategy,

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 to protect its people, businesses and institutions from cyber threats while enhancing the trust of citizens and organisations in the EU's ability to promote secure and reliable digital tools and connectivity, and to promote and protect a global, stable, secure, free and open cyberspace, grounded in the rule of law, human rights, fundamental freedoms and democratic values.
2. RECOGNISING that the COVID-19 pandemic has brought trust and security in Information and Communication Technology (ICT) tools and systems to the forefront of our daily lives, stresses that cybersecurity and the global and open Internet are vital for the functioning of our public administrations and institutions at both national and EU level, for teleworking, tele-education and doing business online and for society as a whole.
3. CALLS FOR the promotion and protection of the core EU values of democracy, human rights, fundamental freedoms including the freedom of expression, the right to free and equal access to information, the freedom of assembly and association, the right to privacy and the protection against mass surveillance and of the rule of law 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 its efforts to prevent the misuse of emerging technologies, notably through the use of diplomatic measures where necessary, as well as the export control of such technologies.
4. HIGHLIGHTS the importance of strengthening the EU's ~~strategic autonomy, particularly its~~ digital and technological leadership in the field of cybersecurity, while preserving an open economy. In this respect, COMMITS itself to promoting the Union's autonomy on the basis of the development of a dynamic Industrial Strategy that supports EU value chains and secures the supply chains in particular in the most strategic domains, while ensuring that access to the single market is gained on fair and equitable terms and with respect for the Union's values.
5. Bearing in mind the shortage of cybersecurity skills in the workforce, STRESSES the importance of developing, retaining and attracting the best cybersecurity talent, for instance through education and training and allocating necessary funds for this, and ENCOURAGES women's increased participation in science, technology, engineering, mathematics ('STEM') education and ICT jobs, upskilling and reskilling in digital skills.

Commented [A42]: In addition to awareness raising being a crucial pillar of cyber security, the need for cyber awareness is prominently mentioned in the strategy and should be referenced in the conclusions as well We suggest adding here additional paragraph 2a

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

Commented [A43]: Considering that this effort requires resources

6. RECALLS that the common and comprehensive EU approach to cyber diplomacy aims to contribute to conflict prevention, the 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. REITERATES the United Nations General Assembly's call that UN Member States be guided by the UNGGE reports' recommendations in their use of ICT and notably the application of international law, in particular the UN Charter, in cyberspace.
7. REAFFIRMS that, with a view to shaping international standards in the areas of emerging technologies and core internet architecture so that these are in line with EU values and a multi-stakeholder approach, the further development of standards within the Union is essential: this will ensure that the Internet remains global, stable, secure, free and open and that digital technologies are human-centric, privacy-preserving, and that their use is lawful, safe and ethical. LOOKS FORWARD to the upcoming Standardisation Strategy and COMMITS itself to proactive and coordinated outreach to promote the EU's objectives at international level, including through cooperation with like-minded partners, civil society and the private sector.
8. STRONGLY SUPPORTS the multi-stakeholder model for Internet governance and commits itself to reinforcing regular and structured exchanges with stakeholders including the private sector, academia and civil society, in particular within the context of the Paris Call and in international fora. PROMOTES universal, affordable and equal access to the Internet and, in particular, the empowerment of persons in vulnerable situations or marginalised groups, in both policy development and in the use of the Internet.
9. EMPHASISES the need to include cybersecurity in all digital investments in the coming years and SUPPORTS the Commission's plan to increase public spending and leverage private investment in the cybersecurity domain, taking into account the prospective increase in the number of sectors to which the Directive on measures for a high common level of cybersecurity across the Union (NIS Directive 2.0) will apply. 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.

Commented [A44]: We suggest adding here a new paragraph 7a

ENCOURAGES the wide-scale use of digital identity and secure authentication solutions, which would increase the security of digital environments. Member States and stakeholders should cooperate on this matter and exchange best practices and solutions.

Commented [A45]: Stronger wording

10. LOOKS FORWARD to the rapid implementation of the Regulation on Cybersecurity Industrial, Technology and Research Competence Centre and Network of Coordination Centres (CCCN) with a view to maximising the effects of investments to strengthen the Union's leadership in the field of cybersecurity, to support technological capacities and skills and to increase the Union's global competitiveness with input from industry and academic communities in cybersecurity, which should be brought into a more systematic collaboration.

11. REITERATES the need to explore the scope of a possible horizontal Union legal act, including for market access, which the Commission may be invited to propose in order to address all relevant aspects of cybersecurity of connected objects and its links with the cybersecurity certification framework under the Cybersecurity Act (CSA), as well as any other product specific instruments, in order to ensure adequate synergies, while avoiding inconsistencies or duplication.

12. ACKNOWLEDGES the importance of a harmonised approach on cybersecurity in the Union, while fully respecting Member States' competences, and WELCOMES the new proposal for a Directive on measures for a high common level of cybersecurity across the Union (NIS Directive 2.0) that builds upon the NIS Directive as an evolution of the efforts undertaken and which has contributed to strengthening and harmonising national cybersecurity frameworks and promoted cooperation between Member States. Furthermore, RECOGNISES the need for close alignment with other sectorial legislation in this domain and seek its further potential to foster innovation and competitiveness within the single market.

13. TAKES NOTE of the Commission's proposal to support Member States in strengthening their national Security Operation Centres (SOCs) and to build a network of SOCs across the EU, to detect signals of attacks on networks and enable responses before harm is done. LOOKS FORWARD to exploring this network's potential to strengthen SOCs as well as their complementarity and coordination with existing networks and actors (for instance CSIRTs Network, ENISA and CERT-EU), including within the scope of the EU's cyber crisis management framework, in order to promote an efficient, secure and reliable information-sharing culture. Within this process, the best use should be made of the work carried out in the context of Artificial Intelligence and High Performance Computing initiatives and by European Digital Innovation Hubs, as well as the entire electronic communications infrastructure such as land and submarine network systems.

14. TAKES NOTE of the possible development of an ultra-secure connectivity system, building on the Euro quantum communication infrastructure (QCI) and EUGOVSATCOM, and COMMENDS that it be based on a robust cybersecurity framework.

Commented [A46]: We should discover ways NIS 2.0 could allow us to break down market barriers inside the EU. The new directive should be a tool to further harmonise cyber security standards for products and services across the union.

15. 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 its operators in guaranteeing that the Internet remains globally accessible and non-fragmented. RECOGNISES that an alternative European service for accessing the global internet (“DNS4EU” initiative), based on a transparent model which conforms to the latest security and data protection and privacy by design and by default standards and rules, can contribute to increased resilience.

16. 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 to increase the overall level of security, resilience and openness of the global internet, while increasing the competitiveness of the EU industry and in particular of the internet infrastructure operators.

17. 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 and other new generation networks, as presented in the appendix to the Cybersecurity Strategy and as based on the review 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. URGES Member States to continue 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 its strong commitment to applying the EU 5G Toolbox, including relevant restrictions on high-risk suppliers for key assets defined as critical and sensitive in the EU coordinated risk assessments and to continuing efforts made to guarantee the cybersecurity of 5G networks.

Commented [A47]: Thinking ahead to ensure readiness for any new technological developments

18. RECOGNISES the relevance of integrating cybersecurity into EU crisis response mechanisms and testing these in relevant exercises and STRESSES the importance of enhancing cooperation and information-sharing amongst the various cybersecurity communities within the EU and of linking the existing structures and procedures (such as the Blueprint, the CSIRT Network, the NIS Cooperation Group, CyCLONE, the European Cybercrime Centre, EU INCEN and the IPCR) in case of large-scale cyber incidents and threats. TAKING INTO ACCOUNT the progress already achieved in this domain, LOOKS FORWARD to INVITES the Commission’s proposal on the process, milestones and timeline for defining and implementing – to analyse whether the creation of a Joint Cyber Unit (JCU) should be proposed with a view to providing significant added value and streamlining the EU cybersecurity crisis management framework, including through preparedness, shared situational awareness, coordinated response and exercises, in a transparent and incremental manner while avoiding duplication and overlap and respecting the competences of the Member States.

Commented [A48]: These crisis response mechanisms need to be tested and validated.

Commented [A49]: It would be too early to look forward to the JCU proposal, clear vision regarding the added value is needed beforehand.

19. ~~As highlighted by the impact of the COVID-19 pandemic,~~ STRESSES the importance of promoting cooperation and exchange between cybersecurity actors and law enforcement and judicial authorities and the need to expand and improve the capacity and resources of these authorities to investigate cybercrime, while fully respecting fundamental rights and striving to ensure the requisite balance between various rights and interests, in particular privacy and security.

Commented [A50]: We suggest adding an additional paragraph 19a here:

HIGHLIGHTS the need to provide relevant cybersecurity authorities and networks both at Member State and EU level sufficient resources and EU funding for effective performance of their tasks, including those related to mutual assistance and cooperation with other authorities and networks.

20. 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 citizens, governments, industry and society while committing to and, at the same time, the need to ensure the ability of the competent law enforcement and judicial authorities to exercise their lawful powers, both online and offline, to protect our societies and citizens.

Commented [A51]: Stronger wording

21. CONTINUES to support and promote the Budapest Convention on Cybercrime as the only binding international instrument on the issue of cybercrime, acknowledging it for also ensuring protection of human rights and liberties, and supporting the ongoing work on the Second Additional Protocol to that Convention. Furthermore, will continue to engage in multilateral exchanges on cybercrime to ensure the respect of human rights and fundamental freedoms.

Commented [A52]: We also ask you to consider moving the second part to a separate paragraph. These two issues – encryption and fight against cybercrime – do not always need to be mentioned in the same paragraph (see also recital 54 of NIS 2.0). This creates an atmosphere where we are constantly fighting for the right to maintain our current encryption standards.

22. 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 INCEN's work, including by exploring the establishment of an EU Cyber Intelligence Working Group.

23. HIGHLIGHTS the importance of a robust and consistent security framework to better protect all EU personnel, data, information, communication networks 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 classified and non-classified EU networks while ensuring that sufficient resources and capabilities are available. WELCOMES, in this context, the ongoing interinstitutional discussions on the establishment of common rules on information security and cybersecurity for all EU institutions, bodies, offices and agencies.

Commented [A53]: Hereby referring to the need to have the necessary classified networks primarily, which EU-I are struggling with.

24. BUILDING ON the EU's cyber diplomacy efforts, COMMITTS itself to increasing the effectiveness and the efficiency of the EU Cyber Diplomacy Toolbox and LOOKS FORWARD to deepening discussions building on lessons learned from the application of this instrument to date. These discussions should aim at building a notion of shared security at international level by strengthening prevention, cooperation and advancing confidence and capacity building and, where necessary, impose restrictions, thereby contributing to the EU's security and integrity and consolidating the EU's cyber posture, in full respect of national competences and prerogatives. In particular, special attention should be given to countering cyberattacks affecting our critical infrastructure, democratic institutions and processes, as well as to countering cyberattacks on supply chain-attacks with systemic effects and cyber-enabled theft of intellectual property.

25. In order to contribute to a global, secure, stable, free and open 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, contributing to the respect for international law in cyberspace and adherence to the norms, rules and principles of responsible state behaviour in cyberspace, for instance 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 outcome of both the current UN GGE and OEWG processes.
26. RECALLS its strong commitment to multilateralism aimed at strengthening cooperation and coordination with international and regional organisations, namely the United Nations, the Council of Europe, the OSCE, the OECD, NATO, 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 the UN Secretary General's Roadmap on digital cooperation. WELCOMES the establishment of 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 EU delegations and MS embassies on international cyber issues in order to strengthen coordinated outreach.
27. ACKNOWLEDGES the importance of strengthening cooperation with international partners, including with NATO, in order to advance the shared understanding of the cyber threat landscape, to develop cooperation mechanisms, to identify, where appropriate, cooperative diplomatic responses as well as to improve information-sharing, including through education, training and exercises. In particular, REAFFIRMS that a strong transatlantic partnership is vital to ensure and to contribute to our common security, stability and prosperity.
28. LOOK 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 security, crisis management and defence agenda, for instance 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 on setting up the Military CERT-Network by the European Defence Agency (EDA) and SUPPORTS efforts made to enhance synergies and coordination between the cybersecurity civilian, defence and space spheres, including through the dedicated PESCO projects.

Commented [A54]: We support this. Since it will be removed from this paragraph we see the need to stress it then in p28 or elsewhere.

29. TAKES NOTE of the development of an EU External Cyber Capacity Building Agenda and the creation of an EU Cyber Capacity Building Board and the establishment of the EU Cyber Capacity Building Network (EU CyberNet) in order to increase cyber resilience and capacities worldwide. In this context, ENCOURAGES cooperation with Member States, as well as with public and private sector partners 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 Neighbourhood.

Commented [A55]: Just like the yet to be created EU Cyber Capacity Building Board, the already present EU CyberNet is a crucial actor in this context and should thus be mentioned in the conclusions as well. Both are present in the strategy and should be reflected here.

Commented [A56]: Strong support

30. 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 partners 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.

31. WELCOMES the comprehensive proposals presented in the Cybersecurity Strategy and ACKNOWLEDGES that all of the initiatives presented therein are important. In order to ensure their seamless implementation, and taking into account the multiannual character of some of these, CONSIDERS it is necessary to set the priorities with an accompanying and detailed implementation plan.

32. MONITORS the progress in the implementation of these Conclusions by the means of an Action Plan to be adopted by the Council by The action plan would be regularly reviewed and updated by the Council in cooperation with the European Commission and the High Representative.

FINLAND

The Council of the European Union,

RECALLING its conclusions on:

- the Joint Communication to the European Parliament and the Council on the Cybersecurity Strategy for the European Union: "An Open, Safe and Secure Cyberspace",
- on Internet Governance,
- the Joint Communication to the European Parliament and the Council: "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU",
- cybersecurity capability and cyber capacity building in the EU,
 - the significance of 5G to the European Economy and the need to mitigate security risks linked to 5G [The 5G cybersecurity Toolbox],
- the future of a highly digitised Europe beyond 2020: "Boosting digital and economic competitiveness across the Union and digital cohesion",
- shaping Europe's Digital Future,
- complementary efforts to enhance resilience and counter hybrid threats,
- strengthening resilience and countering hybrid threats, including countering disinformation in the context of the COVID-19 pandemic,
- Cyber Diplomacy,
- on EU Coordinated Response to Large-Scale Cybersecurity Incidents and Crises
- a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox"),
- EU External Cyber Capacity Building Guidelines,
- the cybersecurity of connected devices,
- and its Council Resolution on Encryption - Security through encryption and security despite encryption.

RECALLING the European Council Conclusions on COVID-19, the Single Market, industry policy, digital and external relations and those on disinformation and hybrid threats,

RECALLING the Global Strategy for the European Union's Foreign and Security Policy,

RECALLING the Communications of the European Commission on shaping Europe's Digital Future and on the EU Security Union Strategy,

RECALLING the joint Communication of the European Commission and the High Representative on a new EU-US agenda for global change.

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 to protect its people, businesses and institutions from cyber threats while enhancing the trust of citizens and organisations in the EU's ability to promote secure and reliable digital tools and connectivity, and to promote and protect a global, stable, secure, free and open cyberspace, grounded in the rule of law, human rights, fundamental freedoms and democratic values.
2. RECOGNISING that the COVID-19 pandemic has brought trust and security in Information and Communication Technology (ICT) tools and systems to the forefront of our daily lives, stresses that cybersecurity and the global and open Internet are vital for the functioning of our public administrations and institutions at both national and EU level, for teleworking, tele-education and doing business online and for society as a whole.
3. CALLS FOR the promotion and protection of the core EU values of democracy, human rights, fundamental freedoms including the freedom of expression, the right to free and equal access to information, the freedom of assembly and association, the right to privacy and the protection against mass surveillance and of the rule of law 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 its efforts to prevent the misuse of emerging technologies, notably through the use of diplomatic measures where necessary, as well as the export control of such technologies.
4. HIGHLIGHTS the importance of strengthening the EU's strategic autonomy, particularly its digital and technological leadership in the field of cybersecurity, while preserving an open economy. In this respect, EMPHASISES the importance of enhanced cooperation with key likeminded partners and COMMITTS itself to promoting the Union's autonomy on the basis of the development of a dynamic Industrial Strategy that supports EU value chains and secures the supply chains in particular in the most strategic domains, while ensuring that access to the single market is gained on fair and equitable terms and with respect for the Union's values.
5. Bearing in mind the shortage of cybersecurity skills in the workforce, STRESSES the importance of developing, retaining and attracting the best cybersecurity talent, for instance through education and training, and ENCOURAGES ensuring all women's and girls' increased full and equal participation in science, technology, engineering, mathematics ('STEM') education and ICT jobs upskilling and reskilling in digital skills.

Commented [A57]: Enhanced cooperation with key likeminded partners necessary to strengthen and consolidate EU's leadership and strategic autonomy.

Commented [A58]: Must be more ambitious. Encourage is too weak.

6. RECALLS that the common and comprehensive EU approach to cyber diplomacy aims to contribute to conflict prevention, the 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. REITERATES the United Nations General Assembly's call that UN Member States be guided by the UNGGE reports' recommendations in their use of ICT and notably the application of international law, in particular the UN Charter, in cyberspace.

7. REAFFIRMS that, with a view to shaping and taking the global lead in setting international norms and standards in the areas of emerging and disruptive technologies and core internet architecture so that these are in line with EU values and a multi-stakeholder approach, the further development of standards within the Union is essential: this will ensure that the Internet remains global, stable, secure, free and open and that digital technologies are human-centric, privacy-preserving, and that their use is lawful, safe and ethical. EMPHASISES the importance of creating regulative frameworks and standards that others will use, follow and adhere to, and RECOGNISES that transatlantic cooperation and cooperation with other likeminded partners and European tech companies –is key to make this happen. LOOKS FORWARD to the upcoming Standardisation Strategy and COMMITTS itself to proactive and coordinated outreach to promote the EU's objectives at international level, including in various international standardisation bodies such as the ITU and through cooperation with like-minded partners, civil society and the private sector.

Commented [A59]: Should be more ambitious. Our goal should be to become global leader on norms, standards and regulation.

Commented [A60]: Very important to emphasise the need and ambition to widen the scope and create frameworks and standards that others will follow, and that close coordination and cooperation with the US, other likeminded key partners and European tech companies is necessary to make this happen. To become global leaders we must develop standards that others will follow.

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

9. EMPHASISES the need to include cybersecurity in all digital investments in the coming years and SUPPORTS the Commission's plan to increase public spending and leverage private investment in the cybersecurity domain, taking into account the prospective increase in the number of sectors to which the Directive on measures for a high common level of cybersecurity across the Union (NIS Directive 2.0) will apply. HIGHLIGHTS the importance of Small and Medium Sized Enterprises (SMEs) in the cybersecurity ecosystem and RECOGNISES the relevant financial instruments available to support a cybersecurity digital transformation over the 2021-2027 Multiannual Financial Framework (MFF) as well as in the Recovery and Resilience Facility.

10. LOOKS FORWARD to the rapid implementation of the Regulation on Cybersecurity Industrial, Technology and Research Competence Centre and Network of Coordination Centres (CCCN) with a view to maximising the effects of investments to strengthen the Union's leadership in the field of cybersecurity, to support technological capacities and skills and to increase the Union's global competitiveness with input from industry and academic communities in cybersecurity, which should be brought into a more systematic collaboration.
11. REITERATES the need to explore the scope of a possible horizontal Union legal act, including for market access, which the Commission may be invited to propose in order to address all relevant aspects of cybersecurity of connected objects and its links with the cybersecurity certification framework under the Cybersecurity Act (CSA), as well as any other product specific instruments, in order to ensure adequate synergies, while avoiding inconsistencies or duplication.
12. ACKNOWLEDGES the importance of a harmonised approach on cybersecurity in the Union, while fully respecting Member States' competences, and WELCOMES the new proposal for a Directive on measures for a high common level of cybersecurity across the Union (NIS Directive 2.0) that builds upon the NIS Directive as an evolution of the efforts undertaken and which has contributed to strengthening and harmonising national cybersecurity frameworks ~~and in response to a need to share information and further enhance cooperation between competent authorities and promoted cross-border-cooperation between Member States at technical, operational and political level.~~ Furthermore, RECOGNISES the need for close alignment with other sectorial legislation in this domain.
13. TAKES NOTE of the Commission's proposal to support Member States in strengthening their national Security Operation Centres (SOCs) and to build a network of SOCs across the EU, to detect signals of attacks on networks and enable responses before harm is done. LOOKS FORWARD to exploring this network's potential to strengthen SOCs as well as their complementarity and coordination with existing networks and actors (for instance CSIRTs Network, ENISA and CERT-EU), including within the scope of the EU's cyber crisis management framework, in order to promote an efficient, secure and reliable information-sharing culture. Within this process, the best use should be made of the work carried out in the context of Artificial Intelligence and High Performance Computing initiatives and by European Digital Innovation Hubs, as well as the entire electronic communications infrastructure such as land and submarine network systems.
14. TAKES NOTE of the possible development of an ultra-secure connectivity system, building on the Euro quantum communication infrastructure (QCI) and EUGOVSATCOM, and COMMENDS that it be based on a robust cybersecurity framework.

Commented [A61]: New Article 11 of the NIS proposal should increase the level of cooperation also between the competent authorities at national level, including the law enforcement.

It should be highlighted that the directive also encourages essential and important entities, on the basis of applicable criminal proceedings rules in compliance with Union law, to report incidents of a suspected serious criminal nature to the relevant law enforcement authorities.

Formatted: Font: (Default) Times New Roman, 12 pt

15. 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 its operators in guaranteeing that the Internet remains globally accessible and non-fragmented. RECOGNISES that an alternative European service for accessing the global internet ("DNS4EU" initiative), based on a transparent model which conforms to the latest security and data protection and privacy by design and by default standards and rules, can contribute to increased resilience.

16. 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 to increase the overall level of security, resilience and openness of the global internet, while increasing the competitiveness of the EU industry and in particular of the internet infrastructure operators.

17. 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: without undermining the ability of law enforcement national security and judicial authorities to maintain and preserve efficient lawful interception capabilities in 5G networks.

18. SUPPORTS the next steps to be taken on the cybersecurity of 5G networks, as presented in the appendix to the Cybersecurity Strategy and as based on the review 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. URGES Member States, EU institutions and other relevant stakeholders for a swift and effective implementation of the EU 5G Toolbox, as envisaged in the new cyber security strategy, 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 its strong commitment to applying and further building on the work of the EU 5G Toolbox, including relevant restrictions on high-risk suppliers for key assets defined as critical and sensitive in the EU coordinated risk assessments and to continuing efforts made to guarantee the cybersecurity of 5G networks. The close cooperation between Member States and the Commission on 5G cybersecurity should serve as an example for other issues in the field of cybersecurity.

19. RECOGNISES the relevance of integrating cybersecurity into EU crisis response mechanisms and STRESSES the importance of enhancing cooperation and information-sharing amongst the various cybersecurity communities within the EU and of linking the existing structures and procedures (such as the Blueprint, the CSIRT Network, the NIS Cooperation Group, CyCLONe, the European Cybercrime Centre, EU INCEN and the IPCR) in case of large-scale cyber incidents and threats. TAKING INTO ACCOUNT the progress already achieved in this domain, LOOKS FORWARD to the Commission's proposal on the process, milestones and timeline for defining and implementing the Joint Cyber Unit (JCU) with a view to providing added value and streamlining the EU cybersecurity crisis management framework, including through preparedness, shared situational awareness, coordinated response and exercises, in a transparent and incremental

Commented [A62]: Law enforcement and other actors protecting public and national security have to cope with higher security standards and encryption incorporated into 5G networks in their daily work to protect the citizens from adversaries benefiting from that same level of security. Therefore, it is essential to ensure the ability of law enforcement and judicial authorities to maintain and preserve efficient lawful interception capabilities in 5G networks.

Commented [A63]: Important to use are good experiences of the 5G Toolbox to advance other cyber issues.

manner while avoiding duplication and overlap and respecting the competences of the Member States.

~~19-20.~~ As highlighted by the impact of the COVID-19 pandemic, STRESSES the importance of promoting cooperation and information exchange between cybersecurity actors, both public and private and law enforcement and judicial authorities and the need to expand and improve the capacity of these authorities to detect, prevent investigate cybercrime, and other cyber-enabled and cyber-dependent crime, and thus ensure the identification and prosecution of offenders, while fully respecting fundamental rights and striving to ensure the requisite balance between various rights and interests, in particular privacy and security.

~~20-21.~~ 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 citizens, governments, industry and society and, at the same time, 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.

~~21-22.~~ CONTINUES to support and promote the Budapest Convention on Cybercrime, and the ongoing work on the Second Additional Protocol to that Convention. Furthermore, will continue to engage in multilateral exchanges on cybercrime to ensure the respect of human rights and fundamental freedoms.

~~22-23.~~ 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, including by exploring the establishment of an EU Cyber Intelligence Working Group.

~~23-24.~~ HIGHLIGHTS the importance of a robust and consistent security framework to better protect all EU personnel, data, information, communication networks 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 classified and non-classified EU networks while ensuring that sufficient resources are available. WELCOMES, in this context, the ongoing interinstitutional discussions on the establishment of common rules on information security and cybersecurity for all EU institutions, bodies, offices and agencies.

Commented [A64]: Large scale cyber enabled crimes are becoming difficult or impossible to detect, prevent and investigate, causing financial and reputational damage to organisations and individuals. Internet frauds and scams may have a negative impact for the consumer's trust in e-commerce and e-banking and it may slow down the economic growth. Finland supports the view that cybercrime should become a strategic communication priority across the EU, to alert Europeans to the risks and to the preventive measures they could take.

