European Parliament
2019-2024

Committee on Industry, Research and Energy

2020/0359(COD)

3.5.2021

***I
DRAFT REPORT

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
(COM(2020)0823 – C9-0422/2020 – 2020/0359(COD))

Committee on Industry, Research and Energy

Rapporteur: Bart Groothuis

Symbols for procedures

*	Consultation procedure
***	Consent procedure
***I	Ordinary legislative procedure (first reading)
***II	Ordinary legislative procedure (second reading)
***III	Ordinary legislative procedure (third reading)

(The type of procedure depends on the legal basis proposed by the draft act.)

Amendments to a draft act

Amendments by Parliament set out in two columns

Deletions are indicated in ***bold italics*** in the left-hand column. Replacements are indicated in ***bold italics*** in both columns. New text is indicated in ***bold italics*** in the right-hand column.

The first and second lines of the header of each amendment identify the relevant part of the draft act under consideration. If an amendment pertains to an existing act that the draft act is seeking to amend, the amendment heading includes a third line identifying the existing act and a fourth line identifying the provision in that act that Parliament wishes to amend.

Amendments by Parliament in the form of a consolidated text

New text is highlighted in ***bold italics***. Deletions are indicated using either the ▌ symbol or strikeout. Replacements are indicated by highlighting the new text in ***bold italics*** and by deleting or striking out the text that has been replaced.
By way of exception, purely technical changes made by the drafting departments in preparing the final text are not highlighted.

CONTENTS

Page

DRAFT EUROPEAN PARLIAMENT LEGISLATIVE RESOLUTION

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
(COM(2020)0823 – C9-0422/2020 – 2020/0359(COD))

(Ordinary legislative procedure: first reading)

The European Parliament,

– having regard to the Commission proposal to Parliament and the Council (COM(2020)0823),

– having regard to Article 294(2) and Article 114 of the Treaty on the Functioning of the European Union, pursuant to which the Commission submitted the proposal to Parliament (C9-0422/2020),

– having regard to Article 294(3) of the Treaty on the Functioning of the European Union,

– having regard to the opinion of the of the European Economic and Social Committee of [xx xx 2021][1],

– after consulting the Committee of the Regions,

– having regard to Rule 59 of its Rules of Procedure,

– having regard to the opinions of the Committee on Foreign Affairs, Committee on the Internal Market and Consumer Protection, Committee on Transport and Tourism and the Committee on Civil Liberties, Justice and Home Affairs,

– having regard to the report of the Committee on Industry, Research and Energy (A9-0000/2021),

1. Adopts its position at first reading hereinafter set out;

2. Calls on the Commission to refer the matter to Parliament again if it replaces, substantially amends or intends to substantially amend its proposal;

3. Instructs its President to forward its position to the Council, the Commission and the national parliaments.

[1] OJ C 0, 0.0.0000, p. 0.

Amendment 1

Proposal for a directive
Recital 15

Text proposed by the Commission	*Amendment*
(15) Upholding and preserving a reliable, resilient and secure domain name system (DNS) is a key factor in maintaining the integrity of the Internet and is essential for its continuous and stable operation, on which the digital economy and society depend. Therefore, this Directive should apply to ***all providers of DNS services along the DNS resolution chain, including operators of root name servers,*** top-level-domain (TLD) name servers, authoritative ***name servers for*** domain ***names and recursive resolvers***.	(15) Upholding and preserving a reliable, resilient and secure domain name system (DNS) is a key factor in maintaining the integrity of the Internet and is essential for its continuous and stable operation, on which the digital economy and society depend. Therefore, this Directive should apply to top-level-domain (TLD) name servers, ***recursive domain name resolution services for internet end-users and*** authoritative domain ***name resolution services as a service procurable by third-party entities***.

Or. en

Justification

Distinguishing between recursive and authoritative domain services is necessary in order to exclude from the scope organisations that run their own DNS, including individual computer enthusiast. Root name servers should be out of scope; regulating them is contrary to the EU's vision of a "single, open, neutral, free, secure and un-fragmented network" and could encourage and empower states advocating for a top-down, state-controlled Internet governance approach, instead of the multi-stakeholder approach.

Amendment 2

Proposal for a directive
Recital 25

Text proposed by the Commission	*Amendment*
(25) As regards personal data, CSIRTs should be able to provide, in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council[19] as regards personal data, on behalf of and upon request by an entity under this Directive, a proactive scanning of the network and information systems used for	(25) As regards personal data, CSIRTs should be able to provide, in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council[19] as regards personal data, on behalf of and upon request by an entity under this Directive***, or in case of a serious threat to national security***, a proactive scanning of

the provision of their services. Member States should aim at ensuring an equal level of technical capabilities for all sectorial CSIRTs. Member States may request the assistance of the European Union Agency for Cybersecurity (ENISA) in developing national CSIRTs.	the network and information systems used for the provision of their services. Member States should aim at ensuring an equal level of technical capabilities for all sectorial CSIRTs. Member States may request the assistance of the European Union Agency for Cybersecurity (ENISA) in developing national CSIRTs.
[19] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).	[19] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

Or. en

Amendment 3

Proposal for a directive
Recital 27 a (new)

Text proposed by the Commission	*Amendment*
	(27a) Member States should, in their national cybersecurity strategies, address specific cybersecurity needs of small and medium-sized enterprises (SMEs). SMEs are struggling to adapt to new business practices in a more connected world, navigating the digital environment, with employees working from home and business increasingly being conducted online. Some SMEs face specific cybersecurity challenges such as low cyber-awareness, a lack of remote IT security, the high cost of cybersecurity solutions and an increased level of threat, such as ransomeware, for which they should receive guidance and support. Member States should have a cybersecurity point of contact for SMEs, that either provides guidance and support

to SMEs or guides them to the right entities for guidance and support on cybersecurity related issues. Member States should also offer SMEs services such as website configuration and logging enabling.

Or. en

Amendment 4

Proposal for a directive
Recital 27 b (new)

Text proposed by the Commission	*Amendment*
	(27b) Member States should adopt policies on the promotion of active cyber defence as part of their national cybersecurity strategies. Active cyber defence is the proactive prevention, detection, monitoring, analysis and mitigation of network security breaches in real time, combined with the use of capabilities deployed outside the victim network. The ability to rapidly and automatically share and understand threat information and analysis, cyber activity alerts, and response action is critical to enabling a unity of effort in successfully detecting, preventing and addressing cyber-attacks.

Or. en

Amendment 5

Proposal for a directive
Recital 30

Text proposed by the Commission	*Amendment*
(30) Access to correct and timely information on vulnerabilities affecting ICT products and services contributes to an	(30) Access to correct and timely information on vulnerabilities affecting ICT products and services contributes to an

enhanced cybersecurity risk management. In that regard, sources of publicly available information on vulnerabilities are an important tool for entities and their users, but also national competent authorities and CSIRTs. For this reason, ENISA should establish a vulnerability ***registry*** where, essential and important entities and their suppliers, as well as entities which do not fall in the scope of application of this Directive may, on a voluntary basis, disclose vulnerabilities and provide the vulnerability information that allows users to take appropriate mitigating measures.

enhanced cybersecurity risk management. In that regard, sources of publicly available information on vulnerabilities are an important tool for entities and their users, but also national competent authorities and CSIRTs. For this reason, ENISA should establish a vulnerability ***database*** where, essential and important entities and their suppliers, as well as entities which do not fall in the scope of application of this Directive may, on a voluntary basis, disclose vulnerabilities and provide the vulnerability information that allows users to take appropriate mitigating measures. ***The aim of that database is to address the unique challenges posed by cybersecurity risks to European entities. Furthermore, ENISA should establish a procedure regarding the publication process, in order to give entities the time to take mitigating measures as regards their vulnerabilities.***

Or. en

Amendment 6

Proposal for a directive
Recital 31

Text proposed by the Commission	*Amendment*
(31) ***Although similar vulnerability registries or databases do exist, these are hosted and maintained by entities which are not established in the Union. A*** European vulnerability registry ***maintained by ENISA would provide improved transparency regarding the publication process before the vulnerability is officially disclosed, and resilience in cases of disruptions or interruptions on the provision of similar services***. To avoid duplication of efforts and seek complementarity to the extent possible, ENISA should explore the possibility of entering into structured cooperation	(31) ***The*** European vulnerability ***database should leverage the global Common Vulnerabilities and Exposures (CVE)*** registry***, which comprises a list of records for international publicly known cybersecurity vulnerabilities***. To avoid duplication of efforts and seek complementarity to the extent possible, ENISA should explore the possibility of entering into structured cooperation agreements with ***the CVE registry and other*** similar registries in third country jurisdictions.

agreements with similar registries in third country jurisdictions.

