European Parliament
2019-2024

Committee on Foreign Affairs

2020/0359(COD)

15.7.2021

OPINION

of the Committee on Foreign Affairs

for the Committee on Industry, Research and Energy

on the proposal for a directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148
(2020/0359(COD))

Rapporteur for opinion: Markéta Gregorová

PA_Legam

AMENDMENTS

The Committee on Foreign Affairs calls on the Committee on Industry, Research and Energy, as the committee responsible, to take into account the following amendments:

Amendment 1

Proposal for a directive
Recital 2

Text proposed by the Commission	*Amendment*
(2) Since the entry into force of Directive (EU) 2016/1148 significant progress has been made in increasing the Union's level of cybersecurity resilience. The review of that Directive has shown that it has served as a catalyst for the institutional and regulatory approach to cybersecurity in the Union, paving the way for a significant change in mind-set. That Directive has ensured the completion of national frameworks by defining national cybersecurity strategies, establishing national capabilities, and implementing regulatory measures covering essential infrastructures and actors identified by each Member State. It has also contributed to cooperation at Union level through the establishment of the Cooperation Group[12] and a network of national Computer Security Incident Response Teams ('CSIRTs network')[13] . Notwithstanding those achievements, the review of Directive (EU) 2016/1148 has revealed inherent shortcomings that prevent it from addressing effectively contemporaneous and emerging cybersecurity challenges.	(2) Since the entry into force of Directive (EU) 2016/1148 significant progress has been made in increasing the Union's level of cybersecurity resilience. The review of that Directive has shown that it has served as a catalyst for the institutional and regulatory approach to cybersecurity in the Union, paving the way for a significant change in mind-set. That Directive has ensured the completion of national frameworks by defining national cybersecurity strategies, establishing national capabilities, and implementing regulatory measures covering essential infrastructures and actors identified by each Member State. It has also contributed to cooperation at Union level through the establishment of the Cooperation Group[12] and a network of national Computer Security Incident Response Teams ('CSIRTs network')[13]***. Directive (EU) 2016/1148 was the first Union-wide legislative act on cybersecurity, providing legal measures to boost the overall level of cyber resilience also in the security and defence domain in the Union by ensuring Member States' cooperation and a culture of security across sectors***. Notwithstanding those achievements, the review of Directive (EU) 2016/1148 has revealed inherent shortcomings that prevent it from addressing effectively contemporaneous and emerging cybersecurity challenges***, which very often originate from outside***

	the Union, posing a serious threat to internal and external security at Union level.
[12] Article 11 of Directive (EU) 2016/1148.	[12] Article 11 of Directive (EU) 2016/1148.
[13] Article 12 of Directive (EU) 2016/1148.	[13] Article 12 of Directive (EU) 2016/1148.

Amendment 2

Proposal for a directive
Recital 3 a (new)

Text proposed by the Commission	*Amendment*
	(3a) The Union understands hybrid campaigns to be 'multidimensional, combining coercive and subversive measures, using both conventional and unconventional tools and tactics (diplomatic, military, economic, and technological) to destabilise the adversary. They are designed to be difficult to detect or attribute, and can be used by state and non-state actors'[1a]. The internet and online networks allow State and non-State actors to conduct aggressive action in new ways. They can be used to hack critical infrastructure and democratic processes, launch persuasive disinformation and propaganda campaigns, steal information and upload sensitive data into the public domain. In the worst cases, cyber attacks allow an adversary to take control of assets such as military systems and command structures[1b]. At the same time, thorough cooperation with the private sector and civilian stakeholders, including industries and entities involved in the management of critical infrastructures, is crucial and should be reinforced due to the intrinsic characteristics of the cyber domain, in which technological innovation is mainly driven by private companies that often do not operate in the military field. Such large-scale cybersecurity incidents and crises at Union level should be adequately

prepared for and protected against via joint training exercises as they have the potential to invoke Article 222 TFEU (the 'solidarity clause').

[1a] ***European Commission/High Representative of the Union for Foreign Affairs and Security Policy, "Joint Communication on Increasing Resilience and Bolstering Capabilities to Address Hybrid Threats", JOIN(2018) 16 final, Brussels, June 13, 2018, p. 1.***

[1b]

https://www.iss.europa.eu/sites/default/files/EUISSFiles/CP_151.pdf

Amendment 3

Proposal for a directive
Recital 3 b (new)

Text proposed by the Commission	*Amendment*
	(3b) During large-scale cyber security incidents and crises at Union level, the high degree of interdependence between sectors and countries require a coordinated action to ensure a rapid and effective response, as well as better prevention and preparedness for similar situations in the future. The availability of cyber-resilient networks and information systems and the availability, confidentiality and integrity of data are vital for the security of the Union within as well as beyond its borders. The Union's ambition to acquire a more prominent geopolitical role also rests on credible cyber defence and deterrence, including the capacity to identify malicious actions in a timely, effective manner and to respond adequately. Given the blurring of lines between the realms of civilian and military matters and the dual-use nature of cyber tools and technologies, there is a need for a comprehensive and holistic approach to the digital domain. This also

applies to Common Security and Defence Policy (CSDP) operations and missions conducted by the Union to ensure peace and stability in its neighbourhood and beyond. In this regard the Union's Strategic Compass should enhance and guide the implementation of the Union's level of ambition in the field of security and defence, and translate that ambition into capability needs in cyber defence, thereby increasing the ability of the Union and Member States to prevent, discourage, deter, respond to and recover from malicious cyber activities by strengthening its posture, situational awareness, tools, procedures and partnerships. The Union's cooperation with international organisations such as NATO contributes to discussions on how to prevent, deter and respond to hybrid and cyber-attacks, and explore ways to establish a common cyber threat analysis.