Commented [A65]: Agreed language (Council conclusions on encryption, from last year).

~~24-25.~~ BUILDING ON the EU's cyber diplomacy efforts, COMMITTS itself to increasing the effectiveness and the efficiency of the EU Cyber Diplomacy Toolbox and LOOKS FORWARD to ~~deepening discussions~~strengthening its implementation by and further broadening the scope and the use of the Toolbox building on lessons learned from the application of this instrument to date, as well as taking into account that the ability and willingness of state actors to pursue their geostrategic objectives through the means of malicious cyber activities has continued to increase. These discussions should aim at building a notion of shared security at international level by strengthening prevention, cooperation and advancing confidence and capacity building and, where necessary, impose restrictions, thereby contributing to the EU's security and integrity and consolidating the EU's cyber posture, in full respect of national competences and prerogatives. In particular, special attention should be given to countering cyberattacks affecting our critical infrastructure, democratic institutions and processes, including disinformation campaigns, as well as to countering ~~cyberattacks on~~ supply chain-attacks ~~with systemic effects~~ and cyber-enabled theft of intellectual property.

Commented [A66]: Digital disinformation is clearly on the rise, as seen also during the Covid-19 pandemic. The diplomatic toolbox should ultimately also address hacking based disinformation, where the illegality of the hacking would constitute grounds for the use of the diplomatic toolbox.

~~25-26.~~ In order to contribute to a global, secure, stable, free and open cyberspace, which is of ever-increasing importance for the continued prosperity, growth, security, well-being, connectivity and integrity of our societies, COMMITTS itself to continuous engagement in norm-setting processes in international organisations, especially in the UN first-committee related processes, ~~contributing to the respect for~~ promoting the application of international law in cyberspace and adherence to the norms, rules and principles of responsible state behaviour in cyberspace, for instance 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 outcome of both the current UN GGE and OEWG processes. REAFFIRMS that a universal cyber security framework can only be grounded in existing international law, including the Charter of the United Nations in its entirety, international humanitarian law, and international human rights law.

Commented [A67]: Important to also mention the negotiations in the 3rd Committee, and emphasise the importance of a comprehensive multilateral approach.

Commented [A68]: Agreed language 10786/20.

Commented [A69]: Agreed language 10786/20.

~~26-27.~~ RECALLS its strong commitment to rules-based multilateralism and its determination to aimed at strengthening cooperation and coordination with international and regional organisations, namely the United Nations, the Council of Europe, the OSCE, the OECD, NATO, 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. To step up these efforts CONSIDERS formulating an EU position on the application of international law to the use of ICT technologies by States. STRESSES its active support to the UN, in particular in relation to its Agenda 2030, including the Sustainable Development Goals, and the UN Secretary General's Roadmap on digital cooperation. WELCOMES the establishment of 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 EU delegations and MS embassies on international cyber issues in order to strengthen coordinated outreach.

Commented [A70]: Good!

27-28. ACKNOWLEDGES the importance of strengthening cooperation with international partners, including with NATO, in order to advance the shared understanding of the cyber threat landscape, to develop cooperation mechanisms, to identify, where appropriate, cooperative diplomatic responses as well as to improve information-sharing, including through education, training and exercises. In particular, REAFFIRMS that a strong transatlantic partnership is vital to ensure and to contribute to our common security, stability and prosperity. WELCOMES the chapter on technology, trade and standards in the joint Communication of the European Commission and the High Representative on a new EU-US agenda for global change, and LOOKS FORWARD to its swift operationalisation and implementation.

28-29. LOOK 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 security, crisis management and defence agenda, for instance 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 on setting up the Military CERT-Network by the European Defence Agency (EDA) and SUPPORTS efforts made to enhance synergies and coordination between the cybersecurity civilian, defence and space spheres, including through the dedicated PESCO projects.

29-30. TAKES NOTE of the development of an EU External Cyber Capacity Building Agenda and the creation of an EU Cyber Capacity Building Board in order to increase cyber resilience and capacities worldwide. In this context, ENCOURAGES cooperation with Member States, as well as with public and private sector partners 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 Neighbourhood.

31. 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 partners 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.

30-32. ACKNOWLEDGES the importance of close coordination and cooperation between the European Commission and the European External Action Service to ensure a holistic and intersectoral approach to cybersecurity. COMMENDS the Commission and External Action Service for their close cooperation in developing the Cybersecurity Strategy, and ENCOURAGES them to regularise and consolidate their joint planning and stocktaking on cyber issues.

Commented [A71]: Important to set ambitious and concrete goals for transatlantic cooperation, and elaborate on how the goals will be reached. One way to do that could be to express our support for the proposed steps in the Communication's technology, trade and standards chapter, and to signal our expectation with regards to their swift operationalisation and implementation.

~~31-33.~~_____ WELCOMES the comprehensive proposals presented in the Cybersecurity Strategy and ACKNOWLEDGES that all of the initiatives presented therein are important. In order to ensure their seamless implementation, and taking into account the multiannual character of some of these, **CONSIDERS** it is necessary to set the priorities with an accompanying and detailed implementation plan.

Commented [A72]: Yes! Very important.

~~32-34.~~_____ MONITORS the progress in the implementation of these Conclusions by the means of an Action Plan to be adopted by the Council by The action plan would be regularly reviewed and updated by the Council in cooperation with the European Commission and the High Representative.

FRANCE

ANNEX

The Council of the European Union,

RECALLING its conclusions on:

- the Joint Communication to the European Parliament and the Council on the Cybersecurity Strategy for the European Union: "An Open, Safe and Secure Cyberspace",
- ~~on~~ Internet Governance,
- the Joint Communication to the European Parliament and the Council: "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU",
- cybersecurity capability and cyber capacity building in the EU,
- the significance of 5G to the European Economy and the need to mitigate security risks linked to 5G [The 5G cybersecurity Toolbox],
- the future of a highly digitised Europe beyond 2020: "Boosting digital and economic competitiveness across the Union and digital cohesion",
- shaping Europe's Digital Future,
- complementary efforts to enhance resilience and counter hybrid threats,
- strengthening resilience and countering hybrid threats, including countering disinformation in the context of the COVID-19 pandemic,
- Cyber Diplomacy,
- ~~on~~ EU Coordinated Response to Large-Scale Cybersecurity Incidents and Crises
- a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox"),
- EU External Cyber Capacity Building Guidelines,
- the cybersecurity of connected devices,
- its declaration on building the next generation cloud for business and the public sector in the EU,
- and its Council Resolution on Encryption - Security through encryption and security despite encryption.

RECALLING the European Council Conclusions on COVID-19, the Single Market, industry policy, digital and external relations and those on disinformation and hybrid threats,

RECALLING the Global Strategy for the European Union's Foreign and Security Policy,

RECALLING the Communications of the European Commission on shaping Europe's Digital Future and on the EU Security Union **Strategy**,

Without prejudice to the outcome of the legislative process:

Commented [A73]: You might want to add a reference to European Council conclusions of June 20th 2019 "a new strategic agenda 2019-2024"

2. RECOGNISING that the COVID-19 pandemic has brought trust and security in Information and Communication Technology (ICT) tools and systems to the forefront of our daily lives, stresses that cybersecurity and the global and open Internet are vital for the functioning of our public administrations and institutions at both national and EU level, for teleworking, tele-education and doing business online and for society as a whole.
3. CALLS FOR the promotion and protection of the core EU values of democracy, human rights, fundamental freedoms including the freedom of expression, the right to free and equal access to information, the freedom of assembly and association, the right to privacy and the protection against mass surveillance and of the rule of law 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 its efforts to prevent the misuse of emerging technologies, notably through the use of diplomatic measures where necessary, as well as the export control of such technologies.
4. HIGHLIGHTS the importance of strengthening the EU's strategic autonomy, particularly its digital and technological sovereignty and leadership in the field of cybersecurity, ~~while preserving an open economy~~. In this respect, COMMITTS itself to promoting the Union's autonomy on the basis of the development of a dynamic Industrial Strategy that supports EU value chains and secures the supply chains in particular in the most strategic domains, while ensuring that access to the single market is gained on fair and equitable terms and with respect for the Union's values.
5. Bearing in mind the shortage of cybersecurity skills in the workforce, STRESSES the importance of developing, retaining and attracting the best cybersecurity talent, for instance through education and training, and ENCOURAGES women's increased participation in science, technology, engineering, mathematics ('STEM') education and ICT jobs upskilling and reskilling in digital skills.

Commented [A74]: We would welcome some more assertive introductory remarks covering the resilience aspect set out in the strategy.

It might be relevant to add elements on the growing interconnection of MS's economy and their increased exposure to a wide variety cyber threats and stresses the idea that a better resilience of information systems leads to a stronger development of the Union economic and industrial fabric.

Commented [A75]: This term would deserve clarification.

6. RECALLS that the common and comprehensive EU approach to cyber diplomacy aims to contribute to conflict prevention, the 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. REITERATES the United Nations General Assembly's call that UN Member States be guided by the UNGGE reports' recommendations in their use of ICT and ~~notably~~ REAFFIRMS the full applicability of international law, in particular of the UN Charter, in cyberspace.

Commented [A76]: We fully agree with this substance of this paragraph but wonder whether this should not be paired other paragraphs dealing with EU cyber diplomacy.

12.

6.7 REAFFIRMS that, with a view to shaping international standards in the areas of emerging technologies and core internet architecture so that these are in line with EU values and a multi-stakeholder approach, the further development of standards within the Union is essential: this will ensure that the Internet remains global, stable, secure, free and open and that digital technologies are human-centric, privacy-preserving, and that their use is lawful, safe and ethical. LOOKS FORWARD to the upcoming Standardisation Strategy and COMMITS itself to proactive and coordinated outreach to promote the EU's objectives at international level, including through cooperation with like-minded partners, civil society and the private sector.

Formatted: Indent: Left: 1.14 cm, No bullets or numbering

7.8 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 particular within the context of the Paris Call for Trust and Security in Cyberspace and in international fora.

8.9 PROMOTES universal, affordable and equal access to the Internet and, in particular, the empowerment of persons in vulnerable situations or marginalised groups, in both policy development and in the use of the Internet.

10. EMPHASISES the need to include cybersecurity in all digital investments in the coming years and SUPPORTS the Commission's plan to increase public spending and leverage private investment in the cybersecurity domain, taking into account the prospective increase in the number of sectors to which the Directive on measures for a high common level of cybersecurity across the Union (NIS Directive 2.0) will apply. HIGHLIGHTS the importance of Small and Medium Sized Enterprises (SMEs) in the cybersecurity ecosystem and RECOGNISES the relevant financial instruments available to support a cybersecurity digital transformation over the 2021-2027 Multiannual Financial Framework (MFF) as well as in the Recovery and Resilience Facility.

12. WELCOMES the ongoing work led by ENISA, along with Member States and interested stakeholders, to provide the EU with cybersecurity certification schemes that will eventually contribute to raising the overall level of cybersecurity within the Digital Single Market. STRESSES the pioneering role of the EU to enforce standards that will -shape the cybersecurity landscape thus contributing to its sovereignty. -RECALLS the importance for EU businesses and public sector to be able to maintain control over strategic and sensitive personal and non-personal data when using public cloud infrastructure-. In this STRESSES regard, STRESSES the pivotal role of the EU cybersecurity certification scheme on cloud service providers to establish a mechanism allowing for a verification that no access request to such data can be granted if it comes from a foreign government or if it is not fully compliant with EU legislation and case law.

13. ENCOURAGES the upcoming publication and implementation of the Union Rolling Work Program to identify the priorities on that matter. REITERATES the need to explore the scope of a possible horizontal Union legal act, including for market access, which the Commission may be invited to propose in order to address all relevant aspects of cybersecurity of connected objects and its links with the cybersecurity certification framework under the Cybersecurity Act (CSA), as well as any other product specific instruments, in order to ensure adequate synergies, while avoiding inconsistencies or duplication.

14. ACKNOWLEDGES the importance of a harmonised approach on cybersecurity in the Union, while fully respecting Member States' competences, and WELCOMES the new proposal for a Directive on measures for a high common level of cybersecurity across the Union (NIS Directive 2.0) to further strengthen EU Member States capacities considering the evolution of the cyber threat landscape ; WELCOMES that it builds upon the NIS Directive as an evolution of the efforts undertaken and which has contributed to strengthening and harmonising national cybersecurity frameworks and promoted cooperation between Member States while proposing addressing new stakes by -to- develop completing national and EU crisis management frameworks as well as encompassing the security of digital ecosystems of the entities that are essential to EU economic and societal activities. Furthermore, RECOGNISES STRESSES the need for close alignment and proper articulation with other sectorial legislation in this domain.

15. TAKES NOTE of the Commission's proposal to support Member States in strengthening their national Security Operation Centres (SOCs) and to build a network of SOCs across the EU, to detect-monitor and anticipate signals of attacks on networks-and enable responses before harm is done. LOOKS FORWARD to exploring this network's potential to strengthen SOCs as well as their complementarity and coordination with existing networks-and actors-(for instancesuch as the CSIRTs Network, ENISA and CERT-EU), including within the scope of the EU's cyber crisis management framework, in order to

promote an efficient, secure and reliable information-sharing culture. Within this process, the best use should be made of the work carried out in the context of Artificial Intelligence and High Performance Computing initiatives and by European Digital Innovation Hubs, as well as the entire electronic communications infrastructure such as land and submarine network systems.

~~14-16.~~ TAKES NOTE of the possible development of an ultra-secure connectivity system, building on the Euro quantum communication infrastructure (QCI) and EUGOVSATCOM, and COMMENDS that it be based on a robust cybersecurity framework.

~~15-17.~~ 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 its operators in guaranteeing that the Internet remains globally accessible and non-fragmented. RECOGNISES that an alternative European service for accessing the global internet ("DNS4EU" initiative), based on a transparent model which conforms to the latest security and data protection and privacy by design and by default standards and rules, can contribute to increased resilience.

Commented [A78]: ENISA role herein would need to be clarified / aligned with its mandate

~~16-18.~~ 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 to increase the overall level of security, resilience and openness of the global internet, while increasing the competitiveness of the EU industry and in particular of the internet infrastructure operators.

~~17-19.~~ 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 Cybersecurity Strategy and as based on the review 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. URGES Member States to continue 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 its strong commitment to applying the EU 5G Toolbox, including relevant restrictions on high-risk suppliers for key assets defined as critical and sensitive in the EU coordinated risk assessments and to continuing efforts made to guarantee the cybersecurity of 5G networks.

~~18-20.~~ RECOGNISES the relevance of further integrating cybersecurity into EU crisis response mechanisms and STRESSES the importance of enhancing cooperation and information-sharing amongst the various cybersecurity communities within the EU and of linking the existing structures and procedures (such as the Blueprint, the CSIRT Network, the NIS Cooperation Group, the CyCLONe, the European Cybercrime Centre, EU INCEN and the IPCR) in case of large-scale cyber incidents and threats. TAKING INTO ACCOUNT the progress already achieved in this domain while implementing the Blueprint, going even further than the initial recommendation, LOOKS FORWARD to the Commission's proposal on the process, milestones and timeline for defining and implementing the Joint Cyber Unit (JCU) with a view to providing added value and streamlining the EU cybersecurity crisis management framework, including through preparedness, shared situational awareness, coordinated response and exercises, in a transparent and incremental manner while avoiding duplication and overlap and respecting the competences of the Member States. CALLS FOR the Member States and the EU institutions to initiate discussions and conduct exercises with a view to developing on the solidarity mechanisms and mutual assistance processes in case of major large-scale incidents or attacks, and COMMITTS to ensure the coherence of its responses outside and inside of the Union. HIGHLIGHTS the need to develop a trusted industrial base should the EU be severely impacted by a cyber crisis, notably via the certification of incident response service providers.

~~19-21.~~ As highlighted by the impact of the COVID-19 pandemic, STRESSES the importance of promoting cooperation and exchange between cybersecurity actors and law enforcement and judicial authorities and the need to ~~expand and~~ improve the skills and expertise capacity of these authorities to investigate cybercrime, while fully respecting privacy, fundamental rights and the security of communications, ~~and striving to ensure the requisite balance between various rights and interests, in particular privacy and security.~~

Commented [A79]: We do not see privacy and security as conflicting objectives

~~20-22.~~ 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 citizens, governments, industry and society and, at the same time, the need to ensure the ability of the competent law enforcement and judicial authorities to exercise their lawful powers, both online and offline, to protect our societies and citizens, in full respect of the principles of legality, transparency, necessity and proportionality.

~~21-23.~~ CONTINUES to support and promote the Budapest Convention on Cybercrime, and the ongoing work on the Second Additional Protocol to that Convention. Furthermore, will continue to engage in multilateral exchanges on cybercrime to ensure the respect of human rights and fundamental freedoms.

~~22-24.~~ 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 INCEN's work, including by exploring the establishment of ~~an informal working groups when needed to and EU Cyber Intelligence Working Group~~, foster information exchange.

~~23-25.~~ HIGHLIGHTS the importance of a robust and consistent security framework to better protect all EU personnel, data, information, communication networks 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 are made available, including in the context of the reinforcement of CERT-EU. ~~WELCOMES~~LOOKS FORWARD, in this context, ~~to the ongoing interinstitutional 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 ~~and~~ cybersecurity for all EU institutions, bodies, offices and agencies.

26. BUILDING ON the EU's cyber diplomacy efforts, COMMITTS itself to increasing the effectiveness and the efficiency of the EU Cyber Diplomacy Toolbox and LOOKS FORWARD to deepening discussions building on lessons learned from the application of this instrument to date. These discussions should aim at building a notion of shared security at international level by strengthening prevention, cooperation and advancing confidence and capacity building and, where necessary, impose restrictions, thereby contributing to the EU's security and integrity and consolidating the EU's cyber posture, in full respect of national competences and prerogatives. In particular, special attention should be given to countering cyberattacks affecting our critical infrastructure, democratic institutions and processes, as well as to countering cyberattacks on supply chain ~~attacks~~ with systemic effects and cyber-enabled theft of intellectual property.

~~24-27.~~ In order to contribute to a global, secure, stable, free and open cyberspace, which is of ever-increasing importance for the continued prosperity, growth, security, well-being, connectivity and integrity of our societies, COMMITTS itself to continuous engagement in norm-setting processes in international organisations, especially in the UN first-committee related processes, contributing to the respect for international law in cyberspace and adherence to the norms, rules and principles of responsible state behaviour in cyberspace, for instance 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 outcome of both the current UN GGE and OEWG processes.

~~25-28.~~ RECALLS its strong commitment to multilateralism aimed at strengthening cooperation and coordination with international and regional organisations, namely the United Nations, the Council of Europe, the OSCE, the OECD, NATO, 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 the UN Secretary General's Roadmap on digital cooperation. WELCOMES the establishment of 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 EU delegations and MS embassies on international cyber issues in order to strengthen coordinated outreach.

Formatted: Indent: Left: 1.14 cm, No bullets or numbering

~~26-29.~~ ACKNOWLEDGES the importance of strengthening cooperation with international partners, ~~including with NATO~~, in order to advance the shared understanding of the cyber threat landscape, to develop cooperation mechanisms, to identify, where appropriate, cooperative diplomatic responses as well as to improve information-sharing, including through education, training and exercises. In particular, REAFFIRMS that a strong transatlantic partnership is vital to ensure and to contribute to our common security, stability and prosperity.

30. LOOK 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 security, crisis management and defence agenda, for instance 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 on setting up the Military CERT-Network by the European Defence Agency (EDA) and SUPPORTS efforts made to enhance synergies and coordination between the cybersecurity civilian, defence and space spheres, including through the dedicated PESCO projects.

~~27-31.~~ ~~TAKES NOTE~~ WELCOMES ~~of~~ the development of an EU External Cyber Capacity Building Agenda and the creation of an EU Cyber Capacity Building Board in order to increase cyber resilience and capacities worldwide. In this context, ENCOURAGES cooperation with Member States, as well as with public and private sector partners 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 Neighbourhood.

~~28-32.~~ 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 partners 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. WELCOMES the comprehensive proposals presented in the Cybersecurity Strategy and ACKNOWLEDGES that all of the initiatives presented therein are important. In order to ensure their seamless implementation, and taking into account the multiannual character of some of these, ENCOURAGES the Commission and the High Representative to establish a detailed implementation plan setting the priorities and the schedule of planned actions.

~~13.~~ ~~CONSIDERS it is necessary to set the priorities with an accompanying and detailed implementation plan.~~

~~29-34.~~ These Conclusions will be implemented by the means of an Action Plan to be adopted by the Council before The action plan as a living document would be regularly reviewed and updated by the Council ~~MONITORS the progress in the implementation of these Conclusions by the means of an Action Plan to be adopted by the Council by The action plan would be regularly reviewed and updated by the Council~~ in cooperation with the European Commission and the High Representative.

Formatted: Justified, Space After: 0 pt, Don't add space between paragraphs of the same style, Outline numbered + Level: 1 + Numbering Style: 1, 2, 3, ... + Start at: 1 + Alignment: Left + Aligned at: 0.5 cm + Indent at: 1.14 cm, Don't hyphenate

Formatted: Justified, Indent: Left: 1.14 cm, Space After: 0 pt, Don't add space between paragraphs of the same style

Formatted: Indent: Left: 1.14 cm, No bullets or numbering

GERMANY

The Council of the European Union,

RECALLING its conclusions on:

- the Joint Communication to the European Parliament and the Council on the Cybersecurity Strategy for the European Union: "An Open, Safe and Secure Cyberspace",
- ~~on~~ Internet Governance,
- the Joint Communication to the European Parliament and the Council: "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU",
- cybersecurity capability and cyber capacity building in the EU,
 - the significance of 5G to the European Economy and the need to mitigate security risks linked to 5G [The 5G cybersecurity Toolbox],
- the future of a highly digitised Europe beyond 2020: "Boosting digital and economic competitiveness across the Union and digital cohesion",
- shaping Europe's Digital Future,
- complementary efforts to enhance resilience and counter hybrid threats,
- strengthening resilience and countering hybrid threats, including countering disinformation in the context of the COVID-19 pandemic,
- Cyber Diplomacy,
- ~~on~~ EU Coordinated Response to Large-Scale Cybersecurity Incidents and Crises
- a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox"),
- EU External Cyber Capacity Building Guidelines,
- the cybersecurity of connected devices,
- and its Council Resolution on Encryption - Security through encryption and security despite encryption.

RECALLING the European Council Conclusions on COVID-19, the Single Market, industry policy, digital and external relations and those on disinformation and hybrid threats,

RECALLING the Global Strategy for the European Union's Foreign and Security Policy,

RECALLING the Communications of the European Commission on shaping Europe's Digital Future and on the EU Security Union Strategy,

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 to protect its people, businesses and institutions from cyber threats while enhancing the trust of citizens and organisations in the EU's ability to promote secure and reliable digital tools, infrastructure and connectivity, and to promote and protect an open, free, stable and secure ~~global, stable, secure, free and open~~ cyberspace, grounded in the rule of law, human rights, fundamental freedoms and democratic values.
2. RECOGNISING that the COVID-19 pandemic has brought trust and security in Information and Communication Technology (ICT) tools and systems to the forefront of our daily lives, stresses that cybersecurity and the global and open Internet are vital for the functioning of our public administrations and institutions at both national and EU level, for teleworking, tele-education and doing business online and for society as a whole.
3. CALLS FOR the promotion and protection of the core EU values of democracy, human rights, fundamental freedoms including the freedom of expression, the right to free and equal access to information, the freedom of assembly and association, the right to privacy and the protection against mass surveillance and of the rule of law 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 its efforts to prevent the misuse of emerging technologies, notably through the use of diplomatic measures where necessary, as well as the export control of such technologies.
4. HIGHLIGHTS the importance of strengthening the EU's strategic autonomy, particularly its digital and technological leadership in the field of cybersecurity, while preserving an open economy. In this respect, COMMITTS itself to promoting the Union's autonomy on the basis of the development of a dynamic Industrial Strategy that supports EU value chains and secures the supply chains in particular in the most strategic domains, while ensuring that access to the single market is gained on fair and equitable terms and with respect for the Union's values.
5. Bearing in mind the shortage of cybersecurity skills in the workforce, STRESSES the importance of developing, retaining and attracting the best cybersecurity talent, for instance through education and training, and ENCOURAGES women's increased participation in science, technology, engineering, mathematics ('STEM') education and ICT jobs upskilling and reskilling in digital skills.