Or. en

Justification

CVE records are used in numerous cybersecurity services and products around the world, including many national databases. Structured cooperation agreements could include joining the board of the CVE or becoming a 'root CVE Numbering Authority'.

Amendment 7

Proposal for a directive
Recital 38

Text proposed by the Commission	*Amendment*
(38) For the purposes of this Directive, the term 'risk' should refer to the potential for loss or disruption caused by a cybersecurity incident and should be expressed as a combination of the magnitude of such loss or disruption and the likelihood of occurrence of said incident.	***deleted***

Or. en

Justification

Moved to article 4.

Amendment 8

Proposal for a directive
Recital 39

Text proposed by the Commission	*Amendment*
(39) For the purposes of this Directive, the term 'near misses' should refer to an event which could potentially have caused harm, but was successfully prevented from fully transpiring.	***deleted***

Or. en

Justification

Moved to article 4.

Amendment 9

Proposal for a directive
Recital 44

Text proposed by the Commission	*Amendment*
(44) Among service providers, managed security services providers (MSSPs) in areas such as incident response, penetration testing, security audits and consultancy play a particularly important role in assisting entities in their efforts to detect and respond to incidents. Those MSSPs have however also been the targets of cyberattacks themselves and through their close integration in the operations of operators pose a particular cybersecurity risk. Entities should therefore exercise increased diligence in selecting an MSSP.	(44) Among service providers, managed security services providers (MSSPs) in areas such as incident response, penetration testing, security audits and consultancy play a particularly important role in assisting entities in their efforts to ***prevent,*** detect and respond to incidents. Those MSSPs have however also been the targets of cyberattacks themselves and through their close integration in the operations of operators pose a particular cybersecurity risk. Entities should therefore exercise increased diligence in selecting an MSSP.

Or. en

Amendment 10

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 involving relevant national authorities, in cooperation with the Commission and ENISA, should carry out coordinated ***sectoral*** supply chain risk assessments, as was already done for 5G networks	(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 and ENISA, should carry out coordinated supply chain risk assessments, as was already done for 5G networks following

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.

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. ***The Cooperation Group should also identify measures and mitigation plans against critical dependencies, potential single points of failure, 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).

Or. en

Justification

Supply chain risk assessments should not necessarily be sectoral. There should also be the possibility to assess a critical service provider or a specific supplier. Apart from identifying the risks, the Cooperation Group should also bring forward measures and mitigation plans to deal with the risks.

Amendment 11

Proposal for a directive
Recital 51

Text proposed by the Commission

(51) The internal market is more reliant on the functioning of the internet than ever before. The services of virtually all essential and important entities are dependent on services provided over the internet. In order to ensure the smooth provision of services provided by essential and important entities, it is important that public electronic communications networks, such as, for example, internet backbones or submarine communications cables, have appropriate cybersecurity measures in place and report incidents in relation thereto.

Amendment

(51) The internal market is more reliant on the functioning of the internet than ever before. The services of virtually all essential and important entities are dependent on services provided over the internet. In order to ensure the smooth provision of services provided by essential and important entities, it is important that public electronic communications networks, such as, for example, internet backbones or submarine communications cables, have appropriate cybersecurity measures in place and report incidents in relation thereto. ***The protection of internet***

backbones and submarine communication cables from sabotage and espionage should be considered to be of vital security interest. Member States should actively share information about incidents on public electronic communications networks, fall outs and suspected adversarial ship movements.

Or. en

Amendment 12

Proposal for a directive
Recital 52

Text proposed by the Commission	*Amendment*
(52) Where appropriate, entities should inform their service recipients of particular and significant threats and of measures they can take to mitigate the resulting risk to themselves. ***The requirement to inform those recipients of such threats*** should not discharge entities from the obligation to take, at their own expense, appropriate and immediate measures to prevent or remedy any cyber threats and restore the normal security level of the service. The provision of such information about security threats to the recipients should be free of charge.	(52) Where appropriate, entities should inform their service recipients of particular and significant threats and of measures they can take to mitigate the resulting risk to themselves. ***This*** should not discharge entities from the obligation to take, at their own expense, appropriate and immediate measures to prevent or remedy any cyber threats and restore the normal security level of the service. The provision of such information about security threats to the recipients should be free of charge.

Or. en

Justification

There are some scenarios whereby disclosure would not be desirable, because CSIRTs or other authorities are still investigating the threat. Additionally, service recipients could be, for example households, and would be able to do very little with the threat information.

Amendment 13

Proposal for a directive
Recital 54 a (new)

Text proposed by the Commission	*Amendment*
	(54a) In order to safeguard the security and to prevent abuse and manipulation of electronic communications networks and services, the use of interoperable secure routing standards should be promoted to guarantee the integrity and robustness of routing functions across the ecosystem of internet carriers.

Or. en

Justification

Interoperable secure routing standards are for example Resource-PKI.

Amendment 14

Proposal for a directive
Recital 54 b (new)

Text proposed by the Commission	*Amendment*
	(54b) In order to safeguard the functionality and integrity of the internet and to reduce the security issues relating to DNS, relevant stakeholders including Union businesses, internet service providers and browser vendors should be encouraged to adopt a DNS resolution diversification strategy. Furthermore, Member States should encourage the development and use of a public and secure European DNS resolver service.

Or. en

Amendment 15

Proposal for a directive
Recital 54 c (new)

Text proposed by the Commission	*Amendment*
	(54c) DNS service providers should use state-of-the-art security protocols, offer users the possibility to actively avoid resolving malign traffic, should respect privacy and should be discouraged from monetising user data.

Or. en

Amendment 16

Proposal for a directive
Recital 55

Text proposed by the Commission	*Amendment*
(55) This Directive lays down a two-stage approach to incident reporting in order to strike the right balance between, on the one hand, swift reporting that helps mitigate the potential spread of incidents and allows entities to seek support, and, on the other hand, in-depth reporting that draws valuable lessons from individual incidents and improves over time the resilience to cyber threats of individual companies and entire sectors. Where entities become aware of an incident, they should be required to submit an initial notification within ***24*** hours, followed by a ***final*** report not later than one month after. The initial notification should ***only*** include the information strictly necessary to make the competent authorities aware of the incident and allow the entity to seek assistance, if required. Such notification, where applicable, should indicate whether the incident is presumably caused by unlawful or malicious action. Member States should ensure that the requirement to submit this initial notification does not divert the reporting entity's resources from activities related to incident handling that should be prioritised. To further prevent	(55) This Directive lays down a two-stage approach to incident reporting in order to strike the right balance between, on the one hand, swift reporting that helps mitigate the potential spread of incidents and allows entities to seek support, and, on the other hand, in-depth reporting that draws valuable lessons from individual incidents and improves over time the resilience to cyber threats of individual companies and entire sectors. Where entities become aware of an incident, they should be required to submit an initial notification within ***72*** hours, followed by a ***comprehensive*** report not later than one month after. The initial notification should include the information strictly necessary to make the competent authorities aware of the incident and allow the entity to seek assistance, if required. Such notification, where applicable, should indicate whether the incident is presumably caused by unlawful or malicious action. Member States should ensure that the requirement to submit this initial notification does not divert the reporting entity's resources from activities related to incident handling that should be prioritised. To further prevent

that incident reporting obligations either divert resources from incident response handling or may otherwise compromise the entities efforts in that respect, Member States should also provide that, in duly justified cases and in agreement with the competent authorities or the CSIRT, the entity concerned can deviate from the deadlines of ***24*** hours for the initial notification and one month for the ***final*** report.	that incident reporting obligations either divert resources from incident response handling or may otherwise compromise the entities efforts in that respect, Member States should also provide that, in duly justified cases and in agreement with the competent authorities or the CSIRT, the entity concerned can deviate from the deadlines of ***72*** hours for the initial notification and one month for the ***comprehensive*** report.