Amendment 4

Proposal for a directive
Recital 6

Text proposed by the Commission	*Amendment*
(6) This Directive leaves unaffected the ability of Member States to take the necessary measures to ensure the protection of the essential interests of their security, to safeguard public policy and public security, and to allow for the investigation, detection and prosecution of criminal offences, in compliance with Union law. In accordance with Article 346 TFEU, no Member State is to be obliged to supply information the disclosure of which would be contrary to the essential interests of its public security. In this context, national and Union rules for protecting classified information, non-disclosure agreements, and informal non-disclosure agreements such as the Traffic Light	(6) This Directive leaves unaffected the ability of Member States to take the necessary measures to ensure the protection of the essential interests of their security, to safeguard public policy and public security, and to allow for the investigation, detection and prosecution of criminal offences, in compliance with Union law ***and fundamental rights. Independently of the technological environment, it is essential tofully respect due process and other safeguards, in particular fundamental rights, such as the right to respect for private life and communications and the right to the protection of personal data. Similarly, in order to ensure an all-encompassing resilience, it is necessary not only to***

Protocol[14] , are of relevance.	***strengthen technological infrastructures and to possess response capabilities, but also to raise public awareness about cyber risks and security.*** In accordance with Article 346 TFEU, no Member State is to be obliged to supply information the disclosure of which would be contrary to the essential interests of its public security. In this context, national and Union rules for protecting classified information, non-disclosure agreements, and informal non-disclosure agreements such as the Traffic Light Protocol[14] , are of relevance.
[14] The Traffic Light Protocol (TLP) is a means for someone sharing information to inform their audience about any limitations in further spreading this information. It is used in almost all CSIRT communities and some Information Analysis and Sharing Centres (ISACs).	[14] The Traffic Light Protocol (TLP) is a means for someone sharing information to inform their audience about any limitations in further spreading this information. It is used in almost all CSIRT communities and some Information Analysis and Sharing Centres (ISACs).

Amendment 5

Proposal for a directive
Recital 14 a (new)

Text proposed by the Commission	*Amendment*
	(14a) With a view to develop a secure connectivity system and build on the European quantum communication infrastructure (EuroQCI) and the European Union Governmental Satellite Communication (GOVSATCOM), in particular the implementation of GALILEO GNSS for defence users, where future possible development should, inter alia, take into account the impact of merging the speed and sophistication of quantum computing with highly autonomous military systems, Member States should ensure the protection of entire electronic communications infrastructure, such as space, land and submarine network systems. At the same time, a common

vision on Cloud Adoption Strategy for sensitive sectors should be established, with the aim of defining a Union approach based on shared standards among like-minded partner countries.

Amendment 6

Proposal for a directive
Recital 20

Text proposed by the Commission	*Amendment*
(20) Those growing interdependencies are the result of an increasingly cross-border and interdependent network of service provision using key infrastructures across the Union in the sectors of energy, transport, digital infrastructure, drinking and waste water, health, certain aspects of public administration, as well as space in as far as the provision of certain services depending on ground-based infrastructures that are owned, managed and operated either by Member States or by private parties is concerned, therefore not covering infrastructures owned, managed or operated by or on behalf of the Union as part of its space programmes. Those interdependencies mean that any disruption, even one initially confined to one entity or one sector, can have cascading effects more broadly, potentially resulting in far-reaching and long-lasting negative impacts in the delivery of services across the internal market. The COVID-19 pandemic has shown the vulnerability of our increasingly interdependent societies in the face of low-probability risks.	(20) Those growing interdependencies are the result of an increasingly cross-border and interdependent network of service provision using key infrastructures across the Union in the sectors of energy, transport, digital infrastructure, drinking and waste water, health, certain aspects of public administration, as well as space in as far as the provision of certain services depending on ground-based infrastructures that are owned, managed and operated either by Member States or by private parties is concerned, therefore not covering infrastructures owned, managed or operated by or on behalf of the Union as part of its space programmes. ***Infrastructure that is owned, managed or operated by or on behalf of the Union as part of its space programmes is particularly important for the security of the Union and its Member States and the proper functioning of the CSDP missions. Such infrastructure is to be adequately protected in accordance with Regulation (EU) 2021/696 of the European Parliament and of the Council[18a]***. Those interdependencies mean that any disruption, even one initially confined to one entity or one sector, can have cascading effects more broadly, potentially resulting in far-reaching and long-lasting negative impacts in the delivery of services across the internal market ***and put at risk the security and safety of Union citizens***. The COVID-19 pandemic has shown the

vulnerability of our increasingly interdependent societies in the face of low-probability risks.

_____

*[18a] **Regulation (EU) 2021/696 of the European Parliament and of the Council of 28 April 2021 establishing the Union Space Programme and the European Union Agency for the Space Programme and repealing Regulations (EU) No 912/2010, (EU) No 1285/2013 and (EU) No 377/2014 and Decision No 541/2014/EU (OJ L 170, 12.5.2021, p. 69).***

Amendment 7

Proposal for a directive
Recital 26

Text proposed by the Commission	*Amendment*
(26) Given the importance of international cooperation on cybersecurity, CSIRTs should be able to participate in international cooperation networks in addition to the CSIRTs network established by this Directive.	(26) Given the importance of international cooperation on cybersecurity, CSIRTs should be able to participate in international cooperation networks in addition to the CSIRTs network established by this Directive***, in order to contribute to the development of Union standards that can shape the cybersecurity landscape at international level. Member States could also explore the possibility of increasing cooperation with like-minded partner countries and international organisations such as the Council of Europe, the North Atlantic Treaty Organisation, the Organisation for Economic Cooperation and Development, the Organisation for Security and Co-operation in Europe and the United Nations with the aim to secure multilateral agreements on cyber norms, responsible state and non-state behaviour in cyberspace and effective global digital governance as well as to create an open, free, stable and secure cyberspace based in international law.***