Commented [A80]: suggestion

Commented [A81]: Suggest agreed language

6. RECALLS that the common and comprehensive EU approach to cyber diplomacy aims to contribute to conflict prevention, the 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. REITERATES the United Nations General Assembly's call that UN Member States be guided by the UNGGE reports' recommendations in their use of ICT and notably the application of international law, in particular the UN Charter, in cyberspace.
7. REAFFIRMS that, with a view to shaping international standards in the areas of emerging technologies and core internet architecture so that these are in line with EU values and a multi-stakeholder approach, the further development of standards within the Union is essential: this will ensure that the Internet remains global, stable, secure, free and open and that digital technologies are human-centric, privacy-preserving, and that their use is lawful, safe and ethical. LOOKS FORWARD to the upcoming Standardisation Strategy and COMMITS itself to proactive and coordinated outreach to promote the EU's objectives at international level, including through cooperation with like-minded partners, civil society and the private sector.
8. STRONGLY SUPPORTS the multi-stakeholder model for Internet governance and commits itself to reinforcing regular and structured exchanges with stakeholders including the private sector, academia and civil society, in particular within the context of the Paris Call and in international fora. PROMOTES universal, affordable and equal access to the Internet and, in particular, the empowerment of women and girls and persons in vulnerable situations or marginalised groups, in both policy development and in the use of the Internet.
9. EMPHASISES the need to include cybersecurity in all digital investments in the coming years and SUPPORTS the Commission's plan to increase public spending and leverage private investment in the cybersecurity domain, taking into account the prospective increase in the number of sectors to which the Directive on measures for a high common level of cybersecurity across the Union (NIS Directive 2.0) will-aims to apply. HIGHLIGHTS the importance of Small and Medium Sized Enterprises (SMEs) in the cybersecurity ecosystem and RECOGNISES the relevant financial instruments available to support a cybersecurity digital transformation over the 2021-2027 Multiannual Financial Framework (MFF) as well as in the Recovery and Resilience Facility (RRF).

Commented [A82]: NIS-2 negotiations ongoing

10. LOOKS FORWARD to the rapid implementation of the Regulation on the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres (CCCN) with a view to maximising the effects of investments to strengthen the Union's leadership in the field of cybersecurity, to support technological capacities and skills and to increase the Union's global competitiveness with input from industry and academic communities in cybersecurity, which should be brought into a more systematic and strategic collaboration.
11. REITERATES the need ~~to explore the scope~~ of a ~~possible~~ horizontal Union legal act, including for market access, which the Commission may be invited to propose in order to address all relevant aspects of cybersecurity of connected objects and its links with the cybersecurity certification framework under the Cybersecurity Act (CSA), as well as any other product specific instruments, in order to ensure adequate synergies, while avoiding inconsistencies or duplication. SUGGESTS that this horizontal Union legal act foresees primacy over sectorial legislation in order to ensure a high level of consistency when setting common cybersecurity requirements. LOOKS FORWARD to the Union Rolling Work Programme (URWP) that ensures the continuous development of the CSA and its schemes
12. ACKNOWLEDGES the importance of a harmonised approach on cybersecurity in the Union, while FULLY RESPECTING ~~fully respecting~~ Member States' competences, and WELCOMES the new proposal for a Directive on measures for a high common level of cybersecurity across the Union (NIS Directive 2.0) that builds upon the NIS Directive as an evolution of the efforts undertaken and which has contributed to strengthening and harmonising national cybersecurity frameworks and promoted cooperation between Member States. Furthermore, RECOGNISES the need for close alignment with other sectorial legislation in this domain.
13. TAKES NOTE of the Commission's proposal to support Member States in strengthening their national Security Operation Centres (SOCs) and to build a network of SOCs across the EU, to detect signals of attacks on networks and enable responses before harm is done. LOOKS FORWARD to exploring this network's potential to strengthen SOCs as well as their complementarity and coordination with existing networks and actors (for instance CSIRTs Network, ENISA and CERT-EU), including within the scope of the EU's cyber crisis management framework, in order to promote an efficient, secure and reliable information-sharing culture. Within this process, the best use should be made of the work carried out in the context of Artificial Intelligence and High Performance Computing initiatives and by European Digital Innovation Hubs, as well as the entire electronic communications infrastructure such as land and submarine network systems.
14. TAKES NOTE of the possible development of an ultra-secure connectivity system, building on the Euro quantum communication infrastructure (QCI) and EUGOVSATCOM, and COMMENDS that it should be based on a robust cybersecurity framework.

Commented [A83]: link to 23. With a view to the EMA attack – what about detection of cyberattacks by EU institutions?

15. 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 its operators in guaranteeing that the Internet remains globally accessible and non-fragmented. RECOGNISES that an alternative European service for accessing the global internet ("DNS4EU" initiative), based on a transparent model which conforms to the latest security and data protection and privacy by design and by default standards and rules, can contribute to increased resilience.
16. 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 to increase the overall level of security, resilience and openness of the global internet, while increasing the competitiveness of the EU industry and in particular of the internet infrastructure operators.
17. 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 Cybersecurity Strategy and as based on the review 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. URGES Member States to continue 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 its strong commitment to applying the EU 5G Toolbox, including relevant restrictions on high-risk suppliers for key assets defined as critical and sensitive in the EU coordinated risk assessments and to continuing efforts made to guarantee the cybersecurity of 5G networks.
18. RECOGNISES the relevance of integrating cybersecurity into EU crisis response mechanisms and STRESSES the importance of enhancing cooperation and information-sharing amongst the various cybersecurity communities within the EU and of linking the existing structures and procedures (such as the Blueprint, the CSIRT Network, the NIS Cooperation Group, CyCLONe, the European Cybercrime Centre, EU INTCEN and the IPCR) in case of large-scale and cross-border cyber incidents and threats. TAKING INTO ACCOUNT the progress already achieved in this domain, LOOKS FORWARD to the Commission's proposal on the process, milestones and timeline for defining ~~and implementing~~ the Joint Cyber Unit (JCU) with a view to providing added value and streamlining the EU cybersecurity crisis management framework, including through preparedness, shared situational awareness, coordinated response and exercises, in a transparent and incremental manner while avoiding duplication and overlap and respecting the competences of the Member States.

Commented [A84]: Better not to prejudge the outcome

19. As highlighted by the impact of the COVID-19 pandemic, STRESSES the importance of promoting cooperation and exchange between cybersecurity actors and law enforcement and judicial authorities and the need to expand and improve the capacity of these authorities to investigate cybercrime, while fully respecting fundamental rights and striving to ensure the requisite balance between various rights and interests, in particular privacy and security.
20. 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 citizens, governments, industry and society and, at the same time, the need to ensure the ability of the competent law enforcement and judicial authorities to exercise their lawful powers, both online and offline, to protect our societies and citizens.
21. CONTINUES to support and promote the Budapest Convention on Cybercrime, and the ongoing work on the Second Additional Protocol to that Convention. Furthermore, will continue to engage in multilateral exchanges on cybercrime to ensure the respect of human rights and fundamental freedoms.
22. 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 INCEN's work, including by exploring the establishment of an EU Cyber Intelligence Working Group for possible cooperation between the individual member states.
23. HIGHLIGHTS the importance of a robust and consistent security framework to better protect all EU personnel, data, information, communication networks 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 classified and non-classified EU networks while ensuring that sufficient resources are available. WELCOMES, in this context, the ongoing interinstitutional discussions on the establishment of common rules on information security and cybersecurity for all EU institutions, bodies, offices and agencies.
24. BUILDING ON the EU's cyber diplomacy efforts, COMMITTS itself to increasing the effectiveness and the efficiency of the EU Cyber Diplomacy Toolbox and LOOKS FORWARD to deepening discussions building on lessons learned from the application of this instrument to date. These discussions should aim at building a notion of shared security at international level by strengthening prevention, cooperation and advancing confidence and capacity building and, where necessary, impose restrictions, thereby contributing to the EU's security and integrity and consolidating the EU's cyber posture, in full respect of national competences and prerogatives. In particular, special attention should be given to countering cyberattacks affecting our critical infrastructure, democratic institutions and processes, as well as to countering cyberattacks on supply chain-attacks with systemic effects and cyber-enabled theft of intellectual property.

Commented [A85]: this could be a little more detailed. Suggest adding a reference to the new AHC on cybercrime

Commented [A86]: no information yet on concrete set-up. As this is not EU responsibility, the wording has to be open.

Commented [A87]: should be linked to 13. How does the EU and its institutions respond to cyberattacks?

25. In order to contribute to a global, secure, stable, free and open 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, contributing to the respect for international law in cyberspace and adherence to the norms, rules and principles of responsible state behaviour in cyberspace, for instance 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 outcome of both the current UN GGE and OEWG processes.
26. RECALLS its strong commitment to multilateralism aimed at strengthening cooperation and coordination with international and regional organisations, namely the United Nations, the Council of Europe, the OSCE, the OECD, NATO, 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 the UN Secretary General's Roadmap on digital cooperation. WELCOMES the establishment of 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 EU delegations and MS embassies on international cyber issues in order to strengthen coordinated outreach.
27. ACKNOWLEDGES the importance of strengthening cooperation with international partners, including with NATO, in order to advance the shared understanding of the cyber threat landscape, to develop cooperation mechanisms, to identify, where appropriate, cooperative diplomatic responses as well as to improve information-sharing, including through education, training and exercises. In particular, REAFFIRMS that a strong transatlantic partnership is vital to ensure and to contribute to our common security, stability and prosperity.
28. LOOK 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 security, crisis management and defence agenda, for instance 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 on setting up the Military CERT-Network by the European Defence Agency (EDA) and SUPPORTS efforts made to enhance synergies and coordination between the cybersecurity civilian, defence and space spheres, including through the dedicated PESCO projects.

29. TAKES NOTE of the development of an EU External Cyber Capacity Building Agenda, ~~and~~ the creation of an EU Cyber Capacity Building Board and the establishment of EU CyberNet (EU's Cyber Capacity Building Network) in order to increase cyber resilience and capacities worldwide. In this context, ENCOURAGES cooperation with Member States, as well as with public and private sector partners 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 Neighbourhood.

30. UNDERLINES the need of sharing of good practices on the promotion and protection of fundamental rights in cyberspace with all relevant stakeholders, and to do the same concerning the use and export of technologies that could be misused for surveillance or censorship purposes and in general concerning dual-use technologies.

~~30-31.~~ 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 partners 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.

~~31-32.~~ WELCOMES the comprehensive proposals presented in the EU's Cybersecurity Strategy ~~and ACKNOWLEDGES that all of the initiatives presented therein are important.~~ In order to ensure their seamless implementation, and taking into account the multiannual character of some of these, CONSIDERS it is necessary to set the priorities with an accompanying and detailed implementation plan.

~~32-33.~~ MONITORS the progress in the implementation of these Conclusions by the means of an Action Plan to be adopted by the Council by The action plan would be regularly reviewed and updated by the Council in cooperation with the European Commission and the High Representative.

HUNGARY

The Council of the European Union,

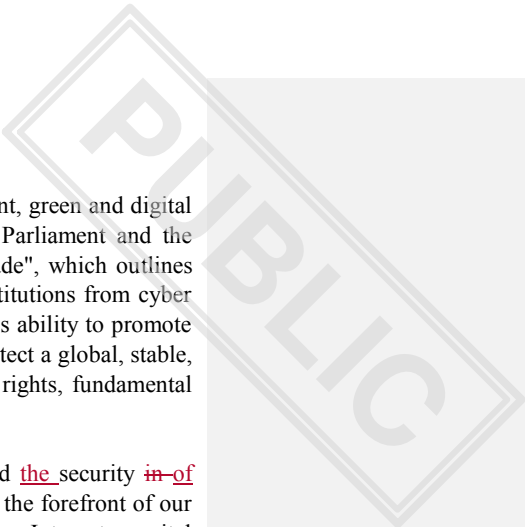
RECALLING its conclusions on:

- the Joint Communication to the European Parliament and the Council on the Cybersecurity Strategy for the European Union: "An Open, Safe and Secure Cyberspace",
- on Internet Governance,
- the Joint Communication to the European Parliament and the Council: "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU",
- cybersecurity capability and cyber capacity building in the EU,
 - the significance of 5G to the European Economy and the need to mitigate security risks linked to 5G [The 5G cybersecurity Toolbox],
- the future of a highly digitised Europe beyond 2020: "Boosting digital and economic competitiveness across the Union and digital cohesion",
- shaping Europe's Digital Future,
- complementary efforts to enhance resilience and counter hybrid threats,
- strengthening resilience and countering hybrid threats, including countering disinformation in the context of the COVID-19 pandemic,
- Cyber Diplomacy,
- on EU Coordinated Response to Large-Scale Cybersecurity Incidents and Crises
- a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox"),
- EU External Cyber Capacity Building Guidelines,
- the cybersecurity of connected devices,
- and its Council Resolution on Encryption - Security through encryption and security despite encryption.

RECALLING the European Council Conclusions on COVID-19, the Single Market, industry policy, digital and external relations and those on disinformation and hybrid threats,

RECALLING the Global Strategy for the European Union's Foreign and Security Policy,

RECALLING the Communications of the European Commission on shaping Europe's Digital Future and on the EU Security Union Strategy,

- 
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 to protect its people, businesses and institutions from cyber threats while enhancing the trust of citizens and organisations in the EU's ability to promote secure and reliable digital tools and connectivity, and to promote and protect a global, stable, secure, free and open cyberspace, grounded in the rule of law, human rights, fundamental freedoms and democratic values.
 2. RECOGNISING that the COVID-19 pandemic has brought trust in and the security ~~in~~ of Information and Communication Technology (ICT) tools and systems to the forefront of our daily lives, ~~stresses~~ **STRESSES** that cybersecurity and the global and open Internet are vital for the functioning of our public administrations and institutions at both national and EU level, for teleworking, tele-education and doing business online and for society as a whole.
 3. CALLS FOR the promotion and protection of the core EU values of democracy, human rights, fundamental freedoms including the freedom of expression, the right to free and equal access to information, the freedom of assembly and association, the right to privacy and the protection against mass surveillance and of the rule of law 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 its efforts to prevent the misuse of emerging technologies, notably through the use of diplomatic measures where necessary, as well as the export control of such technologies.
 4. HIGHLIGHTS the importance of strengthening the EU's strategic autonomy, particularly its digital and technological leadership in the field of cybersecurity, while preserving an open economy. In this respect, COMMITTS itself to promoting the Union's autonomy on the basis of the development of a dynamic Industrial Strategy that supports EU value chains and secures the supply chains in particular in the most strategic domains, while ensuring that access to the single market is gained on fair and equitable terms and with respect for the Union's values.
 5. Bearing in mind the shortage of cybersecurity skills in the workforce, STRESSES the importance of developing, retaining and attracting the best cybersecurity talent, for instance through education and training, and ENCOURAGES women's increased participation in science, technology, engineering, mathematics ('STEM') education and ICT jobs upskilling and reskilling in digital skills.

6. RECALLS that the common and comprehensive EU approach to cyber diplomacy aims to contribute to conflict prevention, the 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. REITERATES the United Nations General Assembly's call that UN Member States be guided by the UNGGE reports' recommendations in their use of ICT and notably the application of international law, in particular the UN Charter, in cyberspace.

Commented [A88]: Consider to move this paragraph before the other paragraphs on cyber diplomacy (24-27) in order to form a separate block on the external dimension.

7. REAFFIRMS that ~~the, with a view to~~ shaping of international standards in the areas of emerging technologies and core internet architecture ~~so that these are~~ in line with EU values and a multi-stakeholder approach ~~is essential to, the further development of standards within the Union is essential: this will~~ ensure that the Internet remains global, stable, secure, free and open and that digital technologies are human-centric, privacy-preserving, and that their use is lawful, safe and ethical. LOOKS FORWARD to the upcoming Standardisation Strategy and COMMITTS itself to proactive leadership and coordinated outreach to promote the EU's objectives at international level, including through enhanced representation in international and European standardisation bodies and cooperation with like-minded partners, civil society and the private sector.

Commented [A89]: Developing standards within the EU will only have an indirect effect on the global internet. We suggest sticking to the original wording in the Strategy.

Commented [A90]: we would encourage a more proactive role here, in line with the strategy.

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

9. EMPHASISES the need to include cybersecurity in all digital investments in the coming years and SUPPORTS the Commission's plan to increase public spending and leverage private investment in the cybersecurity domain, taking into account the prospective increase in the number of sectors to which the Directive on measures for a high common level of cybersecurity across the Union (NIS Directive 2.0) will apply. HIGHLIGHTS the importance of Small and Medium Sized Enterprises (SMEs) in the cybersecurity ecosystem and RECOGNISES the relevant financial instruments available to support a cybersecurity digital transformation over the 2021-2027 Multiannual Financial Framework (MFF) as well as in the Recovery and Resilience Facility.

10. LOOKS FORWARD to the rapid implementation of the Regulation on Cybersecurity Industrial, Technology and Research Competence Centre and Network of Coordination Centres (CCCN) with a view to maximising the effects of investments to strengthen the Union's leadership in the field of cybersecurity, to support technological capacities and skills and to increase the Union's global competitiveness with input from industry and academic communities in cybersecurity, which ~~should~~will be brought into a more systematic collaboration.

11. REITERATES the ~~need to~~importance of explore the scope of assessing the need for a possible horizontal Union legal act, including a new duty of care for manufacturers and conditions for the placement on the market for market access, which the Commission may be invited to propose in order to address all relevant aspects of cybersecurity of connected objects and its links with the cybersecurity certification framework under the Cybersecurity Act (CSA), as well as any other product type specific ~~instruments~~measures, ~~in order to ensure~~while ensuring adequate synergies ~~and, while~~ avoiding inconsistencies or duplication.

Commented [A91]: suggest bringing it in line with the CC on IoTs.

The new duty of care for manufacturers if from the Strategy, the conditions for the placement on the market part is from the CC on IoTs

Commented [A92]: The conditionality "may be invited" is vague. We suggest sticking to the wording of the CC on IoT.

12. ACKNOWLEDGES the importance of a harmonised approach on cybersecurity in the Union, while fully respecting Member States' competences, and WELCOMES the new proposal for a Directive on measures for a high common level of cybersecurity across the Union (NIS Directive 2.0) that builds upon the NIS Directive as an evolution of the efforts undertaken and which has contributed to strengthening and harmonising national cybersecurity frameworks and promoted cooperation between Member States. Furthermore, RECOGNISES the need for close alignment with other sectorial legislation in this domain.

13. TAKES NOTE of the Commission's proposal to support Member States in strengthening their national Security Operation Centres (SOCs) and to build a network of SOCs across the EU, to detect signals of attacks on networks and enable responses before harm is done. LOOKS FORWARD to exploring this network's potential to strengthen SOCs as well as their complementarity and coordination with existing networks and actors (for instance CSIRTs Network, ENISA and CERT-EU, ~~the EU's cyber crises management framework~~), ~~including within the scope of the EU's cyber crisis management framework~~, in order to promote ~~a~~ a rapid, efficient, secure and reliable information-sharing culture. Within this process, the best use should be made of the work carried out in the context of Artificial Intelligence and High Performance Computing initiatives and by European Digital Innovation Hubs, as well as the entire electronic communications infrastructure such as land and submarine network systems.

14. TAKES NOTE of the possible development of an ultra-secure connectivity system, building on the Euro quantum communication infrastructure (QCI) and EUGOVSATCOM, and COMMENDS that it be based on a robust cybersecurity framework.

15. 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 its operators in guaranteeing that the Internet remains globally accessible and non-fragmented. RECOGNISES that an alternative European service for accessing the global internet (“DNS4EU” initiative), based on a transparent model which conforms to the latest security and data protection and privacy by design and by default standards and rules, while respecting law-enforcement data retention needs of Member States, can contribute to increased resilience.

16. 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 to increase the overall level of security, resilience and openness of the global internet, while increasing the competitiveness of the EU industry and in particular of the internet infrastructure operators.

17. 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 Cybersecurity Strategy and as based on the review 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. URGES Member States to continue 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 its strong commitment to applying the EU 5G Toolbox, including relevant restrictions on high-risk suppliers for key assets defined as critical and sensitive in the EU coordinated risk assessments and to continuing efforts made to guarantee the cybersecurity of 5G networks.

18. RECOGNISES the relevance of integrating cybersecurity into EU crisis response mechanisms and STRESSES the importance of enhancing cooperation and information-sharing amongst the various cybersecurity communities within the EU and of linking the existing structures and procedures (such as the Blueprint, the CSIRT Network, the NIS Cooperation Group, the Horizontal Working Party on Cyber Issue, CyCLONE, the European Cybercrime Centre, EU INCEN and the IPCR) in case of large-scale cyber incidents and threats. TAKING INTO ACCOUNT the progress already achieved in this domain, LOOKS FORWARD to the Commission’s proposal on the process, milestones and timeline for defining and implementing the Joint Cyber Unit (JCU) with a view to providing added value and streamlining the EU cybersecurity crisis management framework, including through preparedness, shared situational awareness, coordinated response and exercises, in a transparent and incremental manner while avoiding duplication and overlap and respecting the competences of the Member States.

Commented [A93]: If DNS resolving would be moved from internet service providers to a central EU DNS infrastructure, law enforcement will need the possibility for lawful access.

Commented [A94]: IPv6, being a new and complex protocol might have vulnerabilities which questions its security benefits. This is especially true for IPv6 protocol used in IoT devices.

The transition to IPv6 will become inevitable in the long run when the IPv4 address space is exhausted, but this alone will not necessary increase cybersecurity, which is why we need to support solutions that compensates for the vulnerabilities of IPv6.

19. As highlighted by the impact of the COVID-19 pandemic, STRESSES the importance of promoting cooperation and exchange between cybersecurity actors and law enforcement and judicial authorities and the need to expand and improve the capacity of these authorities to investigate cybercrime, while fully respecting fundamental rights and striving to ensure the requisite balance between various rights and interests, in particular privacy and security.
20. 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 citizens, governments, industry and society and, at the same time, the need to ensure the ability of the competent law enforcement and judicial authorities, without resorting to the use of backdoors or other means of weakening encryption, to exercise their lawful powers, both online and offline, to protect our societies and citizens.
21. CONTINUES to support and promote the Budapest Convention on Cybercrime, and the ongoing work on the Second Additional Protocol to that Convention. Furthermore, will continue to engage in multilateral exchanges on cybercrime to advance efficient cooperation and support capacity building, while ensuring the ~~ensure the~~ respect of human rights and fundamental freedoms.
22. 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, including by exploring the establishment of an EU Cyber Intelligence Working Group.
23. HIGHLIGHTS the importance of a robust and consistent security framework to better protect all EU personnel, data, information, communication networks 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 classified and non-classified EU networks while ensuring that sufficient resources are available. WELCOMES, in this context, the ongoing interinstitutional discussions on the establishment of common rules on information security and cybersecurity for all EU institutions, bodies, offices and agencies.
24. BUILDING ON the EU's cyber diplomacy efforts, COMMITTS itself to increasing the effectiveness and the efficiency of the EU Cyber Diplomacy Toolbox and LOOKS FORWARD to deepening discussions building on lessons learned from the application of this instrument to date, including the preparatory process leading to joint decisions. These discussions should aim at building a notion of shared security at international level by strengthening prevention, cooperation and advancing confidence and capacity building and, where necessary, impose restrictions, thereby contributing to the EU's security and integrity and consolidating the EU's cyber posture, in full respect of national competences and prerogatives. In particular, special attention should be given to countering cyberattacks affecting our critical infrastructure, democratic institutions and processes, as well as to countering cyberattacks on supply chain-attacks with systemic effects and cyber-enabled theft of intellectual property.

Commented [A95]: Article 25 deals with the UN process related engagement (so rule of law, stable open cyberspace, etc.) and Article 1 covers human rights, fundamental freedoms and democratic values .

Ensuring human rights and fundamental freedoms should not be the main feature here. The engagement related to the Budapest Convention should be broader and technical, and should include the fight against cybercrime and capacity building (E.g. GLACY+).

Human rights and fundamental freedoms can remain here, but is much more relevant to article 25 and 1.

25. In order to contribute to a global, secure, stable, free and open 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, contributing to the respect for international law in cyberspace and adherence to the norms, rules and principles of responsible state behaviour in cyberspace, for instance 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 outcome of both the current UN GGE and OEWG processes.

26. RECALLS its strong commitment to multilateralism aimed at strengthening cooperation and coordination with international and regional organisations, namely the United Nations, the Council of Europe, the OSCE, the OECD, NATO, 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~~ the UN Secretary General's Roadmap on digital cooperation, and the UN Secretary General's Agenda for Disarmament fostering accountability and adherence to emerging norms and contributing to the prevention of conflicts by peaceful means. WELCOMES the establishment of 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 EU delegations and MS embassies on international cyber issues in order to strengthen coordinated outreach. LOOKS FORWARD to regular briefings by the EEAS and to discussions on the Network's activities in the Horizontal Working Party on Cyber Issues.

+

~~26-27.~~ ACKNOWLEDGES the importance of strengthening cooperation with international partners, including with NATO, in order to advance the shared understanding of the cyber threat landscape, to develop cooperation mechanisms, to identify, where appropriate, cooperative diplomatic responses as well as to improve information-sharing, including through education, training and exercises. In particular, REAFFIRMS that a strong transatlantic partnership is vital ~~to ensure and to in ensuring contribute to~~ our common security, stability and prosperity.

~~27-28.~~ LOOK 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 security, crisis management and defence agenda, for instance 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 on setting up the Military CERT-Network by the European Defence Agency (EDA) and SUPPORTS efforts made to enhance synergies and coordination between the cybersecurity civilian, defence and space spheres, including through the dedicated PESCO projects.

Formatted: Indent: Left: 0.5 cm, No bullets or numbering, Tab stops: Not at 1.27 cm

Commented [A96]: having both ensuring and contributing is a redundancy.

~~28-29.~~ TAKES NOTE of the development of an EU External Cyber Capacity Building Agenda and the creation of an EU Cyber Capacity Building Board in order to increase cyber resilience and capacities worldwide. In this context, ENCOURAGES cooperation with Member States, as well as with public and private sector partners and other relevant international bodies, to ensure coordination and avoid duplication. In particular, ENCOURAGES focusing the cooperation ~~with partners in the~~ on the Western Balkans and in the EU Neighbourhood.

~~29-30.~~ 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 partners 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.