Or. en

Amendment 17

Proposal for a directive
Recital 59

Text proposed by the Commission	*Amendment*
(59) Maintaining accurate and complete databases of domain names ***and*** registration data (so called 'WHOIS data') ***and providing lawful access to such data*** is essential to ensure the security, stability and resilience of the DNS, which in turn contributes to a high common level of cybersecurity within the Union. Where processing includes personal data such processing shall comply with Union data protection law.	(59) Maintaining accurate***, verified*** and complete databases of domain names registration data (so called 'WHOIS data') is essential to ensure the security, stability and resilience of the DNS, which in turn contributes to a high common level of cybersecurity within the Union. ***In order to ensure the availability of accurate, verified and complete domain name registration data, TLD registries and entities providing domain name registration services should be required to collect domain name registration data. They should aim to ensure the integrity and availability of such data by implementing technical and organisational measures, such as a confirmation process for registrants. In particular, TLD registries and entities providing domain name registration services should establish policies and procedures for the collection and maintenance of accurate, verified and complete registration data, as well as for the prevention and correction of inaccurate registration data.*** Where

processing includes personal data such processing shall comply with Union data protection law.

Or. en

Amendment 18

Proposal for a directive
Recital 60

Text proposed by the Commission	*Amendment*
(60) The availability and timely accessibility of ***these*** data to ***public authorities, including*** competent authorities under Union or national law for the prevention, investigation or prosecution of criminal offences, CERTs, ***(***CSIRTs, and as regards the data of their clients ***to*** providers of electronic communications networks and services and providers of cybersecurity technologies and services ***acting on behalf of those clients, is essential to prevent and combat Domain Name System abuse, in particular to prevent, detect and respond to*** cybersecurity ***incidents***. Such access should comply with Union data protection law insofar as it is related to personal data.	(60) The availability and timely accessibility of ***the domain name registration*** data to ***legitimate access seekers is essential for the purposes of protecting the online ecosystem and preventing DNS abuse, as well as for detecting and preventing crime, protecting minors, protecting intellectual property and protecting against hate speech and fraud. Legitimate access seekers are natural or legal persons making a duly justified request to access to DNS data on the basis of Union or national law, and they may include*** competent authorities under Union or national law for the prevention, investigation or prosecution of criminal offences, CERTs, CSIRTs, and as regards the data of their clients – providers of electronic communications networks and services and providers of cybersecurity technologies and services ***and*** cybersecurity ***researchers***. Such access should comply with Union data protection law insofar as it is related to personal data.

Or. en

Amendment 19

Proposal for a directive
Recital 61

Text proposed by the Commission	*Amendment*
(61) In order to ensure the availability of accurate and complete domain name registration data, TLD registries and the entities providing domain name registration services for the TLD (so-called registrars) should collect and guarantee the integrity and availability of domain names registration data. In particular, TLD registries and the entities providing domain name registration services for the TLD should establish policies and procedures to collect and maintain accurate and complete registration data, as well as to prevent and correct inaccurate registration data in accordance with Union data protection rules.	***deleted***

Or. en

Justification

Moved to recital 59.

Amendment 20

Proposal for a directive
Recital 62

Text proposed by the Commission	*Amendment*
(62) TLD registries and ***the*** entities providing domain name registration services ***for them*** should ***make publically*** available domain name registration data ***that fall outside the scope of Union data protection rules, such as data that concern*** legal persons[25]. TLD registries and ***the*** entities providing domain name registration services ***for the TLD*** should also enable lawful access to specific domain name registration data concerning natural persons to legitimate access seekers, in accordance with Union data	(62) TLD registries and entities providing domain name registration services should ***be required to make publicly*** available domain name registration data ***of*** legal persons[25] ***as registrants upon the registration of a domain***. TLD registries and entities providing domain name registration services should also enable lawful access to specific domain name registration data concerning natural persons to legitimate access seekers, in accordance with Union data protection law. Member States should

protection law. Member States should ensure that TLD registries and ***the*** entities providing domain name registration services ***for them*** should respond without undue delay to requests from legitimate access seekers for the disclosure of domain name registration data. TLD registries and ***the*** entities providing domain name registration services ***for them*** should establish policies and procedures for the publication and disclosure of registration data, including service level agreements to deal with requests for access from legitimate access seekers. The access procedure may also include the use of an interface, portal or other technical tool to provide an efficient system for requesting and accessing registration data. With a view to promoting harmonised practices across the internal market, the Commission may adopt guidelines on such procedures without prejudice to the competences of the European Data Protection Board.	ensure that TLD registries and entities providing domain name registration services should respond without undue delay ***and in any event within 72 hours*** to requests from legitimate access seekers for the disclosure of domain name registration data. TLD registries and entities providing domain name registration services should establish policies and procedures for the publication and disclosure of registration data, including service level agreements to deal with requests for access from legitimate access seekers. The access procedure may also include the use of an interface, portal or other technical tool to provide an efficient system for requesting and accessing registration data. With a view to promoting harmonised practices across the internal market, the Commission may adopt guidelines on such procedures without prejudice to the competences of the European Data Protection Board.
[25] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL recital (14) whereby “this Regulation does not cover the processing of personal data which concerns legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person”.	[25] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL recital (14) whereby “this Regulation does not cover the processing of personal data which concerns legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person”.

Or. en

Amendment 21

Proposal for a directive
Recital 65 a (new)

Text proposed by the Commission	*Amendment*
	(65a) ENISA should create and maintain a registry for essential and important entities that comprise DNS

service providers, TLD name registries and providers of cloud computing services, data centre services, content delivery networks, online marketplaces, online search engines and social networking platforms. Those essential and important entities should submit to ENISA their names, addresses and up-to-date contact details, including their email addresses and telephone numbers. They should notify ENISA about any changes to those details without delay and, in any event, within three months from the date on which the change took effect. ENISA should develop a simple publicly available application programme that those entities can use to update their information.

Or. en

Justification

Following article 25. To prevent administrative red tape, ENISA should develop a simple tool to which entities can easily update their information.

Amendment 22

Proposal for a directive
Recital 66

Text proposed by the Commission	*Amendment*
(66) Where information considered classified according to national or Union law is exchanged, reported or otherwise shared under the provisions of this Directive, the corresponding specific rules on the handling of classified information should be applied.	(66) Where information considered classified according to national or Union law is exchanged, reported or otherwise shared under the provisions of this Directive, the corresponding specific rules on the handling of classified information should be applied. ***In addition, ENISA should have the infrastructure, procedures and rules in place to handle sensitive and classified information in compliance with the applicable security rules for protecting EU classified information.***

Or. en

Amendment 23

Proposal for a directive
Recital 68 a (new)

Text proposed by the Commission	*Amendment*
	(68a) Member States should, in cooperation with ENISA, share best practices in order to facilitate greater voluntary cyber threat information sharing. Such best practices could include the use of tools that automate information sharing, but that also set parameters and standards on information-sharing arrangements, taking into account Union law and safeguarding business-sensitive information.

Or. en

Justification

To help facilitate greater voluntary cyberthreat information sharing, Member States should share best practices. Best practices could include: setting parameters about what type of information can be shared, if and how that information can be further shared beyond the initial recipient, and any limitations on its use. Tools exist that can automate the sharing process and enforce these rules, these are for example TAXII and MISP. Standards such as STIX control what is shared, and how.

Amendment 24

Proposal for a directive
Recital 69

Text proposed by the Commission	*Amendment*
(69) The processing of personal data, to the extent strictly necessary and proportionate for the purposes of ensuring network and information security by entities***, public authorities***, CERTs, CSIRTs***,*** and providers of security technologies and services should ***constitute a*** legitimate ***interest of*** the ***data*** controller ***concerned***, as referred to in Regulation	(69) The processing of personal data, to the extent strictly necessary and proportionate for the purposes of ensuring network and information security by ***essential and important*** entities, CERTs, CSIRTs and providers of security technologies and services***, is necessary for compliance with their legal obligations provided for in this Directive and such***

(EU) 2016/679. ***That should include*** measures related to the prevention, detection, analysis and response to incidents, measures to raise awareness in relation to specific cyber threats, exchange of information in the context of vulnerability remediation and coordinated disclosure, as well as the voluntary exchange of information on those incidents, as well as cyber threats and vulnerabilities, indicators of compromise, tactics, techniques and procedures, cybersecurity alerts and configuration tools***. Such measures may*** require the processing of ***the following types*** of personal data***:*** IP addresses, uniform resources locators (URLs), domain names, ***and*** email addresses.

processing of personal data might also be necessary for the purposes of the legitimate interests pursued by essential and important entities. In that regard, the processing of personal data under this Directive should ***be understood as necessary for compliance with legal obligations on the controller or for the purposes of the*** legitimate ***interests pursued by*** the controller, as referred to in Regulation (EU) 2016/679 ***and should comply with the rules set out in that Regulation***. Measures related to the prevention, detection, analysis and response to incidents, measures to raise awareness in relation to specific cyber threats, exchange of information in the context of vulnerability remediation and coordinated disclosure, as well as the voluntary exchange of information on those incidents, as well as cyber threats and vulnerabilities, indicators of compromise, tactics, techniques and procedures, cybersecurity alerts and configuration tools require the processing of ***certain categories*** of personal data***, such as*** IP addresses, uniform resources locators (URLs), domain names, email addresses***, time stamps, Operation System- or browser-related information, or other information indicating the modus operandi***.