Amendment 8

Proposal for a directive
Recital 27

Text proposed by the Commission	*Amendment*
(27) In accordance with the Annex to Commission Recommendation (EU) 2017/1548 on Coordinated Response to Large Scale Cybersecurity Incidents and Crises ('Blueprint')[20], a large-scale incident should mean an incident with a significant impact on at least two Member States or whose disruption exceeds a Member State's capacity to respond to it. Depending on their cause and impact, large-scale incidents may escalate and turn into fully-fledged crises not allowing the proper functioning of the internal market. Given the wide-ranging scope and, in most cases, the cross-border nature of such incidents, Member States and relevant Union institutions, bodies and agencies should cooperate at technical, operational and political level to properly coordinate the response across the Union.	(27) In accordance with the Annex to Commission Recommendation (EU) 2017/1548 on Coordinated Response to Large Scale Cybersecurity Incidents and Crises ('Blueprint')[20], a large-scale incident should mean an incident with a significant impact on at least two Member States or whose disruption exceeds a Member State's capacity to respond to it. Depending on their cause and impact, large-scale incidents may escalate and turn into fully-fledged crises not allowing the proper functioning of the internal market ***or risk the security and safety of citizens and the economic and financial interest of the Union***. Given the wide-ranging scope and, in most cases, the cross-border nature of such incidents, Member States and relevant Union institutions, bodies and agencies should cooperate at technical, operational and political level to properly coordinate the response across the Union. ***The Union and Member States should also further promote exercises and scenario-based policy discussion on crisis management framework, to ensure internal and external policy coherence and to build a common understanding of the procedures for the implementation of the solidarity clause.***
[20] Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises (OJ L 239, 19.9.2017, p. 36).	[20] Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises (OJ L 239, 19.9.2017, p. 36).

Amendment 9

Proposal for a directive
Recital 36

Text proposed by the Commission	*Amendment*
(36) The Union should, where appropriate, conclude international agreements, in accordance with Article 218 TFEU, with third countries or international organisations, allowing and organising their participation in some activities of the Cooperation Group and the CSIRTs network. Such agreements ***should*** ensure adequate protection of data.	(36) The Union should, where appropriate, conclude international agreements, in accordance with Article 218 TFEU, with third countries or international organisations, allowing and organising their participation in some activities of the Cooperation Group and the CSIRTs network. Such agreements ***are to*** ensure adequate protection of data ***and should promote market access as well as address security risks while increasing global resilience and raise awareness about cyber threats and malicious cyber activities. The Union should also continue to support capacity building in third countries. Member States should, where appropriate, encourage the participation of like-minded partner countries, which share our Union values, in relevant PESCO projects. Therefore, the Union should investigate the possibility to re-launch processes aiming at concluding formal and structured frameworks for cooperation in this field in the future.***

Amendment 10

Proposal for a directive
Recital 37

Text proposed by the Commission	*Amendment*
(37) Member States should contribute to the establishment of the EU Cybersecurity Crisis Response Framework set out in Recommendation (EU) 2017/1584 through the existing cooperation networks, notably the Cyber Crisis Liaison Organisation Network (EU-CyCLONe), CSIRTs network and the Cooperation Group. EU-CyCLONe and the CSIRTs network should cooperate on the basis of procedural arrangements defining the modalities of that cooperation. The EU-CyCLONe's rules of procedures should further specify the modalities through which the network	(37) Member States should contribute to the establishment of the EU Cybersecurity Crisis Response Framework set out in Recommendation (EU) 2017/1584 through the existing cooperation networks, notably the Cyber Crisis Liaison Organisation Network (EU-CyCLONe), CSIRTs network and the Cooperation Group***, the European Cybercrime Centre and the Union's Intelligence and Situation Centre (EU INTCEN), to advance strategic intelligence cooperation on cyber threats and activities, in order to further support Union situational awareness and***

should function, including but not limited to roles, cooperation modes, interactions with other relevant actors and templates for information sharing, as well as means of communication. For crisis management at Union level, relevant parties should rely on the Integrated Political Crisis Response (IPCR) arrangements. The Commission should use the ARGUS high-level cross-sectoral crisis coordination process for this purpose. If the crisis entails an important external or ***Common Security and Defence Policy (***CSDP***)*** dimension, the European External Action Service (EEAS) Crisis Response Mechanism (CRM) should be activated.

decision-making on a joint diplomatic response. EU-CyCLONe and the CSIRTs network should cooperate on the basis of procedural arrangements defining the modalities of that cooperation. The EU-CyCLONe's rules of procedures should further specify the modalities through which the network should function, including but not limited to roles, cooperation modes, interactions with other relevant actors and templates for information sharing, as well as means of communication. For crisis management at Union level, relevant parties should rely on the Integrated Political Crisis Response (IPCR) arrangements***, which also support the coordination at political level of the response to the invoking of the solidarity clause.*** The Commission should use the ARGUS high-level cross-sectoral crisis coordination process for this purpose. If the crisis entails an important external or CSDP dimension, the European External Action Service (EEAS) Crisis Response Mechanism (CRM) should be activated***, as well as any measure aiming to protect CSDP missions and operations and Union delegations. In addition, the Union should make full use of its cyber diplomacy toolbox.***

Amendment 11

Proposal for a directive
Recital 40 a (new)

Text proposed by the Commission	*Amendment*
	(40a) Member States should consider an active cyber defence programme to be part of their national cybersecurity strategy that incorporates regular joint training exercises between Member States and across international organisations. Such a programme should provide a synchronised, real-time capability to discover, detect, analyse, and mitigate threats. Active cyber defence operates at network speed using sensors, software

and intelligence to detect and stop malicious activity ideally before it can affect networks and systems. Moreover, Member States should significantly enhance information sharing method, to define a common communication standard that could be used for classified and non-classified information, in order to enhance the rapid action. The Union and the Member States should also strengthen their capabilities to attribute cyber attacks in order to effectively deter and respond to cyber attacks in a proportionate manner, in line with international law.