~~30-31.~~ WELCOMES the comprehensive proposals presented in the Cybersecurity Strategy and ACKNOWLEDGES that all of the initiatives presented therein are important. In order to ensure their seamless implementation, and taking into account the multiannual character of some of these initiatives, CONSIDERS it is necessary to set the priorities with an accompanying and detailed implementation plan.

~~31-32.~~ MONITORS the progress in the implementation of these Conclusions by the means of an Action Plan to be adopted by the Council by The action plan would be regularly reviewed and updated by the Council in cooperation with the European Commission and the High Representative.

IRELAND

COMMENTS FROM IRELAND

General Comments

Ireland thanks to the Presidency for its draft Conclusions, which, overall, reflect a balanced response to the EU's Cybersecurity Strategy for the Digital Decade.

The following general comments provide the overall context for some specific amendments that we have proposed to the draft conclusions. ~~Textual proposals are in bold red type and strikethrough.~~ International cooperation with likeminded third countries such as the US and the UK is a key priority. The EU needs to remain outward looking and supportive of building a constructive and mutually beneficial transatlantic relationship. Access to global markets and supporting resilient global supply chains as part of an open economy are essential for peace and prosperity, for the wellbeing of our citizens, businesses and societies and for the territorial cohesion of the Union itself.

International connectivity remains vitally important and efforts to improve the resilience of the Internet in Europe through DNS4EU must complement our work in the UN and other international forums towards an open and accessible global and un-fragmented internet. We particularly support the Presidency's proposals with regard to prioritisation of submarine cable infrastructure to enhance international connectivity. We must remain outward looking.

The Strategy and the legislative and investment proposals that accompany it, notably NIS2 and Digital Europe, call for a significant increase in Member State capabilities and resourcing in cybersecurity. It is therefore essential that there be capacity-building measures in place with Member States to boost their capabilities, while respecting Member States' particular sensitivities in the domain of security and defence.

ANNEX

The Council of the European Union,

RECALLING its conclusions on:

- the Joint Communication to the European Parliament and the Council on the Cybersecurity Strategy for the European Union: "An Open, Safe and Secure Cyberspace",
- on Internet Governance,
- the Joint Communication to the European Parliament and the Council: "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU",
- cybersecurity capability and cyber capacity building in the EU,
- the significance of 5G to the European Economy and the need to mitigate security risks linked to 5G [The 5G cybersecurity Toolbox],
- the future of a highly digitised Europe beyond 2020: "Boosting digital and economic competitiveness across the Union and digital cohesion",
- shaping Europe's Digital Future,
- complementary efforts to enhance resilience and counter hybrid threats,
- strengthening resilience and countering hybrid threats, including countering disinformation in the context of the COVID-19 pandemic,
- Cyber Diplomacy,
- on EU Coordinated Response to Large-Scale Cybersecurity Incidents and Crises
- a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox"),
- EU External Cyber Capacity Building Guidelines,
- the cybersecurity of connected devices,
- and its Council Resolution on Encryption - Security through encryption and security despite encryption.

RECALLING the European Council Conclusions on COVID-19, the Single Market, industry policy, digital and external relations and those on disinformation and hybrid threats,

RECALLING the Global Strategy for the European Union's Foreign and Security Policy,

RECALLING the Communications of the European Commission on shaping Europe's Digital Future and on the EU Security Union Strategy,

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 **to improve its resilience and** protect its people, businesses and institutions from cyber **incidents and** threats while enhancing the trust of citizens and organisations in the EU's ability to promote secure and reliable digital tools and connectivity, and to promote and protect a global, stable, secure, free and open cyberspace, grounded in the rule of law, human rights, fundamental freedoms and democratic values.
2. RECOGNISING that the COVID-19 pandemic has brought trust and security in Information and Communication Technology (ICT) tools and systems to the forefront of our daily lives, stresses that cybersecurity and the global and open Internet are vital **for the undertaking of economic and social activity**, for the functioning of our public administrations **and institutions** at both national and EU level, for teleworking, **online learning tele-education and doing business online** and for society as a whole.
3. CALLS FOR the promotion and protection of the core EU values of democracy, human rights, fundamental freedoms including the freedom of expression, the right to free and equal access to information, the freedom of assembly and association, the right to privacy and the protection against mass surveillance and of the rule of law 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 its efforts to prevent 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.**
4. HIGHLIGHTS the importance of strengthening the EU's **strategic autonomy**, particularly its digital and technological leadership in the field of cybersecurity, **while preserving an open economy**. In this respect, COMMITS itself to promoting the Union's autonomy on the basis of the development of a dynamic Industrial Strategy that supports EU value chains and secures the supply chains in particular in the most strategic domains, while ensuring that access to the single market is gained on fair and equitable terms and with respect for the Union's values.
5. Bearing in mind the shortage of cybersecurity skills in the workforce, STRESSES the importance of developing, retaining and attracting the best cybersecurity talent, for instance through education and training, and ENCOURAGES women's increased participation in science, technology, engineering, mathematics ('STEM') education and ICT jobs upskilling and reskilling in digital skills.

Commented [A97]: There is a need for increased emphasis in the paragraph on resilience as well as protection. (Reflecting in particular the proposed NIS2 and DORA proposals).

The new EU level proposals for a CyCLONe Network on cyber crisis management are about large scale cyber incidents and crises. This is broader than mere cyber-attacks. In fact most incidents reported under the NIS Directive have been hazard-related rather than malicious, e.g. human error, environmental damage, system failure etc.

Commented [A98]: Ireland proposes that the emphasis should be on economy and society rather than public bodies.

Commented [A99]: Ireland welcomed the concept of "operationalising" these important documents as expressed in the Strategy.

Commented [A100]: Different language reflecting the need to have resilient and diverse supply chains and global markets for EU know-how on cyber would be preferable.

A secondary danger is that a failure to have open markets on cybersecurity could lead to reluctance to co-operate at operational level, e.g. among CSIRTs or law enforcement. Cyber is borderless and effective takedowns in the EU has required cooperation from cyber authorities in likeminded 3rd countries such as the US and UK. The experience of EC3 in Europol with J-CAT refers.

Commented [A101]: This text is very welcome. If the text could be strengthened by replacing "preserving" with "further developing", this would work better.

6. RECALLS that the common and comprehensive EU approach to cyber diplomacy aims to contribute to conflict prevention, the 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. REITERATES the United Nations General Assembly's call that UN Member States be guided by the UNGGE reports' recommendations in their use of ICT and notably the application of international law, in particular the UN Charter, in cyberspace.
7. REAFFIRMS that, with a view to shaping international standards in the areas of emerging technologies and core internet architecture so that these are in line with EU values and a multi-stakeholder approach, the further development of standards within the Union is essential: this will ensure that the Internet remains global, stable, secure, free and open and that digital technologies are human-centric, privacy-preserving, and that their use is lawful, safe and ethical. LOOKS FORWARD to the upcoming Standardisation Strategy and COMMITS itself to proactive and coordinated outreach to promote the EU's objectives at international level, including through cooperation with like-minded partners, civil society and the private sector.
8. STRONGLY SUPPORTS the multi-stakeholder model for Internet governance and commits itself to reinforcing regular and structured exchanges with stakeholders including the private sector, academia and civil society, in particular within the context of the Paris Call and in international fora. PROMOTES universal, affordable and equal access to the Internet and, in particular, the empowerment of persons in vulnerable situations or marginalised groups, in both policy development and in the use of the Internet.
9. EMPHASISES the need to include cybersecurity in all digital investments in the coming years and SUPPORTS the Commission's plan to increase public spending and leverage private investment in the cybersecurity domain. **REAFFIRMS the importance of ongoing supports for capacity building in all of the Member States, having regard to distinct national approaches to security and to facilitate trust and cooperation between them in the interests of the territorial cohesion of the Union. ~~taking into account the prospective increase in the number of sectors to which the Directive on measures for a high common level of cybersecurity across the Union (NIS Directive 2.0) will apply.~~** HIGHLIGHTS the importance of Small and Medium Sized Enterprises (SMEs) in the cybersecurity ecosystem and RECOGNISES the relevant financial instruments available to support a cybersecurity digital transformation over the 2021-2027 Multiannual Financial Framework (MFF) as well as in the Recovery and Resilience Facility.

Commented [A102]: The resourcing implications arising on Member States in regard to resourcing and developing cyber security capabilities for resilience, operational protection, supervision, regulation and enforcement of economic and societal activities in a country are very significant. Capacity building supports are needed from the EU for both the public and private sector as part of digital investments.

IE has its own distinct approach to security and defence as set out in the Protocol on the concerns of the Irish people on the Treaty of Lisbon, OJEU, L60/131, 2.3.2013

There are emerging substantive risks as regards continued access to the Digital Single Market if security capabilities are not considered adequate by other MS and EU-Institutions.

Commented [A103]: It is premature to refer to extension of scope and prejudicial to ongoing legislative deliberations on the NIS2 file.

10. LOOKS FORWARD to the **prompt rapid** implementation of the Regulation on Cybersecurity Industrial, Technology and Research Competence Centre and Network of Coordination Centres (CCCN) with a view to maximising the effects of investments to strengthen the Union's leadership in the field of cybersecurity, to support technological capacities and skills and to increase the Union's global competitiveness with input from industry and academic communities in cybersecurity. **WELCOMES in particular the support of the Commission for the timely establishment of both the Cybersecurity Competence Centre and National Coordination Centres so that the necessary systematic collaboration and pooling of capacities can take place, which should be brought into a more systematic collaboration.**

Commented [A104]: The Commission has a key role to play in establishing this new EU body and also in assisting Member States in designating and resourcing the National Coordination Centres.

11. REITERATES the need to explore the scope of a possible horizontal Union legal act, **within the scope of the Radio Equipment Directive and the Cybersecurity Act's certification framework**, including for market access, which the Commission may be invited to propose in order to address all relevant aspects of cybersecurity of connected objects **and its links with the cybersecurity certification framework under the Cybersecurity Act (CSA)**, as well as any other product specific instruments, in order to ensure adequate synergies, while avoiding inconsistencies or duplication.

Commented [A105]: It would be important the any Union legal act would be based on existing EU primary legislation, i.e. a delegated act under the Radio Equipment Directive or an implementing act on a bespoke cybersecurity certification scheme under the Cybersecurity Act Regulation.

12. ACKNOWLEDGES the importance of a harmonised approach on cybersecurity in the Union, while fully respecting Member States' competences, and WELCOMES **in principle** the new proposal for a Directive on measures for a high common level of cybersecurity across the Union (NIS Directive 2.0) that builds upon the NIS Directive as an evolution of the efforts undertaken and which has contributed to strengthening and harmonising national cybersecurity frameworks and promoted cooperation between Member States. Furthermore, RECOGNISES the need for close alignment with other sectorial legislation in this domain.

Commented [A106]: The statement should not prejudice legislative deliberations of the proposed NIS2 Directive in the WP.

13. TAKES NOTE of the Commission's proposal to support Member States in strengthening **their national** Security Operation Centres (SOCs) and to build a network of SOCs across the EU, **to improve situational awareness, facilitate information sharing, enable timely handling of threats and incidents and mitigate adverse impacts. detect signals of attacks on networks and enable responses before harm is done.** LOOKS FORWARD to exploring this network's potential to strengthen SOCs as well as their complementarity and coordination with existing networks and actors, **namely CSIRTs and ISACs** (for instance CSIRTs Network, ENISA and CERT-EU), including within the scope of the EU's cyber crisis management framework, in order to promote an efficient, secure and reliable information-sharing culture. **Within** This process, **the best use should be made of the will build on** work carried out in the context of Artificial Intelligence and High Performance Computing initiatives and by European Digital Innovation Hubs, as well as the entire electronic communications infrastructure such as land and submarine network systems.

Commented [A107]: It is important that there be a realistic view of the role of SOCs as part of the Cyber Shield initiative. SOCs exist within a corporate structure in a public or private body. Managed security service providers use SOCs to monitor their clients 'network edge'. The capacity to have SOCs with national reach is very ambitious. Computer security incident response teams (CSIRTs) and Information Sharing and Analysis Centres (ISACs) can use SOC infrastructure to develop an operational picture thereby improving situational awareness. The sharing of threat intelligence on IOCs can enhance incident response.

14. TAKES NOTE of the possible development of an ultra-secure connectivity system, building on the Euro quantum communication infrastructure (QCI) and EUGOVSATCOM, and COMMENDS that it be based on a robust cybersecurity framework.

15. 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 its operators in guaranteeing that the Internet remains globally accessible and non-fragmented. RECOGNISES that an alternative European service for accessing the global internet ("DNS4EU" initiative), based on a transparent model which conforms to the latest security and data protection and privacy by design and by default standards and rules, can contribute to increased resilience, while maintaining and enhancing international connectivity for all Member States.

Commented [A108]: There is a risk that external partners may perceive an inherent conflict between the EU's promotion of a non-fragmented Internet and the development of an EU-only DNS structure, even if DNS4EU provides for baseline take-up of security features such as DNSSEC, DMARC etc.

The preservation and maintenance of an open and accessible global internet is a key priority in our approach to cyber issues and internet governance in international forums.

Commented [A109]: The implications of an EU-only DNS infrastructure for connectivity and routing of traffic are unknown. DNS4EU should not undermine international connectivity. Time delays with resolving IP addresses due to rerouting requirements could introduce latency effects with adverse implications for time critical services such as financial trading.

16. 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 to increase the overall level of security, resilience and openness of the global internet, while increasing the competitiveness of the EU industry and in particular of the internet infrastructure operators.

17. 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 Cybersecurity Strategy and as based on the review 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. URGES Member States to continue 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 its strong commitment to applying the EU 5G Toolbox, including relevant restrictions on high-risk suppliers for key assets defined as critical and sensitive in the EU coordinated risk assessments and to continuing efforts made to guarantee the cybersecurity of 5G networks.

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

19. As highlighted by the impact of the COVID-19 pandemic, STRESSES the importance of promoting cooperation and exchange between cybersecurity actors and law enforcement and judicial authorities and the need to expand and improve the capacity of these authorities to investigate cybercrime, while fully respecting fundamental rights and striving to ensure the requisite balance between various rights and interests, in particular privacy and security.

20. 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 citizens, governments, industry and society and, at the same time, the need to ensure the ability of the competent law enforcement and judicial authorities to exercise their lawful powers, both online and offline, to protect our societies and citizens.

Commented [A110]: The reference to strong encryption is particularly welcomed as a means of upholding fundamental rights and European values. It rules out the use of so called 'backdoors' as a means of providing information to unknown third parties and not only law enforcement thereby undermining trust and privacy and being manifestly at odds with the Charter of Fundamental Rights.

21. CONTINUES to support and promote the Budapest Convention on Cybercrime, and the ongoing work on the Second Additional Protocol to that Convention. Furthermore, will continue to engage in multilateral exchanges on cybercrime to ensure the respect of human rights and fundamental freedoms.

22. 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 INCEN's work, including by exploring the establishment of an EU Cyber Intelligence Working Group.

23. HIGHLIGHTS the importance of a robust and consistent security framework to better protect all EU personnel, data, information, communication networks 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 classified and non-classified EU networks while ensuring that sufficient resources are available. WELCOMES, in this context, the ongoing interinstitutional discussions on the establishment of common rules on information security and cybersecurity for all EU institutions, bodies, offices and agencies.

24. BUILDING ON the EU's cyber diplomacy efforts, COMMITS itself to increasing the effectiveness and the efficiency of the EU Cyber Diplomacy Toolbox and LOOKS FORWARD to deepening discussions building on lessons learned from the application of this instrument to date. These discussions should aim at building a notion of shared security at international level by strengthening prevention, cooperation and advancing confidence and capacity building and, where necessary, impose restrictions, thereby contributing to the EU's security and integrity and consolidating the EU's cyber posture, in full respect of national competences and prerogatives. In particular, special attention should be given to countering cyberattacks affecting our critical infrastructure, democratic institutions and processes, as well as to countering cyberattacks on supply chain-attacks with systemic effects and cyber-enabled theft of intellectual property. **In this context, ACKNOWLEDGES the importance of strengthening cooperation with international in order to advance the shared understanding of the cyber threat landscape, to develop cooperation mechanisms, to identify, where appropriate, cooperative diplomatic responses as well as to improve information-sharing, including through education, training and exercises.**

Commented [A111]: Ireland agrees that agreed language around restrictive measures would be preferable.

Commented [A112]: Moved from paragraph 27 – see accompanying note to paragraph 27.

Reference to NATO removed in accordance with the Presidency's email of 4 February.

25. In order to contribute to a global, secure, stable, free and open 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, contributing to the respect for international law in cyberspace and adherence to the norms, rules and principles of responsible state behaviour in cyberspace, for instance 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 outcome of both the current UN GGE and OEWG processes.

26. RECALLS its strong commitment to multilateralism aimed at strengthening cooperation and coordination with international and regional organisations, namely the United Nations, the Council of Europe, the OSCE, the OECD, NATO, 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 the UN Secretary General's Roadmap on digital cooperation.

Commented [A113]: It might be preferable to avoid such a long list in the body of the text – putting this in a footnote might be an option.

Commented [A114]: Ireland proposes a dedicated paragraph for third country consultations – see 26 bis below.

26 (bis) LOOKS FORWARD to strengthening and expanding its structured cyber dialogues and consultations with third countries to promote its values and vision for cyber space, sharing best practices and seeking to cooperate more effectively. WELCOMES, in this regard, the provisions on cybersecurity cooperation within the EU-UK Trade and Cooperation Agreement and REAFFIRMS that a strong transatlantic partnership is vital to ensure and to contribute to our common security, stability and prosperity.

Commented [A115]: Ireland welcomed the approach in the Strategy, which referred to dialogues with reference to values and vision etc.

Ireland strongly supports a reference to the transatlantic relationship but this should not be limited (as was the case in paragraph 27) to the context of threat landscape and responses.

Furthermore, Ireland wishes to see a reference to the EU-UK TCA.

27 WELCOMES the establishment of 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 EU delegations and MS embassies on international cyber issues in order to strengthen coordinated outreach.

28 ~~ACKNOWLEDGES the importance of strengthening cooperation with international partners, including with NATO, in order to advance the shared understanding of the cyber threat landscape, to develop cooperation mechanisms, to identify, where appropriate, cooperative diplomatic responses as well as to improve information sharing, including through education, training and exercises. In particular, REAFFIRMS that a strong transatlantic partnership is vital to ensure and to contribute to our common security, stability and prosperity.~~

Commented [A116]: The language in this paragraph was drawn from the section of the Strategy dedicated to the Cyber Diplomacy Toolbox and Ireland would prefer to continue to associate it to this part of the Conclusions (have moved the first sentence to para 24).

Reference transatlantic relationship moved to stand-alone paragraph above (26. Bis)

- 29 LOOK 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 security, crisis management and defence agenda, for instance 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 on setting up the Military CERT-Network by the European Defence Agency (EDA) and SUPPORTS efforts made to enhance synergies and coordination between the cybersecurity civilian, defence and space spheres, including through the dedicated PESCO projects.
- 30 TAKES NOTE of the development of an EU External Cyber Capacity Building Agenda and the creation of an EU Cyber Capacity Building Board in order to increase cyber resilience and capacities worldwide. In this context, ENCOURAGES cooperation with Member States, as well as with public and private sector partners 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 Neighbourhood.
- 31 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 partners 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.
- 32 WELCOMES the comprehensive proposals presented in the Cybersecurity Strategy and ACKNOWLEDGES that all of the initiatives presented therein are important. In order to ensure their seamless implementation, and taking into account the multiannual character of some of these, CONSIDERS it is necessary to set the priorities with an accompanying and detailed implementation plan.
- 33 MONITORS the progress in the implementation of these Conclusions by the means of an Action Plan to be adopted by the Council by The action plan would be regularly reviewed and updated by the Council in cooperation with the European Commission and the High Representative.
-

ITALY

The Council of the European Union,

RECALLING its conclusions on:

- the Joint Communication to the European Parliament and the Council on the Cybersecurity Strategy for the European Union: "An Open, Safe and Secure Cyberspace",
- ~~on~~ Internet Governance,
- the Joint Communication to the European Parliament and the Council: "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU",
- cybersecurity capability and cyber capacity building in the EU,
 - the significance of 5G to the European Economy and the need to mitigate security risks linked to 5G [The 5G cybersecurity Toolbox],
- the future of a highly digitised Europe beyond 2020: "Boosting digital and economic competitiveness across the Union and digital cohesion",
- shaping Europe's Digital Future,
- ~~complementary efforts to enhance resilience and counter hybrid threats,~~
- ~~on~~ EU Coordinated Response to Large-Scale Cybersecurity Incidents and Crises
 - a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox"),
- EU External Cyber Capacity Building Guidelines,
- the cybersecurity of connected devices,
- and its Council Resolution on Encryption - Security through encryption and security despite encryption.

RECALLING the European Council Conclusions on COVID-19, the Single Market, industry policy, digital and external relations and those on disinformation and hybrid threats,

RECALLING the Global Strategy for the European Union's Foreign and Security Policy,

RECALLING the Communications of the European Commission on shaping Europe's Digital Future and on the EU Security Union Strategy,

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 to protect its people, businesses and institutions from cyber threats while enhancing the trust of citizens and organisations in the EU's ability to promote secure and reliable digital tools and connectivity, and to promote and protect a global, stable, secure, free and open cyberspace, grounded in the rule of law, human rights, fundamental freedoms and democratic values.
2. RECOGNISING that the COVID-19 pandemic has brought trust and security in Information and Communication Technology (ICT) tools and systems to the forefront of our daily lives, stresses that cybersecurity and the global and open Internet are vital for the functioning of our society as a whole, public administrations and institutions at both national and EU level, for teleworking, tele-education and doing business online, including –and for –society as a whole, public administrations and institutions at both national and EU level.
3. CALLS FOR the promotion and protection of the core EU values of democracy, human rights, fundamental freedoms including the freedom of expression, the right to free and equal access to information, the freedom of assembly and association, the right to privacy and the protection against mass surveillance and of the rule of law 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 its efforts to prevent the misuse of emerging technologies, including Artificial Intelligence and High Performance Computing, notably through the use of diplomatic measures where necessary, as well as the export control of such technologies.
4. HIGHLIGHTS the importance of strengthening the EU's strategic autonomy, particularly its digital and technological leadership in the field of cybersecurity, while preserving an open economy. In this respect, COMMITS itself to promoting the Union's autonomy on the basis of the development of a dynamic and inclusive Industrial Strategy that supports EU value chains and secures the supply chains in particular in the most strategic domains, while ensuring that access to the single market is gained on fair and equitable terms and with respect for the Union's values.
5. Bearing in mind the shortage of cybersecurity skills in the workforce, STRESSES the importance of developing, retaining and attracting the best cybersecurity talent, for instance through education and training, UNDERLINES the importance of mainstreaming gender issues in all policies and ENCOURAGES women's 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, advance the promotion of gender equality at the global level and increase international security.

6. RECALLS that the common and comprehensive EU approach to cyber diplomacy aims ~~to~~^{ing} ~~at~~ contributing to conflict prevention, ~~the~~ 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. REITERATES the United Nations General Assembly's call that UN Member States be guided by the UNGGE reports' recommendations in their use of ICT and notably the application of international law, in particular the UN Charter, in cyberspace.
7. REAFFIRMS that, with a view to shaping international standards in the areas of emerging technologies and core internet architecture so that these are in line with EU values and a multi-stakeholder approach, the further development of standards within the Union is essential: this will ensure that the Internet remains global, stable, secure, free and open and that digital technologies are human-centric, privacy-preserving, and that their use is lawful, safe and ethical. LOOKS FORWARD to the upcoming Standardisation Strategy and COMMITS itself to proactive and coordinated outreach to promote the EU's objectives at international level, including through cooperation with like-minded partners, civil society and the private sector.
8. STRONGLY SUPPORTS the multi-stakeholder model for Internet governance and commits itself to reinforcing regular and structured exchanges with stakeholders including the private sector, academia and civil society, ~~in particular within the context of the Paris Call and in international fora, including within the context of the Paris Call.~~ PROMOTES universal, affordable and equal access to the Internet and, in particular, the empowerment of persons in vulnerable situations or marginalised groups, in both policy development and in the use of the Internet.
9. EMPHASISES the need to include cybersecurity in all digital investments in the coming years and SUPPORTS the Commission's plan to increase public spending and leverage private investment in the cybersecurity domain, taking into account the prospective increase in the number of sectors to which the Directive on measures for a high common level of cybersecurity across the Union (NIS Directive 2.0) will apply. HIGHLIGHTS the importance of Small and Medium Sized Enterprises (SMEs) in the cybersecurity ecosystem and RECOGNISES the ~~relevant~~^{increasing} financial instruments available to support a cybersecurity digital transformation over the 2021-2027 Multiannual Financial Framework (MFF) as well as in the Recovery and Resilience Facility.