Or. en

Justification

Cybersecurity operations are not data-protection neutral. They require the processing of certain categories of personal data in order to ensure that the protective objective of the cybersecurity requirement is met. For processing of data a legal basis is needed. Such legal basis can be legitimate interest under Article 6(1)(f) of GDPR (for example information sharing for cybersecurity), but will in most cases be compliance to a legal obligation to this directive (article 18 & 20). For those cases the legal basis is the compliance to a legal obligation under Article 6(1)(c) of GDPR.

Amendment 25

Proposal for a directive
Recital 82 a (new)

Text proposed by the Commission	*Amendment*
	(82a) This Directive lays down requirements in the area of cybersecurity for Member States as well as essential and important entities established in the Union. Those cybersecurity requirements should also be applied by the Union institutions, bodies, offices and agencies on the basis of a Union legislative act.

Or. en

Amendment 26

Proposal for a directive
Recital 82 b (new)

Text proposed by the Commission	*Amendment*
	(82b) This Directive creates additional tasks for ENISA and in accordance with Regulation (EU) 2019/881 of the European Parliament and of the Council[1a] ENISA should therefore be granted the necessary human and budgetary resources.
	[1a] Regulation (EU)2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)(OJ L 151, 7.6.2019, p.15).

Or. en

Amendment 27

Proposal for a directive
Article 2 – paragraph 1

Text proposed by the Commission	*Amendment*
1. This Directive applies to public and private entities of a type referred to as essential entities in Annex I and as important entities in Annex II. This Directive does not apply to entities that qualify as micro and small enterprises within the meaning of Commission Recommendation 2003/361/EC.***28***	1. This Directive applies to public and private entities of a type referred to as essential entities in Annex I and as important entities in Annex II. This Directive does not apply to entities that qualify as micro and small enterprises within the meaning of ***Article 2(2) and (3) of the Annex to*** Commission Recommendation 2003/361/EC***28***. ***By way of derogation from Article 3(4) of the Annex to Recommendation 2003/361/EC, entities with a stake of 25% by a public body shall be considered to be SMEs.***
[28] Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36).	[28] Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36).

Or. en

Justification

Art. 3 (4) of the Annex to Commission Recommendation 2003/361/EC excludes enterprises with 25% or more of their capital or voting rights controlled by a public body from the SME status. However, these entities should also be exempt from the scope of this Directive.

Amendment 28

Proposal for a directive
Article 2 – paragraph 6 a (new)

Text proposed by the Commission	*Amendment*
	6a. Essential and important entities, CERTs, CSIRTs and providers of security technologies and services, shall process personal data, to the extent strictly necessary and proportionate for the

purposes of ensuring network and information security, to meet the obligations set out in this Directive. Where this Directive requires the processing of personal data for the purpose of cybersecurity, including for contributing to the security, stability and the resilience of the DNS, that processing is considered to be necessary for compliance with a legal obligation as referred to in point (c) of Article 6(1) of Regulation (EU) 2016/679. For the purpose of Articles 26 and 27 of this Directive, processing, as referred to in point (f) of Article 6(1) of Regulation (EU) 2016/679, is considered to be necessary for the purposes of the legitimate interests pursued by the essential and important entities.

Or. en

Justification

This amendment creates a clear legal basis under GDPR Articles 6(1)(c) in cases where there is an obligation to comply with a requirement of this Directive, while allowing for a legitimate interest legal basis where the Directive gives entities optional choices that benefit cybersecurity, but necessitate the processing of personal data.

Amendment 29

Proposal for a directive
Article 4 – paragraph 1 – point 5 a (new)

Text proposed by the Commission	*Amendment*
	(5a) 'near miss' means an event which could have caused harm, but was successfully prevented from fully transpiring;

Or. en

Justification

Moved from recital to definition.

Amendment 30

Proposal for a directive
Article 4 – paragraph 1 – point 7 a (new)

Text proposed by the Commission	*Amendment*
	(7a) 'risk' means the potential for loss or disruption caused by a cybersecurity incident and is to be expressed as a combination of the magnitude of such loss or disruption and the likelihood of occurrence of that incident;

Or. en

Justification

Moved from recital to definition.

Amendment 31

Proposal for a directive
Article 4 – paragraph 1 – point 11

Text proposed by the Commission	*Amendment*
(11) 'technical specification' means a technical specification ***within the meaning*** of Article ***2(4)*** of Regulation (EU) ***No 1025/2012***;	(11) 'technical specification' means a technical specification ***as defined in point (20)*** of Article ***2*** of Regulation (EU) ***No 2019/881***;

Or. en

Justification

This definition should be brought in line with Art 2 (20) of Regulation for ENISA (2019/881) which says: 'technical specification' means a document that prescribes the technical requirements to be met by, or conformity assessment procedures relating to, an ICT product, ICT service or ICT process'. Directly addressing the ICT field.

Amendment 32

Proposal for a directive
Article 4 – paragraph 1 – point 14

Text proposed by the Commission	*Amendment*
(14) 'DNS service provider' means an entity that provides recursive ***or authoritative*** domain name resolution services to internet end-users ***and other DNS*** service ***providers***;	(14) 'DNS service provider' means an entity that provides***:***
	(a) recursive domain name resolution services to internet end-users***; or***
	(b) authoritative domain name resolution services as a service ***procurable by third-party entities***;

Or. en

Justification

Some organisations operate their own authoritative domain name resolution services for their own domain names. By not distinguishing between recursive and authoritative domain name resolution services this definition would bring many organisations in the scope, that should not be considered essential or important, even including individual computer enthusiast that run their own DNS service.

Amendment 33

Proposal for a directive
Article 4 – paragraph 1 – point 15 a (new)

Text proposed by the Commission	*Amendment*
	(15a) 'domain name registration services' means services provided by domain name registries and registrars, privacy or proxy registration service providers, domain brokers or resellers, and any other services which are related to the registration of domain names;

Or. en

Justification

Access to internet domain name registration data (WHOIS data) is important for cybersecurity, criminal investigations and consumer protection. It is therefore essential that the Directive captures all actors involved in collecting, processing, storing and transferring domain name registration data.

Amendment 34

Proposal for a directive
Article 5 – paragraph 1 – point e

Text proposed by the Commission	*Amendment*
(e) a list of the various authorities and actors involved in the implementation of the national cybersecurity strategy;	(e) a list of the various authorities and actors involved in the implementation of the national cybersecurity strategy***,*** ***including a cybersecurity point of contact for SMEs***;

Or. en

Justification

Following amendment 3. SMEs face specific challenges and should be able to easily access guidance and support.

Amendment 35

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 ***promoting cybersecurity for*** SMEs, ***including*** those excluded from the scope of this Directive, ***addressing their specific needs and providing easily accessed*** guidance and support***;***

Or. en

Justification

Easily accessed through a cybersecurity point of contact.

Amendment 36

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

Text proposed by the Commission	*Amendment*
	(ha) a policy on promoting active cyber defence.

Or. en

Justification

Following amendment 4. Member States should not only react to cybersecurity incidents, but should proactively prevent, detect, analyse and mitigate security breaches.

Amendment 37

Proposal for a directive
Article 6 – title

Text proposed by the Commission	*Amendment*
Coordinated vulnerability disclosure and a European vulnerability ***registry***	Coordinated vulnerability disclosure and a European vulnerability ***database***

Or. en

Amendment 38

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	2. ENISA shall develop and maintain a European vulnerability ***database***. 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 addressed to users of vulnerable products and services as to how the risks resulting from disclosed vulnerabilities may be mitigated.	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 ***database*** 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.