Amendment 12

Proposal for a directive
Recital 40 b (new)

Text proposed by the Commission	*Amendment*
	(40b) Member States should come forward with an active cyber defence programme in their national cybersecurity strategies. Active cyber defence is the proactive detection, analysis and mitigation of network security breaches in real-time combined with the use of capabilities deployed outside the victim network. It is based on a defensive strategy that excludes offensive measures against the adversaries critical civilian infrastructure which would constitute a breach of international law (such as of the 1977 Additional Protocol to the Geneva Conventions). The ability to rapidly and automatically share and understand threat information and analysis, cyber activity alerts, and response action is critical to enabling unity of effort in successfully detecting and preventing cyber attacks. Active cyber defence activities could include email server configurations, website configurations, logging enabling and DNS filtering. Member State should adopt

policies able to ensure the widest possible access to the most performing cybersecurity tools, supporting companies, small and medium-sized enterprises and businesses with low financial capabilities, trough benefits, grants, loans or fiscal advantages dedicated to the acquisition of highest-level cybersecurity products and services, avoiding that their costs represent an element of discrimination. Member States should also aim to promote partnerships with academic institutions and other research centres aiming to foster R&D cybersecurity programme in order to develop new common technologies, tools and skills applicable in both civilian and defence sectors through a multidisciplinary approach. Partnerships should be financed by existing and new funding tools under the auspices of the Commission.

Amendment 13

Proposal for a directive
Recital 43

Text proposed by the Commission	*Amendment*
(43) Addressing cybersecurity risks stemming from an entity's supply chain and its relationship with its suppliers is particularly important given the prevalence of incidents where entities have fallen victim to cyber-attacks and where malicious actors were able to compromise the security of an entity's network and information systems by exploiting vulnerabilities affecting third party products and services. Entities should therefore assess and take into account the overall quality of products and cybersecurity practices of their suppliers and service providers, including their secure development procedures.	(43) Addressing cybersecurity risks stemming from an entity's supply chain and its relationship with its suppliers is particularly important given the prevalence of incidents where entities have fallen victim to cyber-attacks and where malicious actors were able to compromise the security of an entity's network and information systems by exploiting vulnerabilities affecting third party products and services. Entities should therefore assess and take into account the overall quality of products and cybersecurity practices of their suppliers and service providers, including their ***risk-management systems***, secure development procedures ***in accordance with Union***

cybersecurity standards.

Amendment 14

Proposal for a directive
Recital 43 a (new)

Text proposed by the Commission	*Amendment*
	(43a) Potential non-technical risk factors, such as undue influence by a third country on suppliers and service providers, especially in the case of alternative models of governance, include concealed vulnerabilities or backdoors and potential systemic supply disruptions, especially in case of technological lock-in or provider dependency. Since the exploitation of vulnerabilities in defence sector may cause significant disruption and harm, cyber security of defence industry requires special measures to ensure the security of the supply chains, particularly entities lower in supply chains, which do not require access to classified information, but that could carry serious risks to the entire sector. Special consideration should be given to the impact any breach could have and the threat of any potential manipulation of network data that could render critical defence assets useless or even override their operating systems making them vulnerable to hijacking.

Amendment 15

Proposal for a directive
Recital 46

Text proposed by the Commission	*Amendment*
(46) To further address key supply chain risks and assist entities operating in sectors covered by this Directive to appropriately manage supply chain and supplier related cybersecurity risks, the Cooperation Group	(46) To further address key supply chain risks and assist entities operating in sectors covered by this Directive to appropriately manage supply chain and supplier related cybersecurity risks, the Cooperation Group

involving relevant national authorities, in cooperation with the Commission ENISA should carry out coordinated sectoral supply chain risk assessments, as was already done for 5G networks following Recommendation (EU) 2019/534 on Cybersecurity of 5G networks[21] , with the aim of identifying per sector which are the critical ICT services, systems or products, relevant threats and vulnerabilities.	involving relevant national authorities, in cooperation with the Commission***,*** ENISA ***and the European External Action Service*** should carry out coordinated sectoral supply chain risk assessments, as was already done for 5G networks following Recommendation (EU) 2019/534 on Cybersecurity of 5G networks[21] , with the aim of identifying per sector which are the critical ICT services, systems or products, relevant threats and vulnerabilities.
[21] Commission Recommendation (EU) 2019/534 of 26 March 2019 Cybersecurity of 5G networks (OJ L 88, 29.3.2019, p. 42).	[21] Commission Recommendation (EU) 2019/534 of 26 March 2019 Cybersecurity of 5G networks (OJ L 88, 29.3.2019, p. 42).

Amendment 16

Proposal for a directive
Recital 68

Text proposed by the Commission	*Amendment*
(68) Entities should be encouraged to collectively leverage their individual knowledge and practical experience at strategic, tactical and operational levels with a view to enhance their capabilities to adequately assess, monitor, defend against, and respond to, cyber threats. It is thus necessary to enable the emergence at Union level of mechanisms for voluntary information sharing arrangements. To this end, Member States should actively support and encourage also relevant entities not covered by the scope of this Directive to participate in such information-sharing mechanisms. Those mechanisms should be conducted in full compliance with the competition rules of the Union as well as the data protection Union law rules.	(68) Entities should be encouraged to collectively leverage their individual knowledge and practical experience at strategic, tactical and operational levels with a view to enhance their capabilities to adequately assess, monitor, defend against, and respond to, cyber threats. It is thus necessary to enable the emergence at Union level of mechanisms for voluntary information sharing arrangements. To this end, Member States should actively support and encourage also relevant entities not covered by the scope of this Directive to participate in such information-sharing mechanisms. ***In addition, Member States could also explore the possibility of reaching out to like-minded partner countries.*** Those mechanisms should be conducted in full compliance with the competition rules of the Union as well as the data protection Union law rules. ***To the same end,***

	Member States should support competent authorities and CSIRTs to establish free-of-charge or accessible cybersecurity assistance, education, and audit programs for entities that fall outside the scope of this Directive, in particular start-ups, SMEs and non-governmental organisations(NGOs).