10. LOOKS FORWARD to the ~~swift-rapid~~ implementation of the Regulation on Cybersecurity Industrial, Technology and Research Competence Centre and Network of Coordination Centres (CCCN) with a view to maximising the effects of investments to strengthen the Union's leadership in the field of cybersecurity, to support technological capacities and skills and to increase the Union's global competitiveness with input from industry and academic communities in cybersecurity, which ~~should be brought into~~ will benefit from a more systematic and inclusive collaboration.
11. REITERATES the need to explore the scope of a possible horizontal Union legal act, including for market access, which the Commission may be invited to propose in order to address all relevant aspects of cybersecurity of connected objects and its links with the cybersecurity certification framework under the Cybersecurity Act (CSA), as well as any other product specific instruments, in order to ensure adequate synergies, while avoiding inconsistencies or duplication.
12. ACKNOWLEDGES the importance of a harmonised approach on cybersecurity in the Union, while fully respecting Member States' competences, and ~~WELCOMES-LOOKS FORWARD to negotiating~~ the new ~~proposal for a~~ Directive on measures for a high common level of cybersecurity across the Union (NIS Directive 2.0) that builds upon the NIS Directive as an evolution of the efforts undertaken and which has contributed to strengthening and harmonising national cybersecurity frameworks and promoted cooperation between Member States. Furthermore, RECOGNISES the need for close alignment with other sectorial legislation in this domain.
13. TAKES NOTE of the Commission's proposal to support Member States in strengthening their national Security Operation Centres (SOCs) and to build a network of SOCs across the EU, to detect signals of attacks on networks and enable responses before harm is done. LOOKS FORWARD to exploring this network's potential to strengthen SOCs as well as their complementarity and coordination with existing networks and actors (for instance CSIRTs Network, ENISA and CERT-EU), including within the scope of the EU's cyber crisis management framework, in order to promote an efficient, secure and reliable information-sharing culture. Within this process, the best use should be made of the work carried out in the context of Artificial Intelligence and High Performance Computing initiatives and by European Digital Innovation Hubs, as well as the entire electronic communications infrastructure such as land and submarine network systems.
14. TAKES NOTE of the possible development of an ultra-secure connectivity system, building on the Euro quantum communication infrastructure (QCI) and EUGOVSAATCOM, and RECOMMENDS that it be based on a robust cybersecurity framework.

15. 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 its operators in guaranteeing that the Internet remains globally accessible and non-fragmented. RECOGNISES that an alternative European service for accessing the global internet (“DNS4EU” initiative), based on a transparent model which conforms to the latest security and data protection and privacy by design and by default standards and rules, can contribute to increased resilience.
16. 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 to increase the overall level of security, resilience and openness of the global internet, while increasing the competitiveness of the EU industry and in particular of the internet infrastructure operators.
17. 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 Cybersecurity Strategy and as based on the review 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 establishing a common level of protection, URGES ENCOURAGES Member States to continue 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 its strong commitment to applying the EU 5G Toolbox, including relevant restrictions on high-risk suppliers for key assets defined as critical and sensitive in the EU coordinated risk assessments and to continuing efforts made to guarantee the cybersecurity of 5G networks and development of 6G.
18. RECOGNISES the relevance of integrating cybersecurity into EU crisis response mechanisms and STRESSES the importance of enhancing cooperation and information-sharing amongst the various cybersecurity communities within the EU and of linking the existing structures and procedures (such as the Blueprint, the CSIRT Network, the NIS Cooperation Group, CyCLONe, the European Cybercrime Centre, EU INCEN and the IPCR) in case of large-scale cyber incidents and threats. TAKING INTO ACCOUNT the progress already achieved in this domain, LOOKS FORWARD to the Commission’s proposal on the process, milestones and timeline for defining ~~and implementing~~ the Joint Cyber Unit (JCU) with a view to providing added value and streamlining the EU cybersecurity crisis management framework, including through preparedness, shared situational awareness, coordinated response and exercises, in a transparent and incremental manner while avoiding duplication and overlap and respecting the competences of the Member States.

19. As highlighted by the impact of the COVID-19 pandemic, STRESSES both the importance of promoting cooperation and exchange between cybersecurity actors and law enforcement and judicial authorities ~~and as well as~~ the need to expand and improve the capacity of these authorities to investigate cybercrime, while fully respecting fundamental rights and striving to ensure the ~~requisite appropriate~~ balance ~~between of~~ various rights and interests, in particular privacy and security.
20. 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 citizens, governments, industry and society and, at the same time, the need to ensure the ability of the competent law enforcement and judicial authorities to exercise their lawful powers, both online and offline, to protect our societies and citizens.
21. CONTINUES to support and promote the Budapest Convention on Cybercrime, and the ongoing work on the Second Additional Protocol to that Convention. Furthermore, will continue to engage in multilateral exchanges on cybercrime to ensure the respect of human rights and fundamental freedoms.
22. 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 INCEN's work, including by exploring the establishment benefits and possible mechanisms of an EU Cyber Intelligence Working Group.
23. HIGHLIGHTS the importance of a robust and consistent security framework to ~~better~~ protect all EU personnel, data, information, communication networks 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 classified and non-classified EU networks while ensuring that sufficient resources are available. WELCOMES, in this context, the ongoing inter-institutional discussions on the establishment of common rules on information security and cybersecurity for all EU institutions, bodies, offices and agencies.
24. BUILDING ON the EU's cyber diplomacy efforts, COMMITS itself to increasing the effectiveness and the efficiency of the EU Cyber Diplomacy Toolbox and LOOKS FORWARD to deepening discussions building on lessons learned from the application of this instrument to date. These discussions should aim at building a notion of shared security at international level by strengthening prevention, cooperation and advancing confidence and capacity building and, where necessary, impose restrictions, thereby contributing to the EU's security and integrity and consolidating the EU's cyber posture, in full respect of national competences and prerogatives. In particular, special attention should be given to countering cyberattacks, that might affecting our critical infrastructure, supply chain with systemic effects, our critical infrastructure, democratic institutions and processes, as well as systemic ~~to countering cyberattacks on supply chain attacks with systemic effects and and~~ cyber-enabled theft of intellectual property.

25. RECALLS its strong commitment to multilateralism aimed at strengthening cooperation and coordination with international and regional organisations, namely the United Nations, the Council of Europe, the OSCE, the OECD, NATO, 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, tailor-made 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 the UN Secretary General's Roadmap on digital cooperation.

25. In order to contribute to a global, secure, stable, free and open 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, contributing to the respect for international law in cyberspace and adherence to the norms, rules and principles of responsible state behaviour in cyberspace, for instance 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 outcome of both the current UN GGE and OEWG processes. In this context,

28-27. ACKNOWLEDGES the importance of strengthening cooperation with international partners, including with NATO, in order to advance the shared understanding of the cyber threat landscape, to develop cooperation mechanisms, to identify, where appropriate, cooperative diplomatic responses as well as to improve information-sharing, including through education, training and exercises. In particular, REAFFIRMS that a strong transatlantic partnership is vital to ensure and to contribute to our common security, stability and prosperity.

29-28. 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 security, crisis management and defence agenda, for instance 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 on setting up the Military CERT-Network by the European Defence Agency (EDA) and SUPPORTS efforts made to enhance synergies and coordination between the cybersecurity civilian, defence and space spheres, including through ~~the~~ dedicated PESCO projects and the use of EDF.

30-29. ~~TAKES NOTE of~~ ENCOURAGES the development of an EU External Cyber Capacity Building Agenda and the creation of an EU Cyber Capacity Building Board in close cooperation with member States in order to increase cyber resilience and capacities worldwide. In this context, ENCOURAGES-WELCOMES cooperation with ~~Member States, as well as with~~ public and private sector partners 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 Neighbourhood.

31-30. 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 partners 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.

~~32.~~ WELCOMES the comprehensive proposals presented in the Cybersecurity Strategy and ACKNOWLEDGES that ~~all of~~ the initiatives presented therein are important and timely. In order to ensure their seamless development, implementation and monitoring, and taking into account the multiannual character of some ~~of these initiatives~~, CONSIDERS ~~it is~~ necessary to ~~set the priorities~~ accompany it with an ~~accompanying and~~ detailed implementation Action plan Plan which will take into account all of the above to be

LATVIA

The Council of the European Union,

RECALLING its conclusions on:

- the Joint Communication to the European Parliament and the Council on the Cybersecurity Strategy for the European Union: "An Open, Safe and Secure Cyberspace",
- on Internet Governance,
- the Joint Communication to the European Parliament and the Council: "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU",
- cybersecurity capability and cyber capacity building in the EU,
 - the significance of 5G to the European Economy and the need to mitigate security risks linked to 5G [The 5G cybersecurity Toolbox],
- the future of a highly digitised Europe beyond 2020: "Boosting digital and economic competitiveness across the Union and digital cohesion",
- shaping Europe's Digital Future,
- complementary efforts to enhance resilience and counter hybrid threats,
- strengthening resilience and countering hybrid threats, including countering disinformation in the context of the COVID-19 pandemic,
- Cyber Diplomacy,
- on EU Coordinated Response to Large-Scale Cybersecurity Incidents and Crises
- a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox"),
- EU External Cyber Capacity Building Guidelines,
- the cybersecurity of connected devices,
- and its Council Resolution on Encryption - Security through encryption and security despite encryption.

RECALLING the European Council Conclusions on COVID-19, the Single Market, industry policy, digital and external relations and those on disinformation and hybrid threats,

RECALLING the Global Strategy for the European Union's Foreign and Security Policy,

RECALLING the Communications of the European Commission on shaping Europe's Digital Future and on the EU Security Union Strategy,

1. HIGHLIGHTS the fact that cybersecurity is one of elements which 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 to protect its people, businesses and institutions from cyber threats while enhancing the trust of citizens and organisations in the EU's ability to promote secure and reliable digital tools and connectivity, and to promote and protect a global, stable, secure, free and open cyberspace, grounded in the rule of law, human rights, fundamental freedoms and democratic values.
2. RECOGNISING that the COVID-19 pandemic has brought trust and security in Information and Communication Technology (ICT) tools and systems to the forefront of our daily lives, stresses that cybersecurity and the global and open Internet are vital for the functioning of our public administrations and institutions at both national and EU level, for teleworking, tele-education and doing business online and for society as a whole.
3. CALLS FOR the promotion and protection of the core EU values of democracy, human rights, fundamental freedoms including the freedom of expression, the right to free and equal access to information, the freedom of assembly and association, the right to privacy and the protection against mass surveillance and of the rule of law 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 its efforts to prevent the misuse of emerging technologies, notably through the use of diplomatic measures where necessary, as well as the export control of such technologies.
4. HIGHLIGHTS the importance of strengthening the EU's strategic autonomy, particularly its digital and technological leadership in the field of cybersecurity, while preserving an open economy. In this respect, COMMITS itself to promoting the Union's autonomy on the basis of the development of a dynamic Industrial Strategy that supports EU value chains and secures the supply chains in particular in the most strategic domains, while ensuring that access to the single market is gained on fair and equitable terms and with respect for the Union's values.
5. Bearing in mind the shortage of cybersecurity skills in the workforce, STRESSES the importance of developing, retaining and attracting the best cybersecurity talent, for instance through education and training, and ENCOURAGES women's increased participation in science, technology, engineering, mathematics ('STEM') education and ICT jobs upskilling and reskilling in digital skills.

Commented [A117]: What is the intended scope?
Which are the most strategic domains?

6. RECALLS that the common and comprehensive EU approach to cyber diplomacy aims to contribute to conflict prevention, including reduction of risks of misperception, escalation and conflict that may stem from ICT incidents, the 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~~. REITERATES the United Nations General Assembly's call upon that UN Member States to be guided by the UNGGE reports' recommendations in their use of ICT and notably the application of international law, in particular the UN Charter, in cyberspace.
7. REAFFIRMS that, with a view to shaping international standards in the areas of emerging technologies and core internet architecture so that these are in line with EU values and a multi-stakeholder approach, ~~the further development of standards within the Union is essential~~; this will ensure that the Internet remains global, stable, secure, free and open and that digital technologies are human-centric, privacy-preserving, and that their use is lawful, safe and ethical. LOOKS FORWARD to the upcoming Standardisation Strategy and COMMITS itself to proactive and coordinated outreach to promote the EU's objectives at international level, including through cooperation with like-minded partners, civil society and the private sector.
8. STRONGLY SUPPORTS the multi-stakeholder model for Internet governance and commits itself to reinforcing regular and structured exchanges of opinions with stakeholders including the private sector, academia and civil society, in particular within the context of the Paris Call and in international fora. PROMOTES universal, affordable and equal access to the Internet and, in particular, the empowerment of persons in vulnerable situations or marginalised groups, in both policy development and in the use of the Internet.
9. EMPHASISES the need to include cybersecurity in all digital investments in the coming years and SUPPORTS the Commission's plan to increase public spending and leverage private investment in the cybersecurity domain, taking into account the prospective increase in the number of sectors to which the Directive on measures for a high common level of cybersecurity across the Union (NIS Directive 2.0) will apply. HIGHLIGHTS the importance of Small and Medium Sized Enterprises (SMEs) in the cybersecurity ecosystem and RECOGNISES the relevant financial instruments available to support a cybersecurity digital transformation over the 2021-2027 Multiannual Financial Framework (MFF) as well as in the Recovery and Resilience Facility.

Commented [A118]: What is meant by development of standards within the EU? What kind of standards are we talking about? Can you please elaborate on this?

10. LOOKS FORWARD to the rapid implementation of the Regulation on Cybersecurity Industrial, Technology and Research Competence Centre and Network of Coordination Centres (CCCN) with a view to maximising the effects of investments to strengthen the Union's leadership in the field of cybersecurity, to support technological capacities and skills and to increase the Union's global competitiveness with input from industry and academic communities in cybersecurity, which should be brought into a more systematic collaboration.
11. REITERATES the need to explore the scope of a possible horizontal Union legal act, including for market access, which the Commission may be invited to propose in order to address all relevant aspects of cybersecurity of connected objects and its links with the cybersecurity certification framework under the Cybersecurity Act (CSA), as well as any other product specific instruments, in order to ensure adequate synergies, while avoiding inconsistencies or duplication.
12. ACKNOWLEDGES the importance of a harmonised approach on cybersecurity in the Union, while fully respecting Member States' competences, and WELCOMES the new proposal for a Directive on measures for a high common level of cybersecurity across the Union (NIS Directive 2.0) that builds upon the NIS Directive as an evolution of the efforts undertaken and which has contributed to strengthening and harmonising national cybersecurity frameworks and promoted cooperation between Member States. Furthermore, RECOGNISES the need for close alignment with other sectorial legislation in this domain.
13. TAKES NOTE of the Commission's proposal to support Member States in strengthening their national Security Operation Centres (SOCs) and to build a network of SOCs across the EU, to detect signals of attacks on networks and enable responses before harm is done. LOOKS FORWARD to exploring this network's potential to strengthen SOCs as well as their complementarity and coordination with existing networks and actors (for instance CSIRTs Network, ENISA and CERT-EU), including within the scope of the EU's cyber crisis management framework, in order to promote an efficient, secure and reliable information-sharing culture. Within this process, the best use should be made of the work carried out in the context of Artificial Intelligence and High Performance Computing initiatives and by European Digital Innovation Hubs, as well as the entire electronic communications infrastructure ~~such as land and submarine network systems~~.
14. TAKES NOTE of the possible development of an ultra-secure connectivity system, building on the Euro quantum communication infrastructure (QCI) and EUGOVSAATCOM, and COMMENDS that it be based on a robust cybersecurity framework.

Commented [A119]: This part doesn't belong here.

Commented [A120]: What is a practical difference between secure and ultra-secure. Maybe "more secure" could be a better alternative.

15. 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 its operators in guaranteeing that the Internet remains globally accessible and non-fragmented. RECOGNISES that an alternative European service for accessing the global internet ("DNS4EU" initiative), based on a transparent model which conforms to the latest security and data protection and privacy by design and by default standards and rules, can contribute to increased resilience.

16. 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 to increase the overall level of security, resilience and openness of the global internet, while increasing the competitiveness of the EU industry and in particular of the internet infrastructure operators.

Commented [A121]: Strong support for this paragraph.

17. 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 Cybersecurity Strategy and as based on the review of the Commission's recommendation on the security of 5G networks Report assessing the impacts of the Commission Recommendations of 26 March 2019 on the Cybersecurity 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. URGES Member States to continue 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 its strong commitment to applying the EU 5G Toolbox, including relevant restrictions on high-risk suppliers for key assets defined as critical and sensitive in the EU coordinated risk assessments and to continuing efforts made to guarantee the cybersecurity of 5G networks.

Commented [A122]: The scope is unclear.

Commented [A123]: There has been only 1 EU risk assessment. Or here are also meant national assessments?

Commented [A124]: Scope of the toolbox doesn't include only cybersecurity but wider security aspects.

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

Commented [A125]: As we haven't agreed on JCU establishment, we can't talk about implementation.

19. ~~As highlighted by the impact of the COVID-19 pandemic,~~ STRESSES the importance of promoting cooperation and exchange between cybersecurity actors and law enforcement and judicial authorities and the need to expand and improve the capacity of ~~these authorities to investigate cybercrime, while fully respecting fundamental rights and striving to ensure the requisite balance between various rights and interests, in particular privacy and security.~~

Commented [A126]: This issue has been important already before COVID19, therefore either delete "As highlighted by the impact of the COVID19 pandemic" or change wording so that COVID 19 is one of things that highlighted this issue.

20. 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 citizens, governments, industry and society and, at the same time, the need to ensure the ability of the competent law enforcement and judicial authorities to exercise their lawful powers, both online and offline, to protect our societies and citizens.

Commented [A127]: "judicial authorities" does not investigate cybercrime, therefore we propose to change wording to:

"(...) and the need to expand and improve the capacity of law enforcement authorities to investigate cybercrime (...)"

or

"(...) and the need to expand and improve the capacity of law enforcement and judicial authorities to investigate and prosecute cybercrime (...)"

21. CONTINUES to support and promote the Budapest Convention on Cybercrime, and the ongoing work on the Second Additional Protocol to that Convention. Furthermore, will continue to engage in multilateral exchanges on cybercrime to ensure the respect of human rights and fundamental freedoms.

Commented [A128]: We agree with the principles in this text, however it does not fully belong here. The main aim of Judicial authorities is not the balancing of different interests and rights.

22. 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 INTCECEN's work, including by exploring the establishment of an EU Cyber Intelligence Working Group.

Commented [A129]: Please correct this paragraph in accordance with Council resolution on encryption (13084/1/20).

In the Council resolution "citizens" are not specifically mentioned and instead of "law enforcement and judicial authorities" formulation "competent authorities in the area of security and criminal justice, e.g. law enforcement and judicial authorities" (which is wider in its scope) is used.

23. HIGHLIGHTS the importance of a robust and consistent security framework to better protect all EU personnel, data, information, communication networks 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 classified and non-classified EU networks while ensuring that sufficient resources are available. WELCOMES, in this context, the ongoing interinstitutional discussions on the establishment of common rules on information security and cybersecurity for all EU institutions, bodies, offices and agencies and INVITES to consider a comprehensive overview on how to enhance the cybersecurity of EU institutions, bodies and agencies, including necessary improvements in the governance and to develop secure information channels with MS.

Commented [A130]: We propose to increase the scope and talk not only about rules, but governance of cybersecurity in EU institutions.

24. BUILDING ON the EU's cyber diplomacy efforts, COMMITTS itself to increasing the effectiveness and the efficiency of the EU Cyber Diplomacy Toolbox and LOOKS FORWARD to deepening discussions building on lessons learned from the application of this instrument to date. These discussions should aim at building a notion of shared security at international level by strengthening prevention, cooperation and advancing confidence and capacity building and, where necessary, imposinge restrictions, thereby contributing to the EU's security and integrity 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 affecting our critical infrastructure, democratic institutions and processes, as well as to countering cyberattacks on supply chain-attacks with systemic effects and cyber-enabled theft of intellectual property.

25. In order to contribute to a global, secure, stable, free and open 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, contributing to the respect for international law in cyberspace and adherence to the norms, rules and principles of responsible state behaviour in cyberspace, for instance 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 outcome of both the current UN GGE and OEWG processes.

26. RECALLS its strong commitment to multilateralism aimed at strengthening cooperation and coordination with international and regional organisations, namely the United Nations, the Council of Europe, the OSCE, the OECD, NATO, 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 the UN Secretary General's Roadmap on digital cooperation. WELCOMES the proposal to establishment of 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 EU delegations and MS embassies on international cyber issues in order to strengthen coordinated outreach.

27. ACKNOWLEDGES the importance of strengthening cooperation with international partners, including with NATO, in order to advance the shared understanding of the cyber threat landscape, to develop cooperation mechanisms, to identify, where appropriate, cooperative diplomatic responses as well as to improve information-sharing, including through education, training and exercises. In particular, REAFFIRMS that a strong transatlantic partnership is vital to ensure and to contribute to our common security, stability and prosperity.

28. LOOK 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 security, crisis management and defence agenda, for instance 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 on setting up the Military CERT-Network by the European Defence Agency (EDA) and SUPPORTS efforts made to enhance synergies and coordination between the cybersecurity civilian, defence and space spheres, including through the dedicated PESCO projects.

Commented [A131]: There is some duplication with 27. Should be considered how to reduce that, for example by joining 26 and 27.p. and moving the part on cyberdiplomacy network after 27.p, or by creating subparagraphs a) more general on international organizations, b) on partnerships - NATO, transatlantic etc, c) on cyberdiplomacy network.

Commented [A132]: In 26 and 27 all organizations either should be in full names or in acronyms.

Commented [A133]: Why Pesco projects are highlighted above all other initiatives?

29. TAKES NOTE of the proposal to develop~~ment~~ of an EU External Cyber Capacity Building Agenda and the creation of an EU Cyber Capacity Building Board in order to increase cyber resilience and capacities worldwide. In this context, ENCOURAGES cooperation with Member States, as well as with public and private sector partners 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 Neighbourhood.

Commented [A134]: We would prefer not to mention any specific region.

30. 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 partners 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.

31. WELCOMES the comprehensive proposals presented in the Cybersecurity Strategy and ACKNOWLEDGES that ~~all of the~~ initiatives presented therein are important. In order to ensure ~~their seamless implementation~~ the implementation of agreed initiatives, and taking into account the multiannual character of some of these, ~~CONSIDERS it is necessary~~ PROPOSES to set the priorities with an accompanying and detailed implementation plan.

Commented [A135]: We don't agree to all of the initiatives, therefore doesn't consider all of them important.

Commented [A136]: We don't agree to implement all of the initiatives, therefore language should be softened.

32. MONITORS the progress in the implementation of these Conclusions by the means of an Action Plan to be adopted by the Council by The action plan would be regularly reviewed and updated by the Council in cooperation with the European Commission and the High Representative.

Commented [A137]: Support the idea of implementation plan/action plan and monitoring of the progress. The question is how to adjust p.31. and 32. To make more clear distinction between different involved actors and their responsibilities.

LITHUANIA

The Council of the European Union,

RECALLING its conclusions on:

- the Joint Communication to the European Parliament and the Council on the Cybersecurity Strategy for the European Union: "An Open, Safe and Secure Cyberspace",
- on Internet Governance,
- the Joint Communication to the European Parliament and the Council: "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU",
- cybersecurity capability and cyber capacity building in the EU,
 - the significance of 5G to the European Economy and the need to mitigate security risks linked to 5G [The 5G cybersecurity Toolbox],
- the future of a highly digitised Europe beyond 2020: "Boosting digital and economic competitiveness across the Union and digital cohesion",
- shaping Europe's Digital Future,
- complementary efforts to enhance resilience and counter hybrid threats,
- strengthening resilience and countering hybrid threats, including countering disinformation in the context of the COVID-19 pandemic,
- Cyber Diplomacy,
- on EU Coordinated Response to Large-Scale Cybersecurity Incidents and Crises
- a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox"),
- EU External Cyber Capacity Building Guidelines,
- the cybersecurity of connected devices,
- and its Council Resolution on Encryption - Security through encryption and security despite encryption.

RECALLING the European Council Conclusions on COVID-19, the Single Market, industry policy, digital and external relations and those on disinformation and hybrid threats,

RECALLING the Global Strategy for the European Union's Foreign and Security Policy,

RECALLING the Communications of the European Commission on shaping Europe's Digital Future and on the EU Security Union Strategy,

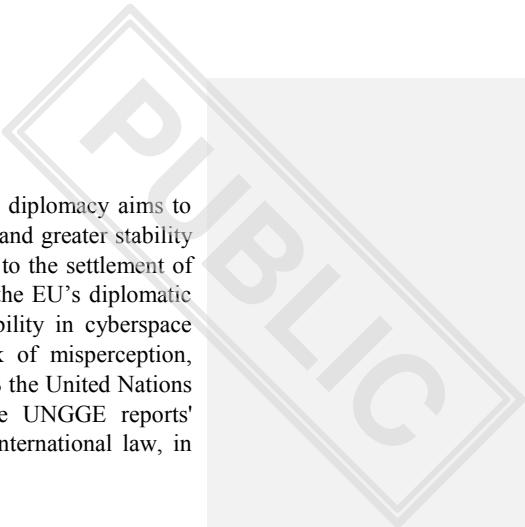
1. HIGHLIGHTS the fact that cybersecurity is essential for building a resilient, green and digital Europe and WELCOMES the Joint Communication to the European Parliament and the Council entitled "The EU's Cybersecurity Strategy for the Digital Decade", which outlines the new framework for the EU to protect its people, businesses and institutions from cyber threats while enhancing the trust of citizens and organisations in the EU's ability to promote secure and reliable digital tools and connectivity, and to promote and protect a global, stable, secure, free and open cyberspace, grounded in the rule of law, human rights, fundamental freedoms and democratic values.
2. RECOGNISING that the COVID-19 pandemic has brought trust in and security of Information and Communication Technology (ICT) tools and systems to the forefront of our daily lives, stresses that cybersecurity and the global and open Internet are vital for the functioning of our public administrations and institutions at both national and EU level, for teleworking, tele-education and doing business online and for society as a whole.
3. CALLS FOR the promotion and protection of the core EU values of democracy, human rights, fundamental freedoms including the freedom of expression, the right to free and equal access to information, the freedom of assembly and association, the right to privacy ~~and the protection against mass surveillance~~ and of the rule of law 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 its efforts to prevent the misuse of emerging technologies, notably through the use of diplomatic measures where necessary, as well as the export control of such technologies.
4. HIGHLIGHTS the importance of strengthening the EU's strategic autonomy, particularly its digital and technological leadership in the field of cybersecurity, while preserving an open economy. This can include diversifying production and supply chains, ensuring strategic stockpiling, fostering and attracting investments and production in Europe, exploring alternative solutions and circular models, and promoting broad industrial cooperation across Member States. In this respect, COMMITS itself to promoting the Union's autonomy on the basis of the development of a dynamic Industrial Strategy that supports EU value chains and secures the supply chains in particular in the most strategic domains, while ensuring that access to the single market is gained on fair and equitable terms and with respect for the Union's values.
5. Bearing in mind the shortage of cybersecurity skills in the workforce, STRESSES the importance of developing, retaining and attracting the best cybersecurity talent, for instance through education and training, and ENCOURAGES women's increased participation in science, technology, engineering, mathematics ('STEM') education and ICT jobs upskilling and reskilling in digital skills.