Or. en

Justification

"Database" might be the better term here.

Amendment 39

Proposal for a directive
Article 8 – paragraph 4

Text proposed by the Commission	*Amendment*
4. Each single point of contact shall exercise a liaison function to ensure cross–border cooperation of its Member State's authorities with the relevant authorities in other Member States, as well as to ensure cross-sectorial cooperation with other national competent authorities within its Member State.	4. Each single point of contact shall exercise a liaison function to ensure cross–border cooperation of its Member State's authorities with the relevant authorities in other Member States, ***the Commission and ENISA,*** as well as to ensure cross-sectorial cooperation with other national competent authorities within its Member State.

Or. en

Amendment 40

Proposal for a directive
Article 9 – paragraph 2

Text proposed by the Commission	*Amendment*
2. Member States shall ensure that each CSIRT has adequate resources to carry out effectively their tasks as set out in Article 10(2).	2. Member States shall ensure that each CSIRT has adequate resources ***and is technically enabled*** to carry out effectively their tasks as set out in Article 10(2).

Or. en

Amendment 41

Proposal for a directive
Article 9 – paragraph 6 a (new)

Text proposed by the Commission	*Amendment*
	6a. Member States shall ensure the possibility of effective, efficient and secure information exchange between their own CSIRTs and the CSIRTs from third countries, where information exchange is reciprocal and beneficial to the security of its citizens.

Or. en

Amendment 42

Proposal for a directive
Article 10 – paragraph 1 – point e

Text proposed by the Commission	*Amendment*
(e) CSIRTs shall be equipped with redundant systems and backup working space to ensure continuity of its services;	(e) CSIRTs shall be equipped with redundant systems and backup working space to ensure continuity of its services ***and real-time monitoring capabilities***;

Or. en

Justification

The proposed amendments in Article 10 build on the proposal of the Commission, expanding on the capabilities that mature CSIRTs should have. CSIRTs should be put in a strategic

position to support essential and important entities in detection, crisis management and the handling of incidents.

Amendment 43

Proposal for a directive
Article 10 – paragraph 2 – point a

Text proposed by the Commission	*Amendment*
(a) monitoring cyber threats, vulnerabilities and incidents at national level;	(a) monitoring cyber threats, vulnerabilities and incidents at national level***, including through the real-time or near-real-time monitoring of networks and information systems***;

Or. en

Amendment 44

Proposal for a directive
Article 10 – paragraph 2 – point d

Text proposed by the Commission	*Amendment*
(d) providing dynamic risk and incident analysis and situational awareness regarding cybersecurity;	(d) ***collecting and analysing forensic data and*** providing dynamic risk and incident analysis and situational awareness regarding cybersecurity***, including reverse-engineering cyber threats***;

Or. en

Amendment 45

Proposal for a directive
Article 10 – paragraph 2 – point e

Text proposed by the Commission	*Amendment*
(e) providing, upon request of an entity, a proactive scanning of the network and information systems used for the	(e) providing, upon request of an entity ***or in the case of a serious threat to national security***, a proactive scanning of the network and information systems used

provision of their services;	for the provision of their services;

Or. en

Amendment 46

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

Text proposed by the Commission	*Amendment*
	(fa) protecting data, including personal data, from unauthorised exfiltration and using network logging;

Or. en

Amendment 47

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

Text proposed by the Commission	*Amendment*
	(fb) enforcing authentication and strong access controls;

Or. en

Amendment 48

Proposal for a directive
Article 10 – paragraph 4 – introductory part

Text proposed by the Commission	*Amendment*
4. In order to facilitate cooperation, CSIRTs shall promote the adoption and use of common or standardised practices, classification schemes and taxonomies in relation to the following:	4. In order to facilitate cooperation, CSIRTs shall promote ***automation of information exchange,*** the adoption and use of common or standardised practices, classification schemes and taxonomies in relation to the following:

Or. en

Amendment 49

Proposal for a directive
Article 12 – paragraph 3 – subparagraph 1

Text proposed by the Commission	*Amendment*
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.	The Cooperation Group shall be composed of representatives of Member States, the Commission and ENISA. The ***European Parliament and the*** European External Action Service shall participate in the activities of the Cooperation Group as ***observers***. 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.

Or. en

Justification

The European Parliament may designate an observer to participate in the activities of the Cooperation Group.

Amendment 50

Proposal for a directive
Article 12 – paragraph 8

Text proposed by the Commission	*Amendment*
8. The Cooperation Group shall meet regularly and at least once a year with the Critical Entities Resilience Group established under Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] to ***promote*** strategic cooperation and ***exchange of*** information.	8. The Cooperation Group shall meet regularly and at least once a year with the Critical Entities Resilience Group established under Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] to ***facilitate*** strategic cooperation and information ***exchange***.

Or. en

Amendment 51

Proposal for a directive
Article 13 – paragraph 3 – point b a (new)

Text proposed by the Commission	*Amendment*
	(ba) improving interoperability with regard to information sharing;

Or. en

Amendment 52

Proposal for a directive
Article 15 – paragraph 1 – introductory part

Text proposed by the Commission	*Amendment*
1. ENISA shall issue, in cooperation with the Commission, a biennial report on the state of cybersecurity in the Union. The report shall in particular include an assessment of the following:	1. ENISA shall issue, in cooperation with the Commission, a biennial report on the state of cybersecurity in the Union ***and submit and present it to the European Parliament***. The report shall in particular include an assessment of the following:

Or. en

Amendment 53

Proposal for a directive
Article 18 – paragraph 2 – point b

Text proposed by the Commission	*Amendment*
(b) incident handling (prevention, detection, ***and*** response to incidents);	(b) incident handling (prevention, detection, response to***, and the mitigation of*** incidents);

Or. en

Amendment 54

Proposal for a directive
Article 18 – paragraph 5

Text proposed by the Commission	*Amendment*
5. The Commission may adopt implementing acts in order to lay down the technical and the methodological specifications of the elements referred to in paragraph 2. Where preparing those acts, the Commission shall proceed in accordance with the examination procedure referred to in Article 37(2) and follow, to the greatest extent possible, international and European standards, as well as relevant technical specifications.	***deleted***

Or. en

Amendment 55

Proposal for a directive
Article 18 – paragraph 6

Text proposed by the Commission	*Amendment*
6. The Commission is empowered to adopt delegated acts in accordance with Article 36 to supplement the elements laid down in paragraph 2 to take account of new cyber threats, technological developments or sectorial specificities.	6. The Commission is empowered to adopt delegated acts***,*** in accordance with Article 36***,*** to supplement the elements laid down in paragraph 2 to take account of new cyber threats, technological developments or sectorial specificities ***as well as to supplement this Regulation by laying down the technical and the methodological specifications of the elements referred to in paragraph 2***.

Or. en

Amendment 56

Proposal for a directive
Article 20 – paragraph 1

Text proposed by the Commission	*Amendment*
1. Member States shall ensure that essential and important entities notify, without undue delay, the competent authorities or the CSIRT in accordance with paragraphs 3 and 4 of any incident having a significant impact ***on the provision of their services***. Where appropriate, those entities shall notify, without undue delay, the recipients of their services of incidents that are likely to adversely affect the provision of that service. Member States shall ensure that those entities report, among others, any information enabling the competent authorities or the CSIRT to determine any cross-border impact of the incident.	1. Member States shall ensure that essential and important entities notify, without undue delay, the competent authorities or the CSIRT in accordance with paragraphs 3 and 4 of any incident having a significant impact. Where appropriate, those entities shall notify, without undue delay, the recipients of their services of incidents that are likely to adversely affect the provision of that service. Member States shall ensure that those entities report, among others, any information enabling the competent authorities or the CSIRT to determine any cross-border impact of the incident.

Or. en

Justification

An incident with significant impact does not necessarily have to impact the provision of their services. It could also impact others, industrial competitiveness or national security (economic/political espionage).

Amendment 57

Proposal for a directive
Article 20 – paragraph 2 – subparagraph 1

Text proposed by the Commission	*Amendment*
Member States shall ensure that essential and important entities notify, without undue delay, the competent authorities or the CSIRT of any significant cyber threat that those entities identify that could have potentially resulted in a significant incident.	***deleted***

Or. en

Justification

It is often impossible for an entity to know if a cyber threat "could have potentially resulted in a significant incident." Furthermore, a cyber threat and a report worthy cyber incident are not the same thing, and making the reporting of threats mandatory might undermine cybersecurity. Article 20 should focus on incidents, not threats. Threat reporting/ threat sharing should be encouraged, but on a voluntary basis (Article 26 & 27).