Amendment 17

Proposal for a directive
Recital 68 a (new)

Text proposed by the Commission	*Amendment*
	(68a) Given that cybersecurity has both a civilian and a military dimension, information exchange across sectors (defence, civilian, law enforcement and external action) should also be encouraged. The Joint Cyber Unit could play an important role in protecting the Union from cyber-attacks by helping actors to acquire a common understanding of the threat landscape and to coordinate their response.

Amendment 18

Proposal for a directive
Recital 73

Text proposed by the Commission	*Amendment*
(73) Where administrative fines are imposed on an undertaking, an undertaking should be understood to be an undertaking in accordance with Articles 101 and 102 TFEU for those purposes. Where administrative fines are imposed on persons that are not an undertaking, the supervisory authority should take account of the general level of income in the Member State as well as the economic situation of the person in considering the appropriate amount of the fine. It should be	(73) Where administrative fines are imposed on an undertaking, an undertaking should be understood to be an undertaking in accordance with Articles 101 and 102 TFEU for those purposes. Where administrative fines are imposed on persons that are not an undertaking, the supervisory authority should take account of the general level of income in the Member State as well as the economic situation of the person in considering the appropriate amount of the fine***, without***

for the Member States to determine whether and to what extent public authorities should be subject to administrative fines. Imposing an administrative fine does not affect the application of other powers by the competent authorities or of other penalties laid down in the national rules transposing this Directive.	***prejudice to the objectives of this Directive***. It should be for the Member States to determine whether and to what extent public authorities should be subject to administrative fines. Imposing an administrative fine does not affect the application of other powers by the competent authorities or of other penalties laid down in the national rules transposing this Directive.

Amendment 19

Proposal for a directive
Article 5 – paragraph 2 – point a

Text proposed by the Commission	*Amendment*
(a) a policy addressing cybersecurity in the supply chain for ICT products and services used by essential and important entities for the provision of their services;	(a) a policy addressing cybersecurity in the supply chain for ICT products and services used by essential and important entities for the provision of their services***, based on a comprehensive assessment of potential threats to supply chains***;

Amendment 20

Proposal for a directive
Article 5 – paragraph 2 – point b a (new)

Text proposed by the Commission	*Amendment*
	(ba) a policy for promoting interoperability and adherence to common Union standards in cybersecurity;

Amendment 21

Proposal for a directive
Article 5 – paragraph 2 – point d

Text proposed by the Commission	*Amendment*
(d) a policy related to sustaining the general availability and integrity of the	(d) a policy related to sustaining the general availability and integrity of the

public core of the open internet;	public core of the open internet***, including cybersecurity, where applicable, of undersea communications cables***;

Amendment 22

Proposal for a directive
Article 5 – paragraph 2 – point f

Text proposed by the Commission	*Amendment*
(f) a policy on supporting academic and research institutions ***to develop*** cybersecurity tools and secure network infrastructure;	(f) a policy on supporting academic and research institutions ***in cybersecurity research and in the development of*** cybersecurity tools and secure network infrastructure;

Amendment 23

Proposal for a directive
Article 5 – paragraph 2 – point h

Text proposed by the Commission	*Amendment*
(h) a policy addressing specific needs of ***SMEs***, in particular those excluded from the scope of this Directive, in relation to guidance and support in improving their resilience to cybersecurity threats***.***	(h) a policy addressing specific needs of ***start-ups, SMEs and NGOs***, in particular those excluded from the scope of this Directive, in relation to guidance and support in improving their resilience to cybersecurity threats***, responding to cybersecurity incidents, and seeking cybersecurity assistance;***

Amendment 24

Proposal for a directive
Article 5 – paragraph 2 – point h a (new)

Text proposed by the Commission	*Amendment*
	(ha) a policy to promote the use and development of open source software.

Amendment 25

Proposal for a directive
Article 6 – paragraph 1

Text proposed by the Commission	*Amendment*
1. Each Member State shall designate one of its CSIRTs as referred to in Article 9 as a coordinator for the purpose of ***coordinated*** vulnerability disclosure. The designated CSIRT shall act as a trusted intermediary, facilitating, where necessary, the interaction between the reporting entity and the manufacturer or provider of ICT products or ICT services. Where the reported vulnerability concerns multiple manufacturers or providers of ICT products or ICT services across the Union, the designated CSIRT of each Member State concerned shall cooperate with the CSIRT network.	1. Each Member State shall designate one of its CSIRTs as referred to in Article 9 as a coordinator for the purpose of ***mandatory responsible*** vulnerability disclosure. The designated CSIRT shall act as a trusted intermediary, facilitating, where necessary, the interaction between the reporting entity and the manufacturer or provider of ICT products or ICT services. Where the reported vulnerability concerns multiple manufacturers or providers of ICT products or ICT services across the Union, the designated CSIRT of each Member State concerned shall cooperate with the CSIRT network.

Amendment 26

Proposal for a directive
Article 6 – paragraph 2

Text proposed by the Commission	*Amendment*
2. ENISA shall develop and maintain a European vulnerability registry. To that end, ENISA shall establish and maintain the appropriate information systems, policies and procedures with a view in particular to enabling important and essential entities and their suppliers of network and information systems to disclose and register vulnerabilities present in ICT products or ICT services, as well as to provide access to the information on vulnerabilities contained in the registry to all interested parties. The registry shall, in particular, include information describing the vulnerability, the affected ICT product or ICT services and the severity of the vulnerability in terms of the circumstances under which it may be exploited, the availability of related patches and, in the absence of available patches, guidance	2. ENISA shall develop and maintain a European vulnerability registry. To that end, ENISA shall establish and maintain the appropriate information systems, policies and procedures with a view in particular to enabling important and essential entities and their suppliers of network and information systems to disclose and register vulnerabilities present in ICT products or ICT services, as well as to provide access to the information on vulnerabilities contained in the registry to all interested parties. ***In accordance with Article 10(2), CSIRTs shall facilitate access to information on vulnerabilities registered in the European vulnerability registry, alongside risk mitigation assistance, to entities that do not fall within the scope of this Directive, in particular start-ups, SMEs and NGOs.***

addressed to users of vulnerable products and services as to how the risks resulting from disclosed vulnerabilities may be mitigated.	The registry shall, in particular, include information describing the vulnerability, the affected ICT product or ICT services and the severity of the vulnerability in terms of the circumstances under which it may be exploited, the availability of related patches and, in the absence of available patches, guidance addressed to users of vulnerable products and services as to how the risks resulting from disclosed vulnerabilities may be mitigated.