Commented [A138]: It is not sufficiently clear, what do we mean by using the term "mass surveillance" - concrete identified cases, actors or countries carrying out such activities. Moreover, protection against illegal surveillance is directly related to the protection of the right to privacy, therefore, we believe, there is no need to mention the surveillance separately.

Commented [A139]: Need for the clarification/identification of whose efforts it is meant in the text.

Commented [A140]: We suggest using agreed language from para 3 of the CC "A recovery advancing the transition towards a more dynamic, resilient and competitive European industry", 16 Nov. 2020.

Commented [A141]: Strong support.

- 
6. RECALLS that the common and comprehensive EU approach to cyber diplomacy aims to contribute to conflict prevention, the 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. REITERATES the United Nations General Assembly's call that UN Member States be guided by the UNGGE reports' recommendations in their use of ICT and notably the application of international law, in particular the UN Charter, in cyberspace.
7. REAFFIRMS that, with a view to shaping international standards in the areas of emerging technologies and core internet architecture so that these are in line with EU values and a multi-stakeholder approach, the further development of standards within the Union is essential: this will ensure that the Internet remains global, stable, secure, free and open and that digital technologies are human-centric, privacy-preserving, and that their use is lawful, safe and ethical. LOOKS FORWARD to the upcoming Standardisation Strategy and COMMITS itself to proactive and coordinated outreach to promote the EU's objectives at international level, including through cooperation with like-minded partners, civil society and the private sector.
8. STRONGLY SUPPORTS the multi-stakeholder model for Internet governance and commits itself to reinforcing regular and structured exchanges with stakeholders including the private sector, academia and civil society, in particular within the context of the Paris Call and in international fora. PROMOTES universal, affordable and equal access to the Internet and, in particular, the empowerment of persons in vulnerable situations or marginalised groups, in both policy development and in the use of the Internet.
9. EMPHASISES the need to include cybersecurity in all digital investments in the coming years and SUPPORTS the Commission's plan to increase public spending and leverage private investment in the cybersecurity domain, taking into account the prospective increase in the number of sectors to which the Directive on measures for a high common level of cybersecurity across the Union (NIS Directive 2.0) will apply. HIGHLIGHTS the importance of Small and Medium Sized Enterprises (SMEs) in the cybersecurity ecosystem and RECOGNISES the relevant financial instruments available to support a cybersecurity digital transformation over the 2021-2027 Multiannual Financial Framework (MFF) as well as in the Recovery and Resilience Facility.

10. LOOKS FORWARD to the rapid implementation of the Regulation on Cybersecurity Industrial, Technology and Research Competence Centre and Network of Coordination Centres (CCCN) with a view to maximising the effects of investments to strengthen the Union's leadership in the field of cybersecurity, to support technological capacities and skills and to increase the Union's global competitiveness with input from industry and academic communities in cybersecurity, which should be brought into a more systematic collaboration.
11. REITERATES the need to explore the scope of a possible horizontal Union legal act, including for market access, which the Commission may be invited to propose in order to address all relevant aspects of cybersecurity of connected objects and its links with the cybersecurity certification framework under the Cybersecurity Act (CSA), as well as any other product specific instruments, in order to ensure adequate synergies, while avoiding inconsistencies or duplication.
12. ACKNOWLEDGES the importance of a harmonised approach on cybersecurity in the Union, while fully respecting Member States' competences, and WELCOMES the new proposal for a Directive on measures for a high common level of cybersecurity across the Union (NIS Directive 2.0) that builds upon the NIS Directive as an evolution of the efforts undertaken and which has contributed to strengthening and harmonising national cybersecurity frameworks and promoted cooperation between Member States. Furthermore, RECOGNISES the need for close alignment with other sectorial legislation in this domain.
13. TAKES NOTE of the Commission's proposal to support Member States in strengthening their national Security Operation Centres (SOCs) and to build a network of SOCs across the EU, to detect signals of attacks on networks and enable responses before harm is done. LOOKS FORWARD to exploring this network's potential to strengthen SOCs as well as their complementarity and coordination with existing networks and actors (for instance CSIRTs Network, ENISA and CERT-EU), including within the scope of the EU's cyber crisis management framework, in order to promote an efficient, secure and reliable information-sharing culture. Within this process, the best use should be made of the work carried out in the context of Artificial Intelligence and High Performance Computing initiatives and by European Digital Innovation Hubs, as well as the entire electronic communications infrastructure such as land and submarine network systems.
14. TAKES NOTE of the possible development of an ultra-secure connectivity system, building on the Euro quantum communication infrastructure (QCI) and EUGOVSAATCOM, and COMMENDS that it be based on a robust cybersecurity framework.

15. 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 its operators in guaranteeing that the Internet remains globally accessible and non-fragmented. RECOGNISES that an alternative European service for accessing the global internet ("DNS4EU" initiative), based on a transparent model which conforms to the latest security and data protection and privacy by design and by default standards and rules, can contribute to increased resilience.
16. 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 to increase the overall level of security, resilience and openness of the global internet, while increasing the competitiveness of the EU industry and in particular of the internet infrastructure operators.
17. 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 Cybersecurity Strategy and as based on the review 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. URGES Member States to continue 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 its strong commitment to applying the EU 5G Toolbox, including relevant restrictions on high-risk suppliers for key assets defined as critical and sensitive in the EU coordinated risk assessments and to continuing efforts made to guarantee the cybersecurity of 5G networks.
18. RECOGNISES the relevance of integrating cybersecurity into EU crisis response mechanisms and STRESSES the importance of enhancing cooperation and information-sharing amongst the various cybersecurity communities within the EU and of linking the existing structures and procedures (such as the Blueprint, the CSIRT Network, the NIS Cooperation Group, CyCLONe, the European Cybercrime Centre, EU INTCEN and the IPCR) in case of large-scale cyber incidents and threats. TAKING INTO ACCOUNT the progress already achieved in this domain, LOOKS FORWARD to the Commission's proposal on the process, milestones and timeline for defining and implementing the Joint Cyber Unit (JCU) with a view to providing added value and streamlining the EU cybersecurity crisis management framework, including through preparedness, shared situational awareness, coordinated response and exercises, in a transparent and incremental manner while respecting the competences of the Member States and avoiding duplication and overlap with both Member States and EU existing structures and initiatives and respecting the competences of the Member States.

Commented [A142]: As relates the common situational awareness, duplication of mandates between JCU and EU IntCen should be avoided. Already continued and targeted exchanges on shared situational awareness take place and this is the main remit of IntCen. Central role should be left to EU IntCen in this regard and properly incorporated into the JCU activities. Threat assessment and a comprehensive situational awareness should be primarily developed by the EU IntCen and its Hybrid Fusion Cell (GAC Conclusions of 10 December, 2019, 12,21 and 22 paragraphs). Taking this into account, we believe, that current wording of the last sentence creates ambiguity and needs some specification.

19. As highlighted by the impact of the COVID-19 pandemic, STRESSES the importance of promoting cooperation and exchange between cybersecurity actors and law enforcement and judicial authorities and the need to expand and improve the capacity of these authorities to investigate cybercrime, while fully respecting fundamental rights and striving to ensure the requisite balance between various rights and interests, in particular privacy and security.

20. 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 citizens, governments, industry and society and, at the same time, the need to ensure the ability of the competent authorities in the area of security and criminal justice law enforcement and judicial authorities to exercise their lawful powers, both online and offline, to protect our societies and citizens.

Commented [A143]: Council recalls its Resolution on Encryption, therefore we believe that the agreed language (in 1, 3 and 5 sections of the resolution) should be used in this paragraph.

21. CONTINUES to support and promote the Budapest Convention on Cybercrime, and the ongoing work on the Second Additional Protocol to that Convention. Furthermore, will continue to engage in multilateral exchanges on cybercrime to ensure the respect of human rights and fundamental freedoms.

22. 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, including by exploring the establishment of an EU Cyber Intelligence Working Group. Furthermore, RECOGNISES the need to ensure appropriate level of INTCEN's resources including professional expertise.

Commented [A144]: As regards the invitation for the Member States to further contribute to IntCen and establishment of an EU Cyber Intelligence Group, we strongly believe, that it is equally important to emphasize the need to further enhance IntCen's analytical capabilities.

23. HIGHLIGHTS the importance of a robust and consistent security framework to better protect all EU personnel, data, information, communication networks 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 institutions, bodies and agencies against cyber threats and by developing strengthening classified and non-classified EU networks while ensuring that sufficient resources are available. WELCOMES, in this context, the ongoing interinstitutional discussions on the establishment of common rules on information security and cybersecurity for all EU institutions, bodies, offices and agencies.

Commented [A145]: We suggest using agreed language from para 10 of CC on resilience and hybrid threats, 15 Dec. 2020.

Commented [A146]: We would propose using "developing" instead of "strengthening", because it better reflects actual and undergoing process.

24. BUILDING ON the EU's cyber diplomacy efforts, COMMITTS itself to increasing the effectiveness and the efficiency of the EU Cyber Diplomacy Toolbox and LOOKS FORWARD to deepening discussions building on lessons learned from the application of this instrument to date. These discussions should aim at building a notion of shared security at international level by strengthening prevention, 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, where necessary, impose restrictions, thereby contributing to the EU's security and integrity and consolidating the EU's cyber posture, in full respect of national competences and prerogatives. In particular, special attention should be given to countering cyberattacks affecting our critical infrastructure, democratic institutions and processes, as well as to countering cyberattacks on supply chain attacks with systemic effects and cyber-enabled theft of intellectual property.

Commented [A147]: Implementation of the EU Cyber diplomacy toolbox and its measures is of utmost importance, respectively, we suggest to underline restrictive measures aim following the agreed language across various CCs and Declarations.

Commented [A148]: Technical correction.

25. In order to contribute to a global, secure, stable, free and open 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, contributing to the respect for international law in cyberspace and adherence to the norms, rules and principles of responsible state behaviour in cyberspace, for instance 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 outcome of both the current UN GGE and OEWG processes.

26. RECALLS its strong commitment to multilateralism aimed at strengthening cooperation and coordination with international and regional organisations, namely the United Nations, NATO, the Council of Europe, the OSCE, the OECD, NATO, 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 the UN Secretary General's Roadmap on digital cooperation. WELCOMES the establishment of 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 EU delegations and MS embassies on international cyber issues in order to strengthen coordinated outreach.

Commented [A149]: Recalling EU-NATO Joint Declarations and its strategic partnership, it is important to mention NATO after the UN.

27. ACKNOWLEDGES the importance of strengthening cooperation with NATO, in full respect of the principles of inclusiveness, reciprocity and decision-making autonomy of both organisations, and international-partner countries, including with NATO, 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, REAFFIRMS that a strong transatlantic partnership is vital to ensure and to contribute to our common security, stability and prosperity.

Commented [A150]: We suggest using agreed language from para 5 of CC on security and defence, 17 June 2019.

28. 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 security, crisis management and defence agenda, for instance in line with 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 on setting up the Military CERT-Network by the European Defence Agency (EDA) and SUPPORTS efforts made to enhance synergies and coordination between the cybersecurity civilian, defence and space spheres, including through the dedicated PESCO projects.

Commented [A151]: Strong support.

29. TAKES NOTE of the development of an EU External Cyber Capacity Building Agenda and the creation of an EU Cyber Capacity Building Board in order to increase cyber resilience and capacities worldwide. In this context, ENCOURAGES cooperation with Member States, as well as with public and private sector partners 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.

Commented [A152]: We propose to specify the notion of EU Neighbourhood and include its Eastern and Southern dimensions.

30. 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 partners 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.

31. WELCOMES the comprehensive proposals presented in the Cybersecurity Strategy and ACKNOWLEDGES that all of the initiatives presented therein are important. In order to ensure their seamless implementation, and taking into account the multiannual character of some of these, CONSIDERS it is necessary to set the priorities with an accompanying and detailed implementation plan.

32. MONITORS the progress in the implementation of these Conclusions by the means of an Action Plan to be adopted by the Council by The action plan would be regularly reviewed and updated by the Council in cooperation with the European Commission and the High Representative.

Commented [A153]: As regards to the Implementation and Action plans, we would call PT Presidency to provide with more clarified text proposal, specifying the responsibilities and goals of such plans.

MALTA

1 General Comment

The EU's Cybersecurity Strategy for Digital Decade, states that "the Commission and the High Representative, in line with their respective competences, will monitor progress under this strategy and develop criteria for evaluation. Inputs to this monitoring should include the reports from ENISA, and the Commission's regular Security Union reports." In this regard, Malta would appreciate having more details about this statement, and what does this imply for Member States. Will there be thresholds that are to be met? And if not met, what is the implication on Member States?

2 Specific Comments

Paragraph 9

Increasing the number of sectors under NIS02, increases the workload for the National Competent Authorities. Such an increase in the number of sectors and sub-sectors was expected and up to a certain extent, needed. Nonetheless, it is not clear why some of the additional sectors were added. This should be clarified during the article by article discussions on NIS 2.

Paragraph 12

Malta stresses that there is no 'One-Size-Fits-All' approach. The differences in size and population within Member States creates a problem for harmonisation. The responsibility for the identification and designation of critical entities (or essential and important categories of critical entities) should remain that of the Member States. In this regard, Malta considers that it is more beneficial to Member States to retain the current terms for the identification, designation and reporting thresholds of designated entities.

Paragraph 13

Malta considers that strengthening SOC's is important. Efforts to build a network of SOC's across the EU is also a positive attempt as it will strengthen collaboration and information sharing in good time, improving potential action to counter potential attacks.

Paragraph 17

Malta considers that improving and reinforcing the cybersecurity of 5G networks is imperative. timeframes.

NETHERLANDS

The Council of the European Union,

RECALLING its conclusions on:

- the Joint Communication to the European Parliament and the Council on the Cybersecurity Strategy for the European Union: "An Open, Safe and Secure Cyberspace",
- on Internet Governance,
- the Joint Communication to the European Parliament and the Council: "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU",
- cybersecurity capability and cyber capacity building in the EU,
 - the significance of 5G to the European Economy and the need to mitigate security risks linked to 5G [The 5G cybersecurity Toolbox],
- the future of a highly digitised Europe beyond 2020: "Boosting digital and economic competitiveness across the Union and digital cohesion",
- shaping Europe's Digital Future,
- complementary efforts to enhance resilience and counter hybrid threats,
- strengthening resilience and countering hybrid threats, including countering disinformation in the context of the COVID-19 pandemic,
- Cyber Diplomacy,
- on EU Coordinated Response to Large-Scale Cybersecurity Incidents and Crises
- a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox"),
- EU External Cyber Capacity Building Guidelines,
- the cybersecurity of connected devices,
- and its Council Resolution on Encryption - Security through encryption and security despite encryption.

RECALLING the European Council Conclusions on COVID-19, the Single Market, industry policy, digital and external relations and those on disinformation and hybrid threats,

RECALLING the Global Strategy for the European Union's Foreign and Security Policy,

RECALLING the Communications of the European Commission on shaping Europe's Digital Future and on the EU Security Union Strategy,

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 to protect its people, businesses and institutions from cyber threats while enhancing the trust of citizens and organisations in the EU's ability to promote secure and reliable network and information systems ~~digital tools~~ and connectivity, and to promote and protect a global, stable, secure, free and open cyberspace, grounded in the rule of law, human rights, fundamental freedoms and democratic values.

Commented [A154]: Does "institutions" refer to institutions at Union level or also to Member States?

Commented [A155]: In consistency with NIS.

2. RECOGNISING that the COVID-19 pandemic has brought the increased need for trust and security in network and information systems ~~Information and Communication Technology (ICT) tools and systems~~ to the forefront of our daily lives, stresses that cybersecurity and the global and open, free and secure Internet are vital for the functioning of our society and economy as a whole ~~public administrations and institutions at both national and EU level, for from~~ teleworking, tele-education and doing business online, ~~and for society as a whole.~~

Commented [A156]: The Covid-19 pandemic has shown us that all parts of society are dependent on ICT technologies, therefore we propose to refer to society as a whole, instead of focussing on public administrations and institutions.

3. CALLS FOR the promotion and protection of the core EU values of democracy, human rights, fundamental freedoms including the freedom of expression, the right to free and equal access to information, the freedom of assembly and association, the right to privacy and the protection against mass surveillance and of the rule of law 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 its efforts to prevent the misuse of emerging technologies, ~~notably through the use of diplomatic measures where necessary, as well as the export control of such technologies.~~

4. HIGHLIGHTS the importance of strengthening the EU's strategic autonomy, particularly its digital and technological leadership in the field of cybersecurity, while preserving an open economy. In this respect, COMMITS itself to promoting the Union's autonomy on the basis of the development of a dynamic Industrial Strategy that supports EU value chains and secures the trusted supply chains in particular in the most strategic domains, while ensuring that access to the single market is gained on fair and equitable terms and with respect for the Union's values.

5. Bearing in mind the shortage of cybersecurity skills in the workforce, STRESSES the importance of developing, retaining and attracting the best cybersecurity talent, for instance through education and training to be able to digitize our society in a cybersecure manner, and ENCOURAGES the workforce's, and in particular women's, increased participation in science, technology, engineering, mathematics ('STEM') education and ICT jobs upskilling and reskilling in digital skills.

~~5.~~

7. RECALLS that the common and comprehensive EU approach to cyber diplomacy aims to contribute to conflict prevention, the 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. REITERATES the United Nations General Assembly's call that UN Member States be guided by the UNGGE reports' recommendations in their use of ICT and notably the application of international law, in particular the UN Charter, in cyberspace.

8. REAFFIRMS that, with a view to shaping international standards in the areas of emerging technologies and ~~core internet architecture~~ the technical and logical infrastructure essential to the general availability or integrity of the public core of the Internet, so that these are in line with EU values and a multi-stakeholder approach, the further development of standards within the Union is essential: this will ensure that the Internet remains global, stable, secure, free and open and that digital technologies are human-centric, privacy-preserving, and that their use is lawful, safe and ethical. LOOKS FORWARD to the upcoming Standardisation Strategy and COMMITS itself to proactive and coordinated outreach to promote the EU's objectives at international level, including through cooperation with like-minded partners, civil society and the private sector.
9. STRONGLY SUPPORTS the multi-stakeholder model for Internet governance and commits itself to reinforcing regular and structured exchanges with stakeholders including the private sector, academia and civil society, in particular within the context of the Paris Call and in international fora. PROMOTES universal, affordable and equal access to the Internet and, in particular, the empowerment of persons in vulnerable situations or marginalised groups, in both policy development and in the use of the Internet.
10. EMPHASISES the need to include cybersecurity in all digital investments and initiatives in the coming years and SUPPORTS the Commission's plan to increase public spending and leverage private investment in the cybersecurity domain, taking into account the prospective increase in the number of sectors to which the Directive on measures for a high common level of cybersecurity across the Union (NIS Directive 2.0) will apply. HIGHLIGHTS the importance of Small and Medium Sized Enterprises (SMEs) in the cybersecurity ecosystem and RECOGNISES the relevant financial instruments available to support a cybersecurity digital transformation over the 2021-2027 Multiannual Financial Framework (MFF) as well as in the Recovery and Resilience Facility.

11. ~~LOOKS FORWARD to the rapid implementation of the Regulation on Cybersecurity Industrial, Technology and Research Competence Centre and Network of Coordination Centres (CCCN) with a view to maximising the effects of investments to strengthen the Union's leadership in the field of cybersecurity, to support technological capacities and skills and to increase the Union's global competitiveness with input from industry and academic communities in cybersecurity, which should be brought into a more systematic collaboration.~~

12. REITERATES the need to explore the scope of a possible horizontal Union legal act, including for market access, which the Commission may be invited to propose in order to address all relevant aspects of cybersecurity of connected ~~objects-devices~~ and its links with the cybersecurity certification framework under the Cybersecurity Act (CSA), as well as any other product specific instruments, in order to ensure adequate synergies, while avoiding inconsistencies or duplication.

13. ACKNOWLEDGES the importance of a ~~harmonised-comprehensive~~ approach on cybersecurity in the Union, while fully respecting Member States' competences and needs, and WELCOMES the new proposal for a Directive on measures for a high common level of cybersecurity across the Union (NIS Directive 2.0) that builds upon the NIS Directive ~~as an evolution of the efforts undertaken and~~ which has contributed to strengthening and harmonising national cybersecurity frameworks and promoted cooperation between Member States. WELCOMES the proposal in the NIS Directive 2.0 to establish a framework for Coordinated Vulnerability Disclosure and to require Member States to designate CSIRTs to act as trusted intermediaries and facilitate the interaction between the reporting entities and the manufacturers or providers of ICT products and ICT services. Furthermore, ~~RECOGNISES-EMPHASIZES~~ the need for close alignment with other sectorial legislation in this domain.

Commented [A157]: Unclear/ambiguous sentence.

14. TAKES NOTE of the Commission's proposal to support Member States in strengthening stimulating organisations, such as their national Security Operation Centres (SOCs) ~~and~~ to build a network of SOCs across the EU, to detect signals of attacks on networks and enable responses before harm is done. RECALLS the efforts undertaken by Member States, supported by the EU, to set up sectoral and regional CSIRTs and national or European ISACs as part of an effective network of cybersecurity partnerships in the Union. LOOKS FORWARD to exploring this network's potential to strengthen SOCs and CSIRTs as well as their complementarity and coordination with existing networks and actors, most notably (for instance) the CSIRTs Network, ENISA and CERT-EU, including within the scope of the EU's cyber crisis management framework, in order to promote an efficient, secure and reliable information-sharing culture. Within this process, the best use should be made of the work carried out in the context of Artificial Intelligence and High Performance Computing initiatives and by European Digital Innovation Hubs, as well as the entire electronic communications infrastructure such as land and submarine network systems.

Commented [A158]: It has not come apparent in the strategy that it would be mainly targeted to strengthen national (public) SOCs. It is our understanding that it is rather the stimulation of SOCs, being public and / or private and/or regional / sectoral.

Commented [A159]: We suggest deletion since ENISA and CERT-EU are part of the CSIRTs Network

Commented [A160]: We would suggest to refrain from linking SOCs to cyber crisis management, since this is more the merit of CSIRTs.

15. TAKES NOTE of the possible development of an ultra-secure connectivity system, building on the Euro quantum communication infrastructure (QCI) and EUGOVSAATCOM, and COMMENDS that it should be based on a robust cybersecurity framework.

16. 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 its operators in guaranteeing that the Internet remains globally accessible and non-fragmented. RECOGNISES WELCOMES further discussion on the option of that an alternative European service for accessing the global internet (“DNS4EU” initiative), based on a transparent model which conforms to the latest security and data protection and privacy by design and by default standards and rules, can in order to contribute to increased resilience.

Commented [A161]: To which operators is being referred to? Alternative wording: “to assess the role of the two EU DNS Root Server Operators when it comes to guaranteeing”

Commented [A162]: We will have to discuss the intention and implications before deciding on such a resolving service.

17. 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 to increase the overall level of security, resilience and openness of the global internet, while increasing the competitiveness of the EU industry and in particular of the internet infrastructure operators.

18. 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 Cybersecurity Strategy and as based on the review 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. URGES Member States to continue 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 its strong commitment to applying the EU 5G Toolbox, including relevant restrictions on high-risk suppliers for key assets defined as critical and sensitive in the EU coordinated risk assessments and to continuing efforts made to guarantee the cybersecurity of 5G networks.

19. RECOGNISES the relevance of integrating cybersecurity into EU crisis response mechanisms and STRESSES the importance of enhancing cooperation and information-sharing amongst the various cybersecurity communities within the EU and of linking the existing structures and procedures (such as the Blueprint, the CSIRT Network, the NIS Cooperation Group, CyCLONE, the European Cybercrime Centre, EU INCEN and the IPCR) in case of large-scale cyber incidents and threats. UNDERLINES that each Member State bears the primary responsibility for enhancing its own cybersecurity and ensuring its response to cyber incidents and crises while the EU can provide a strong added value in supporting the cooperation between the Member States. TAKING INTO ACCOUNT the progress already achieved in this domain, LOOKS FORWARD IS AWAITING to the Commission’s proposal on the process, milestones and timeline for defining and implementing 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, coordinated response and exercises, in a transparent and incremental manner while avoiding duplication and overlap and respecting the competences of the Member States.