Amendment 58

Proposal for a directive
Article 20 – paragraph 2 – subparagraph 2

Text proposed by the Commission	*Amendment*
Where applicable, those entities shall notify, without undue delay, the recipients of their services that are potentially affected by a significant cyber threat of any measures or remedies that those recipients can take in response to that threat. Where appropriate, the entities shall also notify those recipients of the threat itself. The notification shall not make the notifying entity subject to increased liability.	***deleted***

Or. en

Justification

Moved to article 26.

Amendment 59

Proposal for a directive
Article 20 – paragraph 3 – point a

Text proposed by the Commission	*Amendment*
(a) the incident has caused ***or has the potential to cause*** substantial operational disruption or financial losses for the entity concerned;	(a) the incident has caused substantial operational disruption or financial losses for the entity concerned;

Or. en

Justification

A requirement to report incidents that have the potential to cause harm is unrealistic and could result in competent authorities being overwhelmed by receiving too many notifications, which could divert attention and limited security resources away from the essential tasks of actually examining and handling incidents and securing systems. Overreporting of incidents that have not happened will serve to undermine authorities' ability to provide timely and actionable advice to entities that are facing real incidents.

Amendment 60

Proposal for a directive
Article 20 – paragraph 3 – point b

Text proposed by the Commission	*Amendment*
(b) the incident has affected ***or has the potential to affect*** other natural or legal persons by causing considerable material or non-material losses.	(b) the incident has affected other natural or legal persons by causing considerable material or non-material losses.

Or. en

Justification

A requirement to report incidents that have the potential to affect others is unrealistic and could result in competent authorities being overwhelmed by receiving too many notifications, which could divert attention and limited security resources away from the essential tasks of actually examining and handling incidents and securing systems. Overreporting of incidents that have not happened will serve to undermine authorities' ability to provide timely and actionable advice to entities that are facing real incidents.

Amendment 61

Proposal for a directive
Article 20 – paragraph 4 – point a

Text proposed by the Commission	*Amendment*
(a) without undue delay and in any event within ***24*** hours after having become aware of the incident, an initial notification, which, where applicable, shall indicate whether the incident is presumably caused by unlawful or malicious action;	(a) without undue delay and in any event within ***72*** hours after having become aware of the incident, an initial notification, which, where applicable, shall indicate whether the incident is presumably caused by unlawful or malicious action;

Or. en

Justification

24 hours is unnecessarily short and injects additional complexity at a time when entities are faced with the difficult task of responding to a cyber incident (often on a Friday evening). It could increase the likelihood the entity will report inaccurate or inadequately contextualised information that will not be helpful. The full extent and impact of a cybersecurity incident may not be known or well understood within 24 hours of it being realised. The reporting time should therefore be aligned with the GDPR and other Union law.

Amendment 62

Proposal for a directive
Article 20 – paragraph 4 – point c – introductory part

Text proposed by the Commission	*Amendment*
(c) a ***final*** report not later than one month after the submission of the report under point (a), including at least the following:	(c) a ***comprehensive*** report not later than one month after the submission of the report under point (a), including at least the following:

Or. en

Justification

It is not always possible to have a final report within one month's time. Information about cybersecurity incidents often continues to emerge over time.

Amendment 63

Proposal for a directive
Article 20 – paragraph 6

Text proposed by the Commission	*Amendment*
6. Where appropriate, and in particular where the incident referred to in paragraph 1 concerns two or more Member States, the competent authority or the CSIRT shall inform the other affected Member States and ENISA of the incident. In so doing, the competent authorities, CSIRTs and single points of contact shall, in accordance with Union law or national	6. Where appropriate, and in particular where the incident referred to in paragraph 1 concerns two or more Member States, the competent authority or the CSIRT shall inform the other affected Member States and ENISA of the incident ***and provide relevant threat information***. In so doing, the competent authorities, CSIRTs and single points of contact shall,

legislation that complies with Union law, preserve the entity's security and commercial interests as well as the confidentiality of the information provided.	in accordance with Union law or national legislation that complies with Union law, preserve the entity's security and commercial interests as well as the confidentiality of the information provided.

Or. en

Amendment 64

Proposal for a directive
Article 20 – paragraph 8

Text proposed by the Commission	*Amendment*
8. At the request of the competent authority or the CSIRT, the single point of contact shall forward notifications received pursuant to ***paragraphs*** 1 ***and 2*** to the single points of contact of other affected Member States.	8. At the request of the competent authority or the CSIRT, the single point of contact shall forward notifications received pursuant to ***paragraph*** 1 to the single points of contact of other affected Member States.

Or. en

Amendment 65

Proposal for a directive
Article 20 – paragraph 9

Text proposed by the Commission	*Amendment*
9. The single point of contact shall submit to ENISA on a monthly basis a summary report including anonymised and aggregated data on incidents, significant cyber threats and near misses notified in accordance with ***paragraphs*** 1 ***and 2 and in accordance with*** Article 27. In order to contribute to the provision of comparable information, ENISA may issue technical guidance on the parameters of the information included in the summary report.	9. The single point of contact shall submit to ENISA on a monthly basis a summary report including anonymised and aggregated data on incidents, significant cyber threats and near misses notified in accordance with ***paragraph*** 1 ***of this Article and*** Article 27. In order to contribute to the provision of comparable information, ENISA may issue technical guidance on the parameters of the information included in the summary report.

Or. en

Amendment 66

Proposal for a directive
Article 20 – paragraph 10

Text proposed by the Commission	*Amendment*
10. Competent authorities shall provide to the competent authorities designated pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] information on incidents and cyber threats notified in accordance with ***paragraphs*** 1 ***and 2*** by essential entities identified as critical entities, or as entities equivalent to critical entities, pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive].	10. Competent authorities shall provide to the competent authorities designated pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] information on incidents and cyber threats notified in accordance with ***paragraph*** 1 ***of this Article*** by essential entities identified as critical entities, or as entities equivalent to critical entities, pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive].

Or. en

Amendment 67

Proposal for a directive
Article 20 – paragraph 11

Text proposed by the Commission	*Amendment*
11. The Commission, may adopt implementing acts further specifying the type of information, the format and the procedure of a notification submitted pursuant to ***paragraphs*** 1 ***and 2. The Commission may also adopt implementing acts to further specify the cases in which an incident shall be considered significant as referred to in paragraph 3***. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 37(2).	11. The Commission, may adopt implementing acts further specifying the type of information, the format and the procedure of a notification submitted pursuant to ***paragraph*** 1 ***of this Article***. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 37(2).

Or. en

Amendment 68

Proposal for a directive
Article 20 – paragraph 11 a (new)

Text proposed by the Commission	*Amendment*
	11a. The Commission is empowered to adopt delegated acts, in accordance with Article 36, to supplement this Regulation by specifying the type of information submitted pursuant to paragraph 1 of this Article and by further specifying the cases in which an incident shall be considered to be significant as referred to in paragraph 3 of this Article.

Or. en

Amendment 69

Proposal for a directive
Article 21 – paragraph 1

Text proposed by the Commission	*Amendment*
1. In order to demonstrate compliance with certain requirements of Article 18, Member States ***may require*** essential and important entities to certify certain ICT products, ICT services and ICT processes under ***specific*** European cybersecurity ***certification*** schemes adopted pursuant to Article 49 of Regulation (EU) 2019/881**.** ***The products, services and processes subject to*** certification ***may be developed by an essential or important entity or procured from third parties***.	1. In order to demonstrate compliance with certain requirements of Article 18, Member States ***shall encourage*** essential and important entities to certify certain ICT products, ICT services and ICT processes***, either developed by the essential or important entity or procured from third parties,*** under European cybersecurity schemes adopted pursuant to Article 49 of Regulation (EU) 2019/881 ***or under similar internationally recognised*** certification ***schemes***.

Or. en

Justification

The EU cybersecurity certification framework sets out a voluntary mechanism, enabling a period of experimentation and calibration, and is yet to deliver its first EU wide certification scheme. Making these mandatory might be premature. Brand new certification schemes must not be required until at least they have an extensive network of certification bodies and

widespread industry uptake and support. However, leveraging EU- and international certification schemes might be helpful to companies, as they give a clear and concise framework of what is asked of them.