Amendment 27

Proposal for a directive
Article 7 – paragraph 3 – point f

Text proposed by the Commission	*Amendment*
(f) national procedures and arrangements between relevant national authorities and bodies to ensure the Member State's effective participation in and support of the coordinated management of large-scale cybersecurity incidents and crises at Union level.	(f) national procedures and arrangements between relevant national authorities and bodies to ensure the Member State's effective participation in and support of the coordinated management of large-scale cybersecurity incidents and crises at Union level***, including responses to relevant requests under the solidarity clause***.

Amendment 28

Proposal for a directive
Article 7 – paragraph 4

Text proposed by the Commission	*Amendment*
4. Member States shall communicate to the Commission the designation of their competent authorities referred to in paragraph 1 and submit their national cybersecurity incident and crisis response plans as referred to in paragraph 3 within three months from that designation and the adoption of those plans. Member States may exclude specific information from the plan where and to the extent that it is strictly necessary for their national	4. Member States shall communicate to the Commission the designation of their competent authorities referred to in paragraph 1 and submit their national cybersecurity incident and crisis response plans as referred to in paragraph 3 within three months from that designation and the adoption of those plans. Member States may exclude specific information from the plan where and to the extent that it is strictly necessary for their national

security.	security. ***In the event of a large-scale cybersecurity incident and crisis involving more than one Member State, and with relevance to the Union level, appropriate crisis management and governance shall be established. Such structures shall organise exchange of information, coordination and cooperation with the Union's external security and military crisis management structures, and Member States's bodies in charge of security and defence.***

Amendment 29

Proposal for a directive
Article 9 – paragraph 4 a (new)

Text proposed by the Commission	*Amendment*
	4a. CSIRTs shall cooperate and exchange relevant information with national institutions responsible for the maintenance of public security, defence, and national security.

Amendment 30

Proposal for a directive
Article 9 – paragraph 4 b (new)

Text proposed by the Commission	*Amendment*
	4b. CSIRTs shall cooperate and, without prejudice to Union law, in particular Regulation (EU) 2016/679, exchange relevant information with trusted third countries and international organisations on cyber threats, vulnerabilities, best practices, and standards.

Amendment 31

Proposal for a directive
Article 9 – paragraph 4 c (new)

Text proposed by the Commission	*Amendment*
	4c. CSIRTs shall, without prejudice to Union law, in particular Regulation (EU) 2016/679, provide cybersecurity assistance to CSIRTs or equivalent structures in Union candidate countries and to other third countries in the Western Balkans and the Eastern Partnership.

Amendment 32

Proposal for a directive
Article 10 – paragraph 2 – point e a (new)

Text proposed by the Commission	*Amendment*
	(ea) establishing free-of-charge or accessible cybersecurity assistance, education, and audit programs for entities that fall outside the scope of this Directive, in particular start-ups, SMEs and NGOs;

Amendment 33

Proposal for a directive
Article 11 – paragraph 4

Text proposed by the Commission	*Amendment*
4. To the extent necessary to effectively carry out the tasks and obligations laid down in this Directive, Member States shall ensure appropriate cooperation between the competent authorities and single points of contact and law enforcement authorities, data protection authorities, and the authorities responsible for critical infrastructure pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] and the national financial authorities designated in accordance with Regulation (EU) XXXX/XXXX of the European Parliament and of the Council[39] [the	4. To the extent necessary to effectively carry out the tasks and obligations laid down in this Directive, Member States shall ensure appropriate cooperation between the competent authorities and single points of contact and law enforcement authorities, data protection authorities***, national supervisory authorities for artificial intelligence, national competent authorities for data governance***, and the authorities responsible for critical infrastructure pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] and the national financial authorities designated in

DORA Regulation] within that Member State.	accordance with Regulation (EU) XXXX/XXXX of the European Parliament and of the Council[39] [the DORA Regulation] within that Member State.
[39] [insert the full title and OJ publication reference when known]	[39] [insert the full title and OJ publication reference when known]

Amendment 34

Proposal for a directive
Article 12 – paragraph 3 – introductory part

Text proposed by the Commission	*Amendment*
3. The Cooperation Group shall be composed of representatives of Member States, the Commission ***and*** ENISA. The European External Action Service shall participate in the activities of the Cooperation Group as an observer. The European Supervisory Authorities (ESAs) in accordance with Article 17(5)(c) of Regulation (EU) XXXX/XXXX [the DORA Regulation] ***may*** participate in the activities of the Cooperation Group.	3. The Cooperation Group shall be composed of representatives of Member States, the Commission***, EU – CyCLONe,*** ENISA***, and the European Defence Agency***. The European External Action Service shall participate in the activities of the Cooperation Group as an observer. ***National supervisory authorities for artificial intelligence, national competent authorities for data governance, and*** the European Supervisory Authorities (ESAs) in accordance with Article 17(5)(c) of Regulation (EU) XXXX/XXXX [the DORA Regulation] ***shall*** participate in the activities of the Cooperation Group.