Commented [A163]: Since this may conflict with member states’ competences, an alternative wording could be: supporting cooperation between member states for effective response

20. As highlighted by the impact of the COVID-19 pandemic, STRESSES the importance of promoting cooperation and exchange between relevant cybersecurity actors and competent authorities in the area of security and criminal justice, e.g. law enforcement and judicial authorities and the need to expand and improve the capacity of these authorities to investigate cybercrime, while fully respecting fundamental rights and striving to ensure the requisite balance between various rights and interests, in particular privacy and security.

21. 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 citizens, 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.

Commented [A164]: Similar to Council Conclusions on Encryption, November 24, 2020 (13084/1/20)

22. CONTINUES to support and promote the Budapest Convention on Cybercrime, and the ongoing work on the Second Additional Protocol to that Convention. Furthermore, will continue to engage in multilateral exchanges on cybercrime to ensure the exchange of best practices and technical knowledge and to safeguard the respect of human rights and fundamental freedoms.

23. 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~~ further enhance the work of EU INTCEN and its Hybrid Fusion Cell, also taking into account an appropriate level of resources including professional expertise, and including by exploring the possible establishment of an EU Cyber Intelligence Working Group within EU INTCEN.

24. HIGHLIGHTS the importance of a robust and consistent security framework to better protect all EU personnel, data, information, communication networks 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 classified and non-classified EU networks while ensuring that sufficient resources are available. WELCOMES, in this context, the ongoing interinstitutional discussions on the establishment of common rules on information security and cybersecurity for all EU institutions, bodies, offices and agencies, and STRESSES the need for swift implementation of these rules.

25. ACKNOWLEDGES the importance of CERT-EU having an adequate and stable level of resources to fulfil its objectives as stated in its current mandate. TAKES NOTE of the wish of the Commission to strengthen the mandate of CERT-EU, while LOOKING FORWARD to further explanation and discussion on the goals of such a proposed strengthening of the mandate.

~~24.26.~~ BUILDING ON the EU's cyber diplomacy efforts, COMMITS itself to increasing the effectiveness and the efficiency of the EU Cyber Diplomacy Toolbox and LOOKS FORWARD to deepening discussions building on lessons learned from the application of

this instrument to date. These discussions should aim at ~~building a notion of shared security at international level by strengthening prevention, cooperation and advancing confidence and capacity building and, where necessary, impose restrictions,~~ strengthening the EU's capability to use all CFSP measures, including restrictive measures if necessary, 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 the EU's security and integrity and consolidating the EU's cyber posture, in full respect of national competences and prerogatives. In particular, special attention should be given to countering cyberattacks affecting our critical infrastructure, undermining our economic security, democratic institutions and processes, as well as to countering cyberattacks on supply chains ~~s-attacks~~ with systemic effects and cyber-enabled theft of intellectual property.

25-27. In order to contribute to a global, secure, stable, free and open cyberspace, which is of ever-increasing importance for the continued prosperity, growth, security, well-being, connectivity and integrity of our societies, COMMITTS itself to continuous engagement in norm-setting processes in international organisations, especially in the UN first-committee related processes, contributing to the respect for international law in cyberspace and adherence to the norms, rules and principles of responsible state behaviour in cyberspace, for instance 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 outcome of both the current UN GGE and OEWG processes.

26-28. RECALLS its strong commitment to multilateralism aimed at strengthening cooperation and coordination with international and regional organisations, namely the United Nations, the Council of Europe, the OSCE, the OECD, NATO, 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 the UN Secretary General's Roadmap on digital cooperation. WELCOMES the establishment of 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 EU delegations and MS embassies on international cyber issues in order to strengthen coordinated outreach.

27-29. ACKNOWLEDGES the importance of strengthening cooperation with international partners, including with NATO, in order to advance the shared understanding of the cyber threat landscape, to develop cooperation mechanisms, to identify, where appropriate, cooperative diplomatic responses as well as to improve information-sharing, including through education, training and exercises. In particular, REAFFIRMS that a strong transatlantic partnership is vital to ensure and to contribute to our common security, stability and prosperity.

28-30. LOOKS FORWARD TO the forthcoming proposal for a review of the Cyber Defence Policy Framework (CDPF), and COMMITTS itself to pursuing efforts to strengthen cybersecurity and cyber defence dimensions with a view to ensuring that these are fully integrated into the wider security, crisis management and defence agenda, for instance 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 on setting up the Military CERT-Network by the European Defence Agency (EDA) and SUPPORTS efforts made to enhance synergies and coordination between the cybersecurity civilian, defence and space spheres, including through the dedicated PESCO projects.

~~29-31.~~ RECALLS that cyber capacity building is one of the most important topics on the international cyber policy agenda, as demonstrated in relevant outcome documents, EMPHASIZES the need to mobilise the collective expertise of EU Member States for EU-funded external cyber capacity building programmes, support effective coordination of EU-funded external cyber capacity building activities, and increase training opportunities in light of proliferating initiatives in partner countries and regions and the growing demand for cyber-related training, notably by cooperating with and complementing the GFCE network.

Commented [A165]: With reference to Council Conclusions 26/6/2018 "EU External Cyber Capacity Building Guidelines", paragraphs 9 & 27

~~30-32.~~ TAKES NOTE of the development of an EU External Cyber Capacity Building Agenda and the creation of an EU Cyber Capacity Building Board in order to increase cyber resilience and capacities worldwide. In this context, ENCOURAGES cooperation with Member States, as well as with public and private sector partners, the 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 Neighbourhood.

~~31-33.~~ 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 partners 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.

~~32-34.~~ WELCOMES the comprehensive proposals presented in the Cybersecurity Strategy and ACKNOWLEDGES ~~that all of the~~ initiatives presented therein ~~are important could contribute to building strong cybersecurity for the EU~~. In order to ~~ensure their seamless determine their possible~~ implementation, and taking into account the multiannual character of some of these, CONSIDERS it is necessary to set the priorities with an accompanying and detailed implementation plan.

~~33-35.~~ MONITORS the progress in the implementation of these Conclusions by the means of an Action Plan to be adopted by the Council by The action plan would be regularly reviewed and updated by the Council in cooperation with the European Commission and the High Representative.

ROMANIA

Romanian comments

The Council of the European Union,

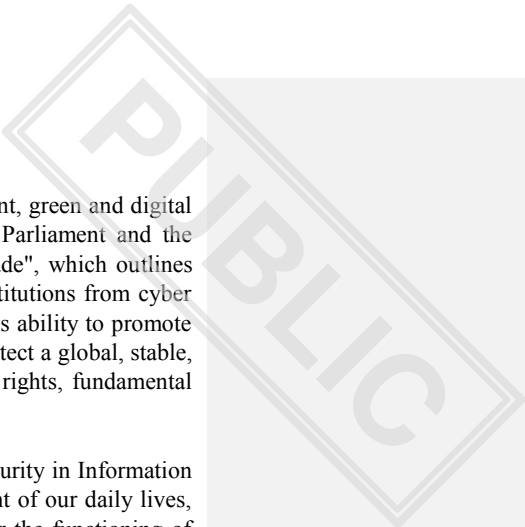
RECALLING its conclusions on:

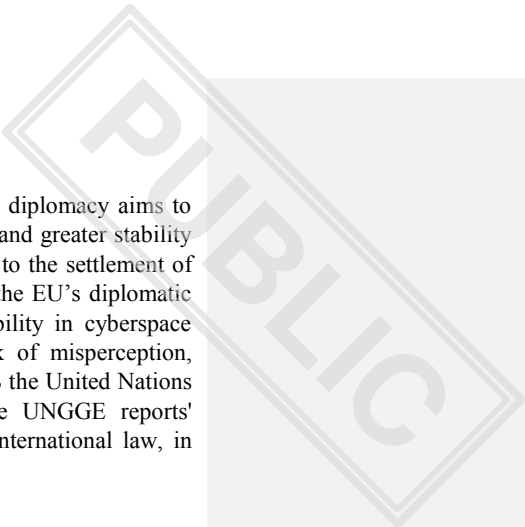
- the Joint Communication to the European Parliament and the Council on the Cybersecurity Strategy for the European Union: "An Open, Safe and Secure Cyberspace",
- on Internet Governance,
- the Joint Communication to the European Parliament and the Council: "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU",
- cybersecurity capability and cyber capacity building in the EU,
- the significance of 5G to the European Economy and the need to mitigate security risks linked to 5G [The 5G cybersecurity Toolbox],
- the future of a highly digitised Europe beyond 2020: "Boosting digital and economic competitiveness across the Union and digital cohesion",
- shaping Europe's Digital Future,
- complementary efforts to enhance resilience and counter hybrid threats,
- strengthening resilience and countering hybrid threats, including countering disinformation in the context of the COVID-19 pandemic,
- Cyber Diplomacy,
- on EU Coordinated Response to Large-Scale Cybersecurity Incidents and Crises
- a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox"),
- EU External Cyber Capacity Building Guidelines,
- the cybersecurity of connected devices,
- and its Council Resolution on Encryption - Security through encryption and security despite encryption.

RECALLING the European Council Conclusions on COVID-19, the Single Market, industry policy, digital and external relations and those on disinformation and hybrid threats,

RECALLING the Global Strategy for the European Union's Foreign and Security Policy,

RECALLING the Communications of the European Commission on shaping Europe's Digital Future and on the EU Security Union Strategy,

- 
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 to protect its people, businesses and institutions from cyber threats while enhancing the trust of citizens and organisations in the EU's ability to promote secure and reliable digital tools and connectivity, and to promote and protect a global, stable, secure, free and open cyberspace, grounded in the rule of law, human rights, fundamental freedoms and democratic values.
 2. RECOGNISING that the COVID-19 pandemic has brought trust and security in Information and Communication Technology (ICT) tools and systems to the forefront of our daily lives, stresses that cybersecurity and the global and open Internet are vital for the functioning of our public administrations and institutions at both national and EU level, for teleworking, tele-education and doing business online and for society as a whole.
 3. CALLS FOR the promotion and protection of the core EU values of democracy, human rights, fundamental freedoms including the freedom of expression, the right to free and equal access to information, the freedom of assembly and association, the right to privacy and the protection against mass surveillance and of the rule of law 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 its efforts to prevent the misuse of emerging technologies, notably through the use of diplomatic measures where necessary, as well as the export control of such technologies.
 4. HIGHLIGHTS the importance of strengthening the EU's strategic autonomy, particularly its digital and technological leadership in the field of cybersecurity, while preserving an open economy. In this respect, COMMITS itself to promoting the Union's autonomy on the basis of the development of a dynamic Industrial Strategy that supports EU value chains and secures the supply chains in particular in the most strategic domains, while ensuring that access to the single market is gained on fair and equitable terms and with respect for the Union's values.
 5. Bearing in mind the shortage of cybersecurity skills in the workforce, STRESSES the importance of developing, retaining and attracting the best cybersecurity talent, for instance through education and training, and ENCOURAGES women's increased participation in science, technology, engineering, mathematics ('STEM') education and ICT jobs upskilling and reskilling in digital skills.

- 
6. RECALLS that the common and comprehensive EU approach to cyber diplomacy aims to contribute to conflict prevention, the 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. REITERATES the United Nations General Assembly's call that UN Member States be guided by the UNGGE reports' recommendations in their use of ICT and notably the application of international law, in particular the UN Charter, in cyberspace.
7. REAFFIRMS that, with a view to shaping international standards in the areas of emerging technologies and core internet architecture so that these are in line with EU values and a multi-stakeholder approach, the further development of standards within the Union is essential: this will ensure that the Internet remains global, stable, secure, free and open and that digital technologies are human-centric, privacy-preserving, and that their use is lawful, safe and ethical. LOOKS FORWARD to the upcoming Standardisation Strategy and COMMITS itself to proactive and coordinated outreach to promote the EU's objectives at international level, including through cooperation with like-minded partners, civil society and the private sector.
8. STRONGLY SUPPORTS the multi-stakeholder model for Internet governance and commits itself to reinforcing regular and structured exchanges with stakeholders including the private sector, academia and civil society, in particular within the context of the Paris Call and in international fora. PROMOTES universal, affordable and equal access to the Internet and, in particular, the empowerment of persons in vulnerable situations or marginalised groups, in both policy development and in the use of the Internet.
9. EMPHASISES the need to include cybersecurity in all digital investments in the coming years and SUPPORTS the Commission's plan to increase public spending and leverage private investment in the cybersecurity domain, taking into account the prospective increase in the number of sectors to which the Directive on measures for a high common level of cybersecurity across the Union (NIS Directive 2.0) will apply. HIGHLIGHTS the importance of Small and Medium Sized Enterprises (SMEs) in the cybersecurity ecosystem and RECOGNISES the relevant financial instruments available to support a cybersecurity digital transformation over the 2021-2027 Multiannual Financial Framework (MFF) as well as in the Recovery and Resilience Facility.

10. LOOKS FORWARD to the rapid implementation of the Regulation on Cybersecurity Industrial, Technology and Research Competence Centre and Network of Coordination Centres (CCCN), including the rapid set up and operationalisation of the cybersecurity competence centre in Bucharest, with a view to maximising the effects of investments to strengthen the Union's leadership in the field of cybersecurity, to support technological capacities and skills and to increase the Union's global competitiveness with input from industry and academic communities in cybersecurity, which should be brought into a more systematic collaboration.
11. REITERATES the need to explore the scope of a possible horizontal Union legal act, including for market access, which the Commission may be invited to propose in order to address all relevant aspects of cybersecurity of connected objects and its links with the cybersecurity certification framework under the Cybersecurity Act (CSA), as well as any other product specific instruments, in order to ensure adequate synergies, while avoiding inconsistencies or duplication.
12. ACKNOWLEDGES the importance of a harmonised approach on cybersecurity in the Union, while fully respecting Member States' competences, and WELCOMES the new proposal for a Directive on measures for a high common level of cybersecurity across the Union (NIS Directive 2.0) that builds upon the NIS Directive as an evolution of the efforts undertaken and which has contributed to strengthening and harmonising national cybersecurity frameworks and promoted cooperation between Member States. Furthermore, RECOGNISES the need for close alignment with other sectorial legislation in this domain.
13. TAKES NOTE of the Commission's proposal to support Member States in strengthening their national Security Operation Centres (SOCs) and to build a network of SOCs across the EU, to detect signals of attacks on networks and enable responses before harm is done. LOOKS FORWARD to exploring this network's potential to strengthen SOCs as well as their complementarity and coordination with existing networks and actors (for instance CSIRTs Network, ENISA and CERT-EU), including within the scope of the EU's cyber crisis management framework, in order to promote an efficient, secure and reliable information-sharing culture. Within this process, the best use should be made of the work carried out in the context of Artificial Intelligence and High Performance Computing initiatives and by European Digital Innovation Hubs, as well as the entire electronic communications infrastructure such as land and submarine network systems.
14. TAKES NOTE of the possible development of an ultra-secure connectivity system, building on the Euro quantum communication infrastructure (QCI) and EUGOVSAATCOM, and COMMENDS that it be based on a robust cybersecurity framework.

15. 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 its operators in guaranteeing that the Internet remains globally accessible and non-fragmented. RECOGNISES that an alternative European service for accessing the global internet ("DNS4EU" initiative), based on a transparent model which conforms to the latest security and data protection and privacy by design and by default standards and rules, can contribute to increased resilience.
16. 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 to increase the overall level of security, resilience and openness of the global internet, while increasing the competitiveness of the EU industry and in particular of the internet infrastructure operators.
17. 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 Cybersecurity Strategy and as based on the review 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. URGES Member States to continue 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 its strong commitment to applying the EU 5G Toolbox, including relevant restrictions on high-risk suppliers for key assets defined as critical and sensitive in the EU coordinated risk assessments and to continuing efforts made to guarantee the cybersecurity of 5G networks.
18. RECOGNISES the relevance of integrating cybersecurity into EU crisis response mechanisms and STRESSES the importance of enhancing cooperation and information-sharing amongst the various cybersecurity communities within the EU and of linking the existing structures and procedures (such as the Blueprint, the CSIRT Network, the NIS Cooperation Group, CyCLONe, the European Cybercrime Centre, EU INCEN and the IPCR) in case of large-scale cyber incidents and threats. TAKING INTO ACCOUNT the progress already achieved in this domain, LOOKS FORWARD to the Commission's proposal on the process, milestones and timeline for defining and implementing the Joint Cyber Unit (JCU) with a view to providing added value and streamlining the EU cybersecurity crisis management framework, including through preparedness, shared situational awareness, coordinated response and exercises, in a transparent and incremental manner while avoiding duplication and overlap and respecting the competences of the Member States.

19. As highlighted by the impact of the COVID-19 pandemic, STRESSES the importance of promoting cooperation and exchange between cybersecurity actors and law enforcement and judicial authorities and the need to expand and improve the capacity of these authorities to investigate cybercrime, while fully respecting fundamental rights and striving to ensure the requisite balance between various rights and interests, in particular privacy and security.
20. 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 citizens, governments, industry and society and, at the same time, the need to ensure the ability of the authorities in the area of security and criminal justice, e.g. competent law enforcement and judicial authorities to exercise their lawful powers, both online and offline, to protect our societies and citizens.
21. CONTINUES to support and promote the Budapest Convention on Cybercrime, and the ongoing work on the Second Additional Protocol to that Convention. Furthermore, will continue to engage in multilateral exchanges on cybercrime to ensure the respect of human rights and fundamental freedoms.
22. 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 INCEN's work, including by exploring the establishment of an EU Cyber Intelligence Working Group.
23. HIGHLIGHTS the importance of a robust and consistent security framework to better protect all EU personnel, data, information, communication networks 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 classified and non-classified EU networks while ensuring that sufficient resources are available. WELCOMES, in this context, the ongoing interinstitutional discussions on the establishment of common rules on information security and cybersecurity for all EU institutions, bodies, offices and agencies.
24. BUILDING ON the EU's cyber diplomacy efforts, COMMITS itself to increasing the effectiveness and the efficiency of the EU Cyber Diplomacy Toolbox and LOOKS FORWARD to deepening discussions building on lessons learned from the application of this instrument to date. These discussions should aim at building a notion of shared security at international level by strengthening prevention, cooperation and advancing confidence and capacity building and, where necessary, impose restrictions, thereby contributing to the EU's security and integrity and consolidating the EU's cyber posture, in full respect of national competences and prerogatives. In particular, special attention should be given to countering cyberattacks affecting our critical infrastructure, democratic institutions and processes, as well as to countering cyberattacks on supply chain-attacks with systemic effects and cyber-enabled theft of intellectual property.

25. In order to contribute to a global, secure, stable, free and open 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, contributing to the respect for international law in cyberspace and adherence to the norms, rules and principles of responsible state behaviour in cyberspace, for instance 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 outcome of both the current UN GGE and OEWG processes.
26. RECALLS its strong commitment to multilateralism aimed at strengthening cooperation and coordination with international and regional organisations, namely the United Nations, the Council of Europe, the OSCE, the OECD, NATO, 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 the UN Secretary General's Roadmap on digital cooperation. WELCOMES the establishment of 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 EU delegations and MS embassies on international cyber issues in order to strengthen coordinated outreach.
27. ACKNOWLEDGES the importance of strengthening cooperation with international partners, including with NATO, in order to advance the shared understanding of the cyber threat landscape, to develop cooperation mechanisms, to identify, where appropriate, cooperative diplomatic responses as well as to improve information-sharing, including through education, training and exercises. In particular, REAFFIRMS that a strong transatlantic partnership is vital to ensure and to contribute to our common security, stability and prosperity.
28. LOOK 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 security, crisis management and defence agenda, for instance 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 on setting up the Military CERT-Network by the European Defence Agency (EDA) and SUPPORTS efforts made to enhance synergies and coordination between the cybersecurity civilian, defence and space spheres, including through the dedicated PESCO projects.

29. TAKES NOTE of the development of an EU External Cyber Capacity Building Agenda and the creation of an EU Cyber Capacity Building Board in order to increase cyber resilience and capacities worldwide. In this context, ENCOURAGES cooperation with Member States, as well as with public and private sector partners 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 Neighbourhood.
30. 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 partners 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.
31. WELCOMES the comprehensive proposals presented in the Cybersecurity Strategy and ACKNOWLEDGES that all of the initiatives presented therein are important. In order to ensure their seamless implementation, and taking into account the multiannual character of some of these, CONSIDERS it is necessary to set the priorities with an accompanying and detailed implementation plan.
32. MONITORS the progress in the implementation of these Conclusions by the means of an Action Plan to be adopted by the Council by The action plan would be regularly reviewed and updated by the Council in cooperation with the European Commission and the High Representative.
-

ANNEX

SPAIN

The Council of the European Union,

RECALLING its conclusions on:

- the Joint Communication to the European Parliament and the Council on the Cybersecurity Strategy for the European Union: "An Open, Safe and Secure Cyberspace",
- on Internet Governance,
- the Joint Communication to the European Parliament and the Council: "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU",
- cybersecurity capability and cyber capacity building in the EU,
 - the significance of 5G to the European Economy and the need to mitigate security risks linked to 5G [The 5G cybersecurity Toolbox],
- the future of a highly digitised Europe beyond 2020: "Boosting digital and economic competitiveness across the Union and digital cohesion",
- shaping Europe's Digital Future,
- complementary efforts to enhance resilience and counter hybrid threats,
- strengthening resilience and countering hybrid threats, including countering disinformation in the context of the COVID-19 pandemic,
- Cyber Diplomacy,
- on EU Coordinated Response to Large-Scale Cybersecurity Incidents and Crises
- a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox"),
- EU External Cyber Capacity Building Guidelines,
- the cybersecurity of connected devices,
- and its Council Resolution on Encryption - Security through encryption and security despite encryption.

RECALLING the European Council Conclusions on COVID-19, the Single Market, industry policy, digital and external relations and those on disinformation and hybrid threats,

RECALLING the Global Strategy for the European Union's Foreign and Security Policy,

RECALLING the Communications of the European Commission on shaping Europe's Digital Future and on the EU Security Union Strategy,

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 to protect its people, businesses and institutions from cyber threats while enhancing the trust of citizens and organisations in the EU's ability to promote secure and reliable digital tools and connectivity, and to promote and protect a global, stable, secure, free and open cyberspace, grounded in the rule of law, human rights, fundamental freedoms and democratic values.
2. RECOGNISING that the COVID-19 pandemic has brought trust and security in Information and Communication Technology (ICT) tools and systems to the forefront of our daily lives, stresses that cybersecurity and the global and open Internet are vital for the functioning of our public administrations and institutions at both national and EU level, for teleworking, tele-education and doing business online and for society as a whole.
3. CALLS FOR the promotion and protection of the core EU values of democracy, human rights, fundamental freedoms including the freedom of expression, the right to free and equal access to information, the freedom of assembly and association, the right to privacy and the protection against mass surveillance and of the rule of law 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 its efforts to prevent the misuse of emerging technologies, notably through the use of diplomatic measures where necessary, as well as the export control of such technologies.
4. HIGHLIGHTS the importance of strengthening the EU's strategic autonomy, particularly its digital and technological leadership in the field of cybersecurity, while preserving an open economy and reducing market dependence from other geographical areas. In this respect, COMMITS itself to promoting the Union's autonomy on the basis of the development of a dynamic Industrial Strategy that supports EU value chains and secures the supply chains in particular in the most strategic domains, while ensuring that access to the single market is gained on fair and equitable terms and with respect for the Union's values.
5. Bearing in mind the shortage of cybersecurity skills in the workforce, STRESSES the importance of developing, retaining and attracting the best cybersecurity talent, for instance through education and training, and ENCOURAGES women's increased participation in science, technology, engineering, mathematics ('STEM') education and ICT jobs upskilling and reskilling in digital skills.

Commented [A166]: ES

6. RECALLS that the common and comprehensive EU approach to cyber diplomacy aims to contribute to conflict prevention, the 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. REITERATES the United Nations General Assembly's call that UN Member States be guided by the UNGGE reports' recommendations in their use of ICT and notably the application of international law, in particular the UN Charter, in cyberspace.
7. REAFFIRMS that, with a view to shaping international standards in the areas of emerging technologies and core internet architecture so that these are in line with EU values and a multi-stakeholder approach, the further development of standards within the Union is essential: this will ensure that the Internet remains global, stable, secure, free and open and that digital technologies are human-centric, privacy-preserving, and that their use is lawful, safe and ethical. LOOKS FORWARD to the upcoming Standardisation Strategy and COMMITS itself to proactive and coordinated outreach to promote the EU's objectives at international level, including through cooperation with like-minded partners, civil society and the private sector.
8. STRONGLY SUPPORTS the multi-stakeholder model for Internet governance and commits itself to reinforcing regular and structured exchanges with stakeholders including the private sector, academia and civil society, in particular within the context of the Paris Call and in international fora. PROMOTES universal, affordable and equal access to the Internet and, in particular, the empowerment of persons in vulnerable situations or marginalised groups, in both policy development and in the use of the Internet.
9. EMPHASISES the need to include cybersecurity in all digital investments in the coming years and the need to progressively increase cybersecurity level playing field SUPPORTS the Commission's plan to increase public spending and leverage private investment in the cybersecurity domain, taking into account the prospective increase in the number of sectors to which the Directive on measures for a high common level of cybersecurity across the Union (NIS Directive 2.0) will apply. HIGHLIGHTS the importance of Small and Medium Sized Enterprises (SMEs) in the cybersecurity ecosystem and RECOGNISES the relevant financial instruments available to support a cybersecurity digital transformation over the 2021-2027 Multiannual Financial Framework (MFF) as well as in the Recovery and Resilience Facility.