Amendment 70

Proposal for a directive
Article 21 – paragraph 2

Text proposed by the Commission	*Amendment*
2. The Commission shall be empowered to adopt delegated acts specifying which categories of essential entities shall be required to obtain a certificate and under which specific European cybersecurity certification schemes pursuant to paragraph 1. The delegated acts shall be adopted in accordance with Article 36.	***deleted***

Or. en

Justification

Establishing mandatory certification does not lend itself to delegation by the Commission and should be done through the assessment as provided under the CSA.

Amendment 71

Proposal for a directive
Article 23 – title

Text proposed by the Commission	*Amendment*
Databases of domain names and registration data	***Database infrastructure*** of domain names and registration data

Or. en

Justification

Domain name registration data is stored across a variety of actors making use of different technologies, which not necessarily have to be 'dedicated' databases.

Amendment 72

Proposal for a directive
Article 23 – paragraph 1

Text proposed by the Commission	*Amendment*
1. For the purpose of contributing to the security, stability and resilience of the DNS, Member States shall ensure that TLD registries and ***the*** entities providing domain name registration services ***for the TLD shall*** collect and maintain accurate and complete domain name registration data in a ***dedicated*** database ***facility with due diligence subject to Union data protection law as regards data which are personal data***.	1. For the purpose of contributing to the security, stability and resilience of the DNS, Member States shall ensure that TLD registries and entities providing domain name registration services ***are required to*** collect and maintain accurate***, verified*** and complete domain name registration data in a database ***infrastructure operated for those purposes***.

Or. en

Justification

The reference to entities providing DNS services for the TLD is too narrow. Many other types of organisations provide domain name registration services, which have been defined in the definition of 'domain name registration services'. Reference to "verified" strengthens the language and provides clarity; entities should have internal processes to confirm that the data submitted is correct and contactable. Reference to data protection law is redundant due to Article 2 6a (new).

Amendment 73

Proposal for a directive
Article 23 – paragraph 2

Text proposed by the Commission	*Amendment*
2. Member States shall ensure that the ***databases*** of domain name registration data referred to in paragraph 1 ***contain*** relevant information to identify and contact the holders of the domain names and the points of contact administering the domain names under the TLDs.	2. Member States shall ensure that the ***database infrastructure*** of domain name registration data referred to in paragraph 1 ***contains*** relevant information***, which shall include at least the registrants' name, their physical and email address as well as their telephone number,*** to identify and contact the holders of the domain names and the points of contact administering the domain names under the TLDs.

Or. en

Justification

Relevant information should contain the registrants' (email) address. The ability to communicate in writing is essential for the enforcement of criminal and civil legal claims that require written records and substantiation of communication attempts for investigative purposes.

Amendment 74

Proposal for a directive
Article 23 – paragraph 3

Text proposed by the Commission	*Amendment*
3. Member States shall ensure that ***the*** TLD registries and ***the*** entities providing domain name registration services ***for the TLD*** have policies and procedures in place to ensure that the ***databases include*** accurate and complete information. Member States shall ensure that such policies and procedures are made publicly available.	3. Member States shall ensure that TLD registries and entities providing domain name registration services have policies and procedures in place to ensure that the ***database infrastructure includes*** accurate***, verified*** and complete information. Member States shall ensure that such policies and procedures are made publicly available.

Or. en

Amendment 75

Proposal for a directive
Article 23 – paragraph 4

Text proposed by the Commission	*Amendment*
4. Member States shall ensure that ***the*** TLD registries and ***the*** entities providing domain name registration services ***for the TLD publish***, without undue delay after the registration of a domain name, domain registration data ***which are not personal data***.	4. Member States shall ensure that TLD registries and entities providing domain name registration services ***make publicly available***, without undue delay after the registration of a domain name, domain registration data ***of legal persons as registrants***.

Or. en

Justification

Legal persons domain registration data are regarded as public and commonly used.

Amendment 76

Proposal for a directive
Article 23 – paragraph 5

Text proposed by the Commission	*Amendment*
5. Member States shall ensure that ***the*** TLD registries and ***the*** entities providing domain name registration services ***for the TLD*** provide access to specific domain name registration data upon ***lawful and*** duly justified requests of legitimate access seekers, in compliance with Union data protection law. Member States shall ensure that ***the*** TLD registries and ***the*** entities providing domain name registration services ***for the TLD*** reply without undue delay to all requests for access. Member States shall ensure that policies and procedures to disclose such data are made publicly available.	5. Member States shall ensure that TLD registries and entities providing domain name registration services ***are required to*** provide access to specific domain name registration data***, including personal data,*** upon duly justified requests of legitimate access seekers, in compliance with Union data protection law. Member States shall ensure that TLD registries and entities providing domain name registration services reply without undue delay ***and in any event within 72 hours*** to all requests for access. Member States shall ensure that policies and procedures to disclose such data are made publicly available.

Or. en

Justification

In cases of justified requests, domain registration data (including personal data) should be given to legitimate access seekers (for example for cybersecurity reasons, detection and prevention of crime, protection of minors and intellectual property, fraud prevention and protection against hate speech).

Amendment 77

Proposal for a directive
Article 26 – paragraph 1 – introductory part

Text proposed by the Commission	*Amendment*
1. ***Without prejudice to Regulation (EU) 2016/679,*** Member States shall	1. Member States shall ensure that essential and important entities may

ensure that essential and important entities may exchange relevant cybersecurity information among themselves including information relating to cyber threats, vulnerabilities, indicators of compromise, tactics, techniques and procedures, cybersecurity alerts and ***configuration tools***, where such information sharing:	exchange relevant cybersecurity information among themselves including information relating to cyber threats, ***near misses,*** vulnerabilities, indicators of compromise, ***adversarial*** tactics, techniques and procedures, ***meta and content data, indicators of compromise, modus operandi, attack attribution information which may include personal data related to the attacker,*** cybersecurity alerts and ***recommended security tool configurations***, where such information sharing:

Or. en

Justification

Reference to Regulation (EU) 2016/679 and the legal basis for this article can be found in the amendment on Article 2. Entities may exchange a wide range of cybersecurity related data.

Amendment 78

Proposal for a directive
Article 26 – paragraph 1 – point b

Text proposed by the Commission	*Amendment*
(b) enhances the level of cybersecurity, in particular through raising awareness in relation to cyber threats, limiting or impeding such threats 'ability to spread, supporting a range of defensive capabilities, vulnerability remediation and disclosure, threat detection techniques, mitigation strategies, ***or*** response and recovery stages.	(b) enhances the level of cybersecurity, in particular through raising awareness in relation to cyber threats, limiting or impeding such threats 'ability to spread, supporting a range of defensive capabilities, vulnerability remediation and disclosure, threat detection ***and prevention*** techniques, mitigation strategies, response and recovery stages ***or promoting collaborative threat research between public and private entities***.

Or. en

Amendment 79

Proposal for a directive
Article 26 – paragraph 2

Text proposed by the Commission	*Amendment*
2. Member States shall ***ensure that*** the exchange of information ***takes place within*** trusted communities of essential and important entities. Such exchange shall be implemented through information sharing arrangements in respect of the potentially sensitive nature of the information shared ***and in compliance with the rules of Union law referred to in paragraph 1***.	2. Member States shall ***support*** the exchange of information ***by encouraging and promoting the creation of*** trusted communities of essential and important entities ***and their service providers***. Such exchange shall be implemented through information sharing arrangements in respect of the potentially sensitive nature of the information shared.

Or. en

Justification

Information sharing is a voluntary and based on trust. It should therefore be facilitated, but not regulated by the Member States. The role of public bodies should be clearly one of contributor to information sharing and not of public policy enforcer, otherwise there is risk that the presence of a public body will impact the quality of information shared. Service providers should include cybersecurity companies and cybersecurity researchers.

Amendment 80

Proposal for a directive
Article 26 – paragraph 3

Text proposed by the Commission	*Amendment*
3. Member States shall ***set out rules specifying*** the procedure, operational elements (including the use of dedicated ICT platforms), content and conditions of the information sharing arrangements referred to in paragraph 2. ***Such rules*** shall ***also*** lay down the details of the involvement of public authorities in such arrangements, as well as operational elements, including the use of dedicated IT platforms. Member States shall offer support to the application of such arrangements in accordance with their	3. Member States shall ***establish best practices on*** the procedure, operational elements (including the use of dedicated ICT platforms ***and automation tools***), content and conditions of the information sharing arrangements referred to in paragraph 2. ***Member States*** shall ***set out rules that*** lay down the details of the involvement of public authorities in such arrangements, as well as operational elements, including the use of dedicated IT platforms. Member States shall offer support to the application of such

policies referred to in Article 5(2) (g).	arrangements in accordance with their policies referred to in Article 5(2) (g).