Amendment 35

Proposal for a directive
Article 12 – paragraph 4 – point e a (new)

Text proposed by the Commission	*Amendment*
	(ea) without prejudice to Union law, engaging in cooperation, mutual assistance, and exchanging best practices and information with trusted third countries and international organisations;

Amendment 36

Proposal for a directive
Article 13 – paragraph 3 – point k

Text proposed by the Commission	*Amendment*
(k) cooperating and exchanging information with regional and Union-level Security Operations Centres (SOCs) in order to improve common situational awareness on incidents and threats across the Union;	(k) cooperating and exchanging information with regional and Union-level Security Operations Centres (SOCs) ***and, where appropriate, with military CERTs*** in order to improve common situational awareness on incidents and threats across the Union;

Amendment 37

Proposal for a directive
Article 14 – paragraph 2

Text proposed by the Commission	*Amendment*
2. EU-CyCLONe shall be composed of the representatives of Member States' crisis management authorities designated in accordance with Article 7, the Commission and ENISA. ENISA shall provide the secretariat of the network and support the secure exchange of information.	2. EU-CyCLONe shall be composed of the representatives of Member States' crisis management authorities designated in accordance with Article 7, the Commission***, the EEAS*** and ENISA. ENISA shall provide the secretariat of the network and support the secure exchange of information. ***Such national crisis management authorities shall be provided by advice by a civil society based advisory group. For large-scale cybersecurity incidents and crises at Union level involving more than one Member State, a Union level crisis management structure involving all relevant actors shall be established. That structure shall include Joint Cyber Unit, CSIRTs, the CSIRTs network, the Coordination Group, the Commission, the EEAS and ENISA. It shall also prepare and implement the invoking and use of the solidarity clause.***

Amendment 38

Proposal for a directive
Article 14 – paragraph 3 – point a

Text proposed by the Commission	*Amendment*
(a) increasing the level of preparedness of the management of large scale incidents and crises;	(a) increasing the level of preparedness of the management of large scale incidents and crises ***and liaising with Member State agencies in charge of state security and territorial defence***;

Amendment 39

Proposal for a directive
Article 17 – paragraph 2

Text proposed by the Commission	*Amendment*
2. Member States shall ensure that members of the management body follow specific trainings, on a regular basis, to gain sufficient knowledge and skills in order to apprehend and assess cybersecurity risks and management practices and their impact on the operations of the entity.	2. Member States shall ensure that members of the management body follow specific trainings, on a regular basis, to gain sufficient knowledge and skills in order to apprehend and assess cybersecurity risks and management practices and their impact on the operations of the entity. ***Member States shall encourage essential and important entities to evaluate, on a regular basis, members of the management bodies referenced in paragraph 1 of this Article on the adequacy of their skills for ensuring compliance with Article 18.***

Amendment 40

Proposal for a directive
Article 18 – paragraph 3

Text proposed by the Commission	*Amendment*
3. Member States shall ensure that, where considering appropriate measures referred to in point (d) of paragraph 2, entities shall take into account the vulnerabilities specific to each supplier and service provider and the overall quality of products and cybersecurity practices of their suppliers and service providers, including their secure development procedures.	3. Member States shall ensure that, where considering appropriate measures referred to in point (d) of paragraph 2, entities shall take into account the vulnerabilities specific to each supplier and service provider and the overall quality of products and cybersecurity practices of their suppliers and service providers, including their secure development procedures ***in accordance with Union***

	cybersecurity standards and law and potential non-technical risk factors, such as concealed vulnerabilities or backdoors and potential systemic supply disruptions.

Amendment 41

Proposal for a directive
Article 19 – paragraph 1

Text proposed by the Commission	*Amendment*
1. The Cooperation Group, in cooperation with the Commission ***and*** ENISA, may carry out coordinated security risk assessments of specific critical ICT services, systems or products supply chains, taking into account technical and, where relevant, non-technical risk factors.	1. The Cooperation Group, in cooperation with the Commission***,*** ENISA ***and the European External Action Service***, may carry out coordinated security risk assessments of specific critical ICT services, systems or products supply chains, taking into account technical and, where relevant, non-technical risk factors.

Amendment 42

Proposal for a directive
Article 19 – paragraph 2

Text proposed by the Commission	*Amendment*
2. The Commission, after consulting with the Cooperation Group ***and*** ENISA, shall identify the specific critical ICT services, systems or products that may be subject to the coordinated risk assessment referred to in paragraph 1.	2. The Commission, after consulting with the Cooperation Group***,*** ENISA ***and the European External Action Service***, shall identify the specific critical ICT services, systems or products that may be subject to the coordinated risk assessment referred to in paragraph 1.

Amendment 43

Proposal for a directive
Article 19 – paragraph 2 a (new)

Text proposed by the Commission	*Amendment*
	2a. Upon identifying risks to specific critical ICT services, systems or production supply chains, the

	Commission, after consulting the Cooperation Group, ENISA, and the European External Action Service shall issue recommendations to Member States and the national competent authorities defined in this Regulation for remedying and increasing resilience to the identified risks.

Amendment 44

Proposal for a directive
Article 25 – paragraph 1 – point c a (new)

Text proposed by the Commission	*Amendment*
	(ca) information on the management body responsible for the cybersecurity risk management measures laid down in Article 18, in accordance with Article 17;

Amendment 45

Proposal for a directive
Article 29 – paragraph 2 – point c

Text proposed by the Commission	*Amendment*
(c) targeted security audits based on risk assessments or risk-related available information;	(c) targeted security audits based on risk assessments or risk-related available information***, including on risks related to supply chains as defined in Article 18(3)***;

Amendment 46

Proposal for a directive
Article 30 – paragraph 2 – point b

Text proposed by the Commission	*Amendment*
(b) targeted security audits based on risk assessments or risk-related available information;	(b) targeted security audits based on risk assessments or risk-related available information***, including on risks related to supply chains as defined in Article 18(3)***;

Amendment 47

Proposal for a directive
Annex I – ESSENTIAL ENTITIES: SECTORS, SUBSECTORS AND TYPES OF ENTITIES – Sector 6 a (new)

Text proposed by the Commission	*Amendment*
	6a. Education and research — Higher education institutions and research institutions