Commented [A167]: ES

10. LOOKS FORWARD to the rapid implementation of the Regulation on Cybersecurity Industrial, Technology and Research Competence Centre and Network of Coordination Centres (CCCN) with a view to maximising the effects of investments to strengthen the Union's leadership in the field of cybersecurity, to support technological capacities and skills and to increase the Union's global competitiveness with input from industry and academic communities in cybersecurity, which should be brought into a more systematic collaboration.
11. REITERATES the need to explore the scope of a possible horizontal Union legal act, including for market access, which the Commission may be invited to propose in order to address all relevant aspects of cybersecurity of connected objects and its links with the cybersecurity certification framework under the Cybersecurity Act (CSA), as well as any other product specific instruments, in order to ensure adequate synergies, while avoiding inconsistencies or duplication.
12. ACKNOWLEDGES the importance of a harmonised approach on cybersecurity in the Union, while fully respecting Member States' competences, and WELCOMES the new proposal for a Directive on measures for a high common level of cybersecurity across the Union (NIS Directive 2.0) that builds upon the NIS Directive as an evolution of the efforts undertaken and which has contributed to strengthening and harmonising national cybersecurity frameworks and promoted cooperation between Member States. Furthermore, RECOGNISES the need for close alignment with other sectorial legislation in this domain.
13. TAKES NOTE of the Commission's proposal to support Member States in strengthening their national Security Operation Centres (SOCs) and to build a network of SOCs across the EU, to detect signals of attacks on networks and enable responses before harm is done. LOOKS FORWARD to exploring this network's potential to strengthen SOCs as well as their complementarity and coordination with existing networks and actors (for instance CSIRTs Network, ENISA and CERT-EU), including within the scope of the EU's cyber crisis management framework, in order to promote an efficient, secure and reliable information-sharing culture. Within this process, the best use should be made of the work carried out in the context of Artificial Intelligence and High Performance Computing initiatives and by European Digital Innovation Hubs, as well as the entire electronic communications infrastructure such as land and submarine network systems. This information-sharing culture should be extended to other systemic digital infrastructure such as platforms with significant market share and gatekeepers
14. TAKES NOTE of the possible development of an ultra-secure connectivity system, building on the Euro quantum communication infrastructure (QCI) and EUGOVSAATCOM, and COMMENDS that it be based on a robust cybersecurity framework.

Commented [A168]: ES

15. 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 its operators in guaranteeing that the Internet remains globally accessible and non-fragmented. RECOGNISES that an alternative European service for accessing the global internet ("DNS4EU" initiative), based on a transparent model which conforms to the latest security and data protection and privacy by design and by default standards and rules, can contribute to increased resilience.
16. 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 to increase the overall level of security, resilience and openness of the global internet, while increasing the competitiveness of the EU industry and in particular of the internet infrastructure operators.
17. 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 Cybersecurity Strategy and as based on the review 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. URGES Member States to continue 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 its strong commitment to applying the EU 5G Toolbox, including relevant restrictions on high-risk suppliers for key assets defined as critical and sensitive in the EU coordinated risk assessments and to continuing efforts made to guarantee the cybersecurity of 5G networks.
18. RECOGNISES the relevance of integrating cybersecurity into EU crisis response mechanisms and STRESSES the importance of enhancing cooperation and information-sharing amongst the various cybersecurity communities within the EU and of linking the existing structures and procedures (such as the Blueprint, the CSIRT Network, the NIS Cooperation Group, CyCLONe, the European Cybercrime Centre, EU INTCEN and the IPCR) in case of large-scale cyber incidents and threats. TAKING INTO ACCOUNT the progress already achieved in this domain, LOOKS FORWARD to the Commission's proposal on the process, milestones and timeline for defining and implementing the Joint Cyber Unit (JCU) with a view to providing added value and streamlining the EU cybersecurity crisis management framework, including through preparedness, shared situational awareness, coordinated response and exercises, in a transparent and incremental manner while avoiding duplication and overlap and respecting the competences of the Member States.

19. As highlighted by the impact of the COVID-19 pandemic, STRESSES the importance of promoting cooperation and exchange between cybersecurity actors and law enforcement and judicial authorities and the need to expand and improve the capacity of these authorities to investigate cybercrime, while fully respecting fundamental rights and striving to ensure the requisite balance between various rights and interests, in particular privacy and security.
20. 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 citizens, governments, industry and society and, at the same time, the need to ensure the ability of the competent law enforcement and judicial authorities to exercise their lawful powers, both online and offline, to protect our societies and citizens.
21. CONTINUES to support and promote the Budapest Convention on Cybercrime, and the ongoing work on the Second Additional Protocol to that Convention. Furthermore, will continue to engage in multilateral exchanges on cybercrime to ensure the respect of human rights and fundamental freedoms.
22. 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 INCEN's work, including by exploring the establishment of an EU Cyber Intelligence Working Group.
23. HIGHLIGHTS the importance of a robust and consistent security framework to better protect all EU personnel, data, information, communication networks 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 classified and non-classified EU networks while ensuring that sufficient resources are available. WELCOMES, in this context, the ongoing interinstitutional discussions on the establishment of common rules on information security and cybersecurity for all EU institutions, bodies, offices and agencies.
24. BUILDING ON the EU's cyber diplomacy efforts, COMMITS itself to increasing the effectiveness and the efficiency of the EU Cyber Diplomacy Toolbox and LOOKS FORWARD to deepening discussions building on lessons learned from the application of this instrument to date. These discussions should aim at building a notion of shared security at international level by strengthening prevention, cooperation and advancing confidence and capacity building and, where necessary, impose restrictions, thereby contributing to the EU's security and integrity and consolidating the EU's cyber posture, in full respect of national competences and prerogatives. In particular, special attention should be given to countering cyberattacks affecting our critical infrastructure, democratic institutions and processes, as well as to countering cyberattacks on supply chain-attacks with systemic effects and cyber-enabled theft of intellectual property.

25. In order to contribute to a global, secure, stable, free and open 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, contributing to the respect for international law in cyberspace and adherence to the norms, rules and principles of responsible state behaviour in cyberspace, for instance 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 outcome of both the current UN GGE and OEWG processes.
26. RECALLS its strong commitment to multilateralism aimed at strengthening cooperation and coordination with international and regional organisations, namely the United Nations, the Council of Europe, the OSCE, the OECD, NATO, 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 the UN Secretary General's Roadmap on digital cooperation. WELCOMES the establishment of 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 EU delegations and MS embassies on international cyber issues in order to strengthen coordinated outreach.
27. ACKNOWLEDGES the importance of strengthening cooperation with international partners, including with NATO, in order to advance the shared understanding of the cyber threat landscape, to develop cooperation mechanisms, to identify, where appropriate, cooperative diplomatic responses as well as to improve information-sharing, including through education, training and exercises. In particular, REAFFIRMS that a strong transatlantic partnership is vital to ensure and to contribute to our common security, stability and prosperity.
28. LOOK 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 security, crisis management and defence agenda, for instance 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 on setting up the Military CERT-Network by the European Defence Agency (EDA) and SUPPORTS efforts made to enhance synergies and coordination between the cybersecurity civilian, defence and space spheres, including through the dedicated PESCO projects.

29. TAKES NOTE of the development of an EU External Cyber Capacity Building Agenda and the creation of an EU Cyber Capacity Building Board in order to increase cyber resilience and capacities worldwide. In this context, ENCOURAGES cooperation with Member States, as well as with public and private sector partners 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 Neighbourhood.
30. 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 partners 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.
31. WELCOMES the comprehensive proposals presented in the Cybersecurity Strategy and ACKNOWLEDGES that all of the initiatives presented therein are important. In order to ensure their seamless implementation, and taking into account the multiannual character of some of these, CONSIDERS it is necessary to set the priorities with an accompanying and detailed implementation plan.
32. MONITORS the progress in the implementation of these Conclusions by the means of an Action Plan to be adopted by the Council by The action plan would be regularly reviewed and updated by the Council in cooperation with the European Commission and the High Representative.
-

SWEDEN

The Council of the European Union,

RECALLING its conclusions on:

- the Joint Communication to the European Parliament and the Council on the Cybersecurity Strategy for the European Union: "An Open, Safe and Secure Cyberspace",
- on Internet Governance,
- the Joint Communication to the European Parliament and the Council: "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU",
- cybersecurity capability and cyber capacity building in the EU,
- the significance of 5G to the European Economy and the need to mitigate security risks linked to 5G [The 5G cybersecurity Toolbox],
- the future of a highly digitised Europe beyond 2020: "Boosting digital and economic competitiveness across the Union and digital cohesion",
- shaping Europe's Digital Future,

- a European Strategy for Data,

- complementary efforts to enhance resilience and counter hybrid threats,
- strengthening resilience and countering hybrid threats, including countering disinformation in the context of the COVID-19 pandemic,
- Cyber Diplomacy,
- on EU Coordinated Response to Large-Scale Cybersecurity Incidents and Crises
- a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox"),
- EU External Cyber Capacity Building Guidelines,
- the cybersecurity of connected devices,
- and its Council Resolution on Encryption - Security through encryption and security despite encryption.

RECALLING the European Council Conclusions on COVID-19, the Single Market, industry policy, digital and external relations and those on disinformation and hybrid threats,

RECALLING the Global Strategy for the European Union's Foreign and Security Policy,

RECALLING the Communications of the European Commission on shaping Europe's Digital Future and on the EU Security Union Strategy,

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 to protect its people, businesses and institutions from cyber threats while enhancing the trust of ~~citizens~~ individuals and organisations in the EU's ability to promote secure and reliable digital tools and connectivity, and to promote and protect a global, stable, secure, free and open cyberspace, grounded in human rights, democracy and the rule of law, human rights, fundamental freedoms and democratic values.
2. RECOGNISING that the COVID-19 pandemic has brought trust and security in Information and Communication Technology (ICT) tools and systems to the forefront of our daily lives, stresses that cybersecurity and the global and open Internet are vital for the functioning of our public administrations and institutions at both national and EU level, for enjoyment of human rights, for teleworking, tele-education and doing business online and for society as a whole.
3. CALLS FOR the promotion and protection of ~~the core EU values of democracy, the rule of law, democracy, and~~ human rights, ~~fundamental freedoms~~ including the right to freedom of expression, ~~the right to free and equal access to and~~ information, the right to freedom of assembly and association, and the right to privacy as well as ~~and~~ the protection against mass surveillance ~~and of the rule of law~~ 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 its 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.
4. HIGHLIGHTS the importance of strengthening the EU's ~~strategic autonomy~~ resilience, particularly its digital and technological leadership in the field of cybersecurity, while preserving an open economy. In this respect, COMMITS itself to promoting the Union's ~~autonomy-technological sovereignty~~ on the basis of the development of a dynamic Industrial Strategy that supports EU value chains human rights, democracy and the rule of law and secures the supply chains in particular in the most strategic domains, while ensuring that access to the single market is gained on fair and equitable terms and with respect for the Union's values.
5. Bearing in mind the shortage of cybersecurity skills in the workforce, STRESSES the importance of developing, retaining and attracting the best cybersecurity talent, for instance through education and training, and ENCOURAGES women's increased participation in science, technology, engineering, mathematics ('STEM') education and ICT jobs upskilling and reskilling in digital skills.

Commented [A169]: Paras 1 and 20: "citizens" should be changed to individuals as we are speaking about enhancing trust or digital security – all individuals have rights, not only citizens.

Commented [A170]: Human rights should be used consistently throughout the document (not strictly necessary to include "fundamental freedoms" as they are covered by "human rights" although "human rights AND fundamental freedoms" is acceptable; "fundamental rights" should not be used as this is limited to an EU context and these conclusions are broader) edits to be made in paras: 1, 3, 19, 20, 21

Commented [A171]: Para 3: should be rephrased to correctly reflect the rights referred to as well as to strengthen the human rights perspective.

Commented [A172]: "EU values" should be replaced with human rights, democracy and the rule of law (to be more specific and spell out what we mean). At the very least "EU founding values" should be used consistently throughout the document, in line with art2 TFEU ("EU common values" is also acceptable) – edits should be made in paras: 3, 4, 7

Commented [A173]: "Strategic autonomy" is not the wording in the strategy, instead "technological sovereignty" is used. Unclear in what context "strategic autonomy" is used here, given the text overall. Resilience seems more relevant given the area

6. RECALLS that the common and comprehensive EU approach to cyber diplomacy aims to contribute to conflict prevention, the 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. REITERATES the United Nations General Assembly's call that UN Member States be guided by the UNGGE reports' recommendations in their use of ICT and notably the application of international law, in particular the UN Charter, in cyberspace.
7. REAFFIRMS that, with a view to shaping international standards in the areas of emerging technologies and core internet architecture so that these are in line with EU values human rights, democracy and the rule of law and a multi-stakeholder approach, the further development of standards which are attractive for others to join within the Union is essential: this will ensure that the Internet remains global, stable, secure, free and open and that the use and development of digital technologies are human-centric human rights respecting, privacy-preserving, and that their use is lawful, safe and ethical human rights based. LOOKS FORWARD TAKES NOTE to the upcoming Standardisation Strategy and COMMITTS itself to underline the importance of proactive and coordinated outreach to promote EU leadership and the EU's objectives at international level, including through transatlantic cooperation and cooperation with like-minded partners, civil society and the private sector.
8. STRONGLY SUPPORTS the multi-stakeholder model for Internet governance and commits itself to reinforcing regular and structured exchanges with stakeholders including the private sector, academia and civil society, in particular within the context of the Paris Call and in international fora. PROMOTES universal, affordable and equal access to the Internet and, in particular, the empowerment of persons in vulnerable or marginalised situations or marginalised groups, in both policy development and in the use of the Internet.
9. EMPHASISES the need to include cybersecurity in all digital investments in the coming years and SUPPORTS NOTES the Commission's plan to increase public spending and leverage private investment in the cybersecurity domain, taking into account the prospective increase in the number of sectors to which the Directive on measures for a high common level of cybersecurity across the Union (NIS Directive 2.0) will apply. HIGHLIGHTS the importance of Small and Medium Sized Enterprises (SMEs) in the cybersecurity ecosystem and RECOGNISES NOTES the relevant financial instruments available to support a cybersecurity digital transformation over the 2021-2027 Multiannual Financial Framework (MFF) as well as in the Recovery and Resilience Facility.

Commented [A174]: -Para 7: "human centric" and "ethical" should be replaced with "human rights respecting" or "human rights based" (meaning "privacy-preserving" can be removed as it is included in human rights). Additionally the sentence should be edited to speak about the "use and development of" digital technologies rather than separately.

Commented [A175]: As we have not seen the Standardisation Strategy yet, it is too early to welcome it.

Commented [A176]: - Para 8: proposed shifting "persons in vulnerable OR MARGINALISED situations or marginalised groups"

Commented [A177]: Negotiation is ongoing, support is too early

10. LOOKS FORWARD to the rapid implementation of the Regulation on Cybersecurity Industrial, Technology and Research Competence Centre and Network of Coordination Centres (CCCN) with a view to maximising the effects of investments to strengthen the Union's leadership in the field of cybersecurity, to support technological capacities and skills and to increase the Union's global competitiveness with input from industry and academic communities in cybersecurity, which should be brought into a more systematic collaboration.

11. REITERATES the need to ~~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, explore the scope of a possible horizontal Union legal act, including for market access, which the Commission may be invited to propose in order to address all relevant aspects of cybersecurity of connected objects and its links with the cybersecurity certification framework under the Cybersecurity Act (CSA), as well as any other product specific instruments, in order to ensure adequate synergies, while avoiding inconsistencies or duplication.~~

Commented [A178]: We interpret "reiterates" as this is the same action as in the council conclusions on connected devices (dec 2020). As nothing yet has been proposed from those conclusions, we would like to keep the action as from dec 2020.

12. ACKNOWLEDGES the importance of a harmonised approach on cybersecurity in the Union, while fully respecting Member States' competences, and ~~WELCOMES NOTES~~ the new proposal for a Directive on measures for a high common level of cybersecurity across the Union (NIS Directive 2.0) that builds upon the NIS Directive as an evolution of the efforts undertaken and which has contributed to strengthening and harmonising national cybersecurity frameworks and promoted cooperation between Member States. Furthermore, RECOGNISES the need for close alignment with other sectorial legislation in this domain.

13. TAKES NOTE of the Commission's proposal to support Member States in strengthening their national Security Operation Centres (SOCs) and to build a network of SOCs across the EU, to detect signals of attacks on networks and enable responses before harm is done. ~~LOOKS FORWARD to exploring this network's potential to strengthen SOCs as well as their complementarity and coordination with existing networks and actors (for instance CSIRTs Network, ENISA and CERT EU), including within the scope of the EU's cyber crisis management framework, in order to promote an efficient, secure and reliable information sharing culture. Within this process, EMPHASISES that the best use should be made of the work carried out in the context of Artificial Intelligence and High Performance Computing initiatives and by European Digital Innovation Hubs, as well as the entire electronic communications infrastructure such as land and submarine network systems.~~

Commented [A179]: Premature statement. The first sentence in 13 is enough.

Commented [A180]: This can also be deleted as it is a follow up to the previous deleted sentence. If kept, it could start with "EMPHASISES".

14. ~~TAKES NOTE of the possible development of an ultra-secure connectivity system, building on the Euro quantum communication infrastructure (QCI) and EUGOVSATCOM, and COMMENDS that it be based on a robust cybersecurity framework.~~

Commented [A181]: Refers to initiative (QCI) that is built on uncertain technical solutions at best. Should not be included in CC.

Also there is no such thing as ultra secure, especial in regards to an initiative that has a long way to go before any (if any) can be deemed practical/useful

~~15-14.~~ 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 its operators in guaranteeing that the Internet remains globally accessible and non-fragmented. RECOGNISES that an alternative European service for accessing the global internet ("DNS4EU" initiative), based on a transparent model which conforms to the latest security and data protection and privacy by design and by default standards and rules, can contribute to increased resilience.

~~16-15.~~ 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 to increase the overall level of security, resilience and openness of the global internet, while increasing the competitiveness of the EU industry and in particular of the internet infrastructure operators.

~~17-16.~~ 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 Cybersecurity Strategy and as based on the review 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. URGES Member States to continue 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 its strong commitment to a full and swift application applying of the EU 5G Toolbox, including relevant restrictions on high-risk suppliers for key assets defined as critical and sensitive in the EU coordinated risk assessments and to continuing efforts made to guarantee the cybersecurity of 5G networks. HIGHLIGHTS the opportunity to build on the positive experiences and lessons learned from the work on the 5G toolbox in other areas.

~~18-17.~~ RECOGNISES the relevance of integrating cybersecurity into EU crisis response mechanisms and ~~STRESSES-HIGHLIGHTS~~ the importance of enhancing cooperation and information-sharing amongst the various cybersecurity communities within the EU and of linking the existing structures and procedures (such as the Blueprint, the CSIRT Network, the NIS Cooperation Group, CyCLONe, the European Cybercrime Centre, EU INCEN and the IPCR) in case of large-scale cyber incidents and threats. TAKING INTO ACCOUNT the progress already achieved in this domain, ~~LOOKS FORWARD-ACKNOWLEDGES~~ the Commission's coming proposal on the process, milestones and timeline for defining and implementing the Joint Cyber Unit (JCU) with a view to providing added value and streamlining the EU cybersecurity crisis management framework, including through preparedness, shared situational awareness, coordinated response and exercises, in a transparent and incremental manner while avoiding duplication and overlap and respecting the competences of the Member States.

Commented [A182]: In what sense?

~~19-18.~~ As highlighted by the impact of the COVID-19 pandemic, STRESSES the importance of promoting cooperation and exchange between cybersecurity actors and law enforcement and judicial authorities and the need to expand and improve the capacity of these authorities to investigate cybercrime, while fully respecting ~~fundamental human~~ rights and striving to ensure the requisite balance between various rights and interests, in particular privacy and security.

~~20-19.~~ REAFFIRMS its support to the development, implementation and use of strong encryption as a necessary means of protecting ~~fundamental human~~ rights and the digital security of citizens, governments, ~~civil society actors~~, industry and society and, at the same time, the need to ensure the ability of the competent law enforcement and judicial authorities to exercise their lawful powers, both online and offline, to protect our societies and ~~citizens~~ individuals.

Commented [A183]: In para 20 **civil society actors** should be included in listing of actors who rely on encryption

~~21-20.~~ CONTINUES to support and promote the Budapest Convention on Cybercrime, and the ongoing work on the Second Additional Protocol to that Convention. Furthermore, will continue to engage in multilateral exchanges on cybercrime to ensure the respect of human rights ~~and fundamental freedoms~~.

~~22-21.~~ 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, including by exploring the possible establishment of an EU Cyber Intelligence Working Group.

~~23-22.~~ HIGHLIGHTS the importance of a robust and consistent security framework to better protect all EU personnel, data, information, communication networks 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 classified and non-classified EU networks while ensuring that sufficient resources are available. WELCOMES, in this context, the ongoing interinstitutional discussions on the establishment of common rules on information security and cybersecurity for all EU institutions, bodies, offices and agencies.

Commented [A184]: Needs to be clarified.

~~24-23.~~ BUILDING ON the EU's cyber diplomacy efforts, COMMITS itself to increasing the effectiveness and the efficiency of the EU Cyber Diplomacy Toolbox and LOOKS FORWARD to deepening discussions building on lessons learned from the application of this instrument to date. These discussions should aim at ~~building a notion of contributing to~~ shared security at international level by strengthening prevention, cooperation and advancing confidence and capacity building and, ~~when necessary~~ appropriate, impose restrictions, thereby contributing to the EU's security, ~~and~~ integrity and ~~consolidating the EU's~~ cyber posture, in full respect of national competences and prerogatives. The toolbox should continually be updated to enable countering threats in an ever-changing global threat landscape. In particular, special attention should be given to countering cyberattacks affecting our critical infrastructure, democratic institutions and processes, as well as to countering cyberattacks on supply chain attacks with systemic effects and cyber-enabled theft of intellectual property.

Commented [A185]: Clarification of "cyber posture" welcomed.

Commented [A186]: Premature and too detailed. It is not necessary to define specific clusters of potential targets to serve a discussion on lessons learned from the toolbox so far, nor for what a potentially developed toolbox might be used to counter. Furthermore, these clusters of potential targets are not mentioned anywhere else in the conclusions.

25-24. In order to contribute to a global, secure, stable, free and open 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, contributing to the respect for international law in cyberspace and adherence to the norms, rules and principles of responsible state behaviour in cyberspace, for instance 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 outcome of both the current UN GGE and OEWG processes.

Commented [A187]: Para 25: Important to not only focus on first committee. Negotiations on cybercrime convention in third committee equally important and should primarily be dealt with from a foreign/security policy perspective.

26-25. RECALLS its strong commitment to multilateralism aimed at strengthening cooperation and coordination with international and regional organisations, namely the United Nations, the Council of Europe, the OSCE, the OECD, NATO, 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 the UN Secretary General's Roadmap on digital cooperation. WELCOMES the establishment of 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 EU delegations and MS embassies on international cyber issues in order to strengthen coordinated outreach.

27-26. ACKNOWLEDGES the importance of strengthening cooperation with international partners, including with NATO, in order to advance the shared understanding of the cyber threat landscape, to develop cooperation mechanisms, to identify, where appropriate, cooperative diplomatic responses as well as to improve information-sharing, including through education, training and exercises. In particular, REAFFIRMS that a strong transatlantic partnership is vital to ensure and to contribute to our common security, stability and prosperity.

28-27. ~~LOOK FORWARD TO~~ACKNOWLEDGES the forthcoming proposal for a review of the Cyber Defence Policy Framework (CDPF), and ~~COMMITTS itself~~ WELCOMES to pursuing efforts to strengthen cybersecurity and cyber defence dimensions with a view to ensuring that these are fully integrated into the wider security, crisis management and defence agenda, for instance 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~~ ACKNOWLEDGES the initiative on setting up the Military CERT-Network by the European Defence Agency (EDA) and SUPPORTS efforts made to enhance synergies and coordination between the cybersecurity civilian, defence and space spheres, including through the dedicated PESCO projects. WELCOMES the Joint Communication on A new EU-US agenda for global change, including transatlantic cooperation on technology, trade and standards.

~~29-28.~~ TAKES NOTE of the development of an EU External Cyber Capacity Building Agenda and the creation of an EU Cyber Capacity Building Board in order to increase cyber resilience and capacities worldwide. In this context, ENCOURAGES cooperation with Member States, as well as with public and private sector partners 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 Neighbourhood.

~~30-29.~~ 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 partners 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.

~~30. WELCOMES the comprehensive proposals presented in the Cybersecurity Strategy and ACKNOWLEDGES that all of the initiatives presented therein are important. In order to ensure their seamless implementation, and taking into account the multiannual character of some of these, CONSIDERS it is necessary to set the priorities with an accompanying and detailed implementation plan.~~

Commented [A188]: Premature. Some proposals are vague.

31. NOTES the well-executed cooperation between the Commission and EEAS on the EU Cybersecurity Strategy. ENCOURAGES regularized and consolidated cooperation and coordination between the Commission and EEAS on cyber issues.

32. MONITORS the progress in the implementation of these Conclusions by the means of an Action Plan to be adopted by the Council by The action plan would be regularly reviewed and updated by the Council in cooperation with the European Commission and the High Representative.