European Parliament
2019-2024

Committee on Foreign Affairs

2020/0359(COD)

3.5.2021

DRAFT 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.

[13] Article 12 of Directive (EU) 2016/1148.

[12] Article 11 of Directive (EU) 2016/1148.

[13] Article 12 of Directive (EU) 2016/1148.

Or. en

Amendment 2

Proposal for a directive
Recital 3 a (new)

Text proposed by the Commission	*Amendment*
	(3 a) 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 unload 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]. Such large-scale cybersecurity incidents and crises at Union level 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

Or. en

Amendment 3

Proposal for a directive
Recital 3 b (new)

Text proposed by the Commission	*Amendment*
	(3 b) 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. 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 operations and missions conducted by the Union to ensure peace and stability in its neighbourhood and beyond.

Or. en

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 Protocol[14] , are of relevance.	(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***. Independently of the technological environment of the day, it is essential to always fully respect due process and other safeguards, as well as fundamental rights, in particular the right to the respect for private life and communications and the right to the protection of personal data***. 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).

Or. en

Amendment 5

Proposal for a directive
Recital 14 a (new)

Text proposed by the Commission	*Amendment*
	(14 a) In view of the development of a secure connectivity system, building 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, any future possible development should take into account the entire electronic communications infrastructure such as space, land and submarine network systems.

Or. en

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. 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.

Or. en

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***.

Or. en

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	(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

Union institutions, bodies and agencies should cooperate at technical, operational and political level to properly coordinate the response across the Union.	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).

Or. en

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***.

Or. en

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 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.	(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 EU INTCEN, to advance strategic intelligence cooperation on cyber threats and activities, in order to further support Union situational awareness and 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 Common Security and Defence Policy (CSDP) dimension, the European External Action Service (EEAS) Crisis Response Mechanism (CRM) should be activated***, as well as any measure aiming to protect Common Security and Defence Policy***

missions and operations and Union delegations.

Or. en

Amendment 11

Proposal for a directive
Recital 40 a (new)

Text proposed by the Commission	*Amendment*
	(40 a) Member States should consider an active cyber defense programme to be part of their national cybersecurity strategy. 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.

Or. en

Amendment 12

Proposal for a directive
Recital 40 b (new)

Text proposed by the Commission	*Amendment*
	(40 b) 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.

Or. en

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 ***financial health, their commitment to other customers, their risk-management systems, their staff recruitment and retention, their delivery performance and their*** secure development procedures.

Or. en

Amendment 14

Proposal for a directive
Recital 43 a (new)

Text proposed by the Commission	*Amendment*
	(43 a) 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.

Or. en

Amendment 15

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

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

Or. en

Amendment 16

Proposal for a directive
Article 6 – title

Text proposed by the Commission	*Amendment*
6 ***Coordinated*** vulnerability disclosure and a European vulnerability registry	6 ***Mandatory responsible*** vulnerability disclosure and a European vulnerability registry

Or. en

Amendment 17

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.

Or. en

Amendment 18

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***.

Or. en

Amendment 19

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 security.	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. ***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 mangement structures, and Member States's bodies in charge of external security and territorial defence.***

Or. en

Amendment 20

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*** 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] ***shall*** participate in the activities of the Cooperation Group.

Or. en

Amendment 21

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 advised 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 shall be established. That structure shall include 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.***

Or. en

Amendment 22

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***;

Or. en