Amendment 48

Proposal for a directive
Annex I – ESSENTIAL ENTITIES: SECTORS, SUBSECTORS AND TYPES OF ENTITIES – Sector 9 Public administration – Type of entities

Text proposed by the Commission	*Amendment*
– Public administration entities of central governments	– Public administration entities of central governments
– Public administration entities of NUTS level 1 regions listed in Annex I of Regulation (EC) No 1059/2003 ([27])	– Public administration entities of NUTS level 1 regions listed in Annex I of Regulation (EC) No 1059/2003 ([27, 27 a (new)])
– Public administration entities of NUTS level 2 regions listed in Annex I of Regulation (EC) No 1059/2003	– Public administration entities of NUTS level 2 regions listed in Annex I of Regulation (EC) No 1059/2003 ***(27 b (new))***
[27] Regulation (EC) No 1059/2003 of the European Parliament and of the Council of 26 May 2003 on the establishment of a common classification of territorial units for statistics (NUTS) (OJ L 154, 21.6.2003, p. 1).	[27] Regulation (EC) No 1059/2003 of the European Parliament and of the Council of 26 May 2003 on the establishment of a common classification of territorial units for statistics (NUTS) (OJ L 154, 21.6.2003, p. 1). ***27 a (new) Or the equivalent administrative units, in Member States where the NUTS classification is not yet reflected in the administration institutional setup.*** ***27 b (new) Or the equivalent administrative units, in Member States where the NUTS classification is not yet reflected in the administration institutional setup.***

PROCEDURE – COMMITTEE ASKED FOR OPINION

Title	Measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148
References	COM(2020)0823 – C9-0422/2020 – 2020/0359(COD)
Committee responsible Date announced in plenary	ITRE 21.1.2021
Opinion by Date announced in plenary	AFET 21.1.2021
Rapporteur for the opinion Date appointed	Markéta Gregorová 22.2.2021
Discussed in committee	25.5.2021 16.6.2021 17.6.2021
Date adopted	14.7.2021
Result of final vote	+: 59 –: 5 0: 6
Members present for the final vote	Alviina Alametsä, Alexander Alexandrov Yordanov, Maria Arena, Petras Auštrevičius, Traian Băsescu, Anna Bonfrisco, Reinhard Bütikofer, Fabio Massimo Castaldo, Susanna Ceccardi, Włodzimierz Cimoszewicz, Katalin Cseh, Tanja Fajon, Anna Fotyga, Michael Gahler, Giorgos Georgiou, Sunčana Glavak, Raphaël Glucksmann, Klemen Grošelj, Bernard Guetta, Márton Gyöngyösi, Andrzej Halicki, Sandra Kalniete, Dietmar Köster, Maximilian Krah, Andrius Kubilius, Ilhan Kyuchyuk, David Lega, Miriam Lexmann, Nathalie Loiseau, Antonio López-Istúriz White, Jaak Madison, Claudiu Manda, Thierry Mariani, Vangelis Meimarakis, Sven Mikser, Francisco José Millán Mon, Javier Nart, Urmas Paet, Demetris Papadakis, Kostas Papadakis, Tonino Picula, Manu Pineda, Giuliano Pisapia, Thijs Reuten, Jérôme Rivière, María Soraya Rodríguez Ramos, Nacho Sánchez Amor, Isabel Santos, Jacek Saryusz-Wolski, Andreas Schieder, Radosław Sikorski, Jordi Solé, Sergei Stanishev, Tineke Strik, Hermann Tertsch, Hilde Vautmans, Harald Vilimsky, Idoia Villanueva Ruiz, Viola Von Cramon-Taubadel, Thomas Waitz, Witold Jan Waszczykowski, Charlie Weimers, Isabel Wiseler-Lima, Salima Yenbou, Željana Zovko
Substitutes present for the final vote	Ioan-Rareş Bogdan, Andrey Kovatchev, Marisa Matias, Gabriel Mato, Milan Zver

FINAL VOTE BY ROLL CALL IN COMMITTEE ASKED FOR OPINION

59	+
ECR	Anna Fotyga, Jacek Saryusz-Wolski, Hermann Tertsch, Witold Jan Waszczykowski
ID	Anna Bonfrisco, Susanna Ceccardi
NI	Fabio Massimo Castaldo, Márton Gyöngyösi
PPE	Alexander Alexandrov Yordanov, Traian Băsescu, Ioan-Rareş Bogdan, Michael Gahler, Sunčana Glavak, Andrzej Halicki, Sandra Kalniete, Andrey Kovatchev, Andrius Kubilius, David Lega, Miriam Lexmann, Antonio López-Istúriz White, Gabriel Mato, Vangelis Meimarakis, Francisco José Millán Mon, Radosław Sikorski, Isabel Wiseler-Lima, Željana Zovko, Milan Zver
Renew	Petras Auštrevičius, Katalin Cseh, Klemen Grošelj, Bernard Guetta, Ilhan Kyuchyuk, Nathalie Loiseau, Javier Nart, Urmas Paet, María Soraya Rodríguez Ramos, Hilde Vautmans
S&D	Maria Arena, Włodzimierz Cimoszewicz, Tanja Fajon, Raphaël Glucksmann, Dietmar Köster, Claudiu Manda, Sven Mikser, Demetris Papadakis, Tonino Picula, Giuliano Pisapia, Thijs Reuten, Nacho Sánchez Amor, Isabel Santos, Andreas Schieder, Sergei Stanishev
Verts/ALE	Alviina Alametsä, Reinhard Bütikofer, Jordi Solé, Tineke Strik, Viola Von Cramon-Taubadel, Thomas Waitz, Salima Yenbou

5	-
NI	Kostas Papadakis
The Left	Giorgos Georgiou, Marisa Matias, Manu Pineda, Idoia Villanueva Ruiz

6	0
ECR	Charlie Weimers
ID	Maximilian Krah, Jaak Madison, Thierry Mariani, Jérôme Rivière, Harald Vilimsky

Key to symbols:
+ : in favour
- : against
0 : abstention