Or. en

Justification

These information sharing arrangements might best be organized bottom-up, instead of top-down. Strict rules might stifle the flexibility that each sharing arrangement or group of companies might need.

Amendment 81

Proposal for a directive
Article 26 a (new)

Text proposed by the Commission	*Amendment*
	Article 26a
	Voluntary notification of relevant information by essential and important entities
	Member States shall ensure that essential and important entities are able to submit notifications, on a voluntary basis, of significant cyber threats and near misses to the competent authorities or the CSIRT. Where applicable, those entities may notify the recipients of their services that are at risk of being affected by a significant cyber threat of any measures or remedies that those recipients can take in response to that threat. Where appropriate, those entities can also notify those recipients of the threat itself. The notification shall not make the notifying entity subject to increased liability.

Or. en

Justification

The proposed amendments take out the obligation to notify potential incidents. However, entities should be able to notify competent authorities or the CSIRT and the recipients of their services, if they deem it to be necessary/helpful/contributing.

Amendment 82

Proposal for a directive
Article 27 – title

Text proposed by the Commission	*Amendment*
Voluntary notification of relevant information	Voluntary notification of relevant information ***by entities falling outside the scope***

Or. en

Amendment 83

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

Text proposed by the Commission	*Amendment*
(b) regular audits;	(b) regular audits***, that take place no more frequently than once a year, unless justified on the ground of a significant incident or non-compliance by the essential entity***;

Or. en

Justification

Annual cybersecurity audits should be sufficient.

Amendment 84

Proposal for a directive
Article 29 – paragraph 4 – point j

Text proposed by the Commission	*Amendment*
(j) impose or request the imposition by the relevant bodies or courts according to national laws of an administrative fine pursuant to Article 31 in addition to***, or instead of,*** the measures referred to in	(j) impose or request the imposition by the relevant bodies or courts according to national laws of an administrative fine pursuant to Article 31 in addition to the measures referred to in points (a) to (i) of

points (a) to (i) of this paragraph, depending on the circumstances of each individual case.	this paragraph, depending on the circumstances of each individual case.

Or. en

Justification

Fines should be used as a measure to remedy persistent non-compliance, and should be used after measures in points (a) to (i) proved ineffective.

Amendment 85

Proposal for a directive
Article 29 – paragraph 5 – point b

Text proposed by the Commission	*Amendment*
(b) impose or request the imposition by the relevant bodies or courts according to national laws of a temporary ban against any person discharging managerial responsibilities at chief executive officer or legal representative level in that essential entity, and of any other natural person held responsible for the breach, from exercising managerial functions in that entity.	***deleted***

Or. en

Justification

Proportionality

Amendment 86

Proposal for a directive
Article 29 – paragraph 7 – point c

Text proposed by the Commission	*Amendment*
(c) the ***actual*** damage caused or losses incurred ***or potential damage or losses that could have been triggered, insofar as they can be determined. Where evaluating this***	(c) the damage caused or losses incurred***, including*** financial or economic losses, effects on other services ***and the***

aspect, account shall be taken, amongst others, of actual or potential financial or economic losses, effects on other services**,** number of users affected ***or potentially affected***;	number of users affected;

Or. en

Amendment 87

Proposal for a directive
Article 29 – paragraph 9 a (new)

Text proposed by the Commission	*Amendment*
	9a. Member States shall ensure that their competent authorities cooperate with the relevant competent authorities of the Member State concerned designated pursuant to Regulation (EU) XXXX/XXXX [DORA].

Or. en

Justification

Although the DORA proposal foresees a clear hierarchy between DORA and the NIS for financial entities, it does not do the same for critical ICT third-party service providers. This could create redundancy between the two frameworks. A structural, workable solution must be found in order to avoid that two sets of authorities conduct overlapping supervision over the same services. Cooperation between the Lead Overseer under DORA and the NIS2 national competent authorities should be formalised.

Amendment 88

Proposal for a directive
Article 30 – paragraph 1

Text proposed by the Commission	*Amendment*
1. When provided with evidence or indication that an important entity is not in compliance with the obligations laid down in this Directive, and in particular in Articles 18 and 20, Member States shall	1. When provided with evidence or indication that an important entity is not in compliance with the obligations laid down in this Directive, and in particular in Articles 18 and 20, Member States shall

ensure that the competent authorities take action, where necessary, through ex post supervisory measures.	ensure that the competent authorities take action, where necessary, through ex post supervisory measures. ***Member States shall ensure that these measures are effective, proportionate and dissuasive, taking into account the circumstances of each individual case.***

Or. en

Amendment 89

Proposal for a directive
Article 30 – paragraph 4 – point i

Text proposed by the Commission	*Amendment*
(i) impose or request the imposition by the relevant bodies or courts according to national laws of an administrative fine pursuant to Article 31 in addition to***, or instead of,*** the measures referred to in points (a) to (h) of this paragraph, depending on the circumstances of each individual case.	(i) impose or request the imposition by the relevant bodies or courts according to national laws of an administrative fine pursuant to Article 31 in addition to the measures referred to in points (a) to (h) of this paragraph, depending on the circumstances of each individual case.

Or. en

Justification

Fines should be used as a measure to remedy persistent non-compliance, and should be used after measures in points (a) to (i) proved ineffective.

Amendment 90

Proposal for a directive
Article 31 – paragraph 2

Text proposed by the Commission	*Amendment*
2. Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to***, or instead of,*** measures referred to in points (a) to (i) of Article 29(4), Article	2. Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to measures referred to in points (a) to (i) of Article 29(4), Article 29(5) and points (a)

29(5) and points (a) to (h) of Article 30(4). to (h) of Article 30(4).

Or. en

Justification

Fines should be used as a measure to remedy persistent non-compliance.

Amendment 91

Proposal for a directive
Annex II – table – row 6 a (new)

Text proposed by the Commission

Amendment

6a. Education and research		***— Higher education institutions and research institutions***

Or. en

EXPLANATORY STATEMENT

The Rapporteur wants Europe to become the best place to live in and to carry out business in.

The Rapporteur therefore welcomes the Directive on measures for a high common level of cybersecurity across the Union (NIS2), which replaces the original NIS Directive (NIS1). The proposal reflects the changed cybersecurity threat landscape and introduces a minimum harmonization of measures across the EU.

Nowadays, European police forces increasingly struggle to cope with the steep rise of cybercrime incidents. These can include high-tech crime, cyber enabled crime and CEO-fraud, but the Rapporteur wishes to explicitly highlight the aggressive rise in ransomware gangs hacking and blackmailing European targets, irrespective of their size or turnover. In turn, adversarial nation state actors are focussing on intellectual property theft on an industrial scale, which requires a corresponding answer.

Yet, according to ENISA, the general spending on cybersecurity is 41 % lower by organisations in the EU than by their US counterparts. Moreover, information sharing between countries and within countries has been seriously hampered due to GDPR-liability fears. This is evident in both public and private entities who are fearful of sharing data. The NIS2 must therefore be clear that information sharing is essential for the requirements on cybersecurity to be met.

A common level of cybersecurity in the EU is crucial for the functioning of the internal market. Well-defined legislation is necessary so that enterprises who operate in different Member States fall under the same set of rules. NIS2 wants to remove uncertainty and the current lack of clarity.

In an age where cybercrime, espionage or sabotage operations can have cascading effects, the NIS2 justly widens the **scope** significantly. The proposal includes sectors that previously were not considered essential or important, but are definitely regarded as such by ransomware gangs or certain nation states. Based on the services entities deliver for societies, these are divided into the following two legal categories: ‘essential’ and ‘important’ entities. The Rapporteur shares the ambition of the proposal by the Commission, and believes research and academic institutions should be included as a new sector. These institutions are heavily targeted, and their intellectual property deserves protection under the NIS2.

The administrative burden and **red tape on enterprises** must be a constant concern to all legislators. The Rapporteur supports the exclusion of micro- and small enterprises. He, furthermore, believes that the NIS2 should not just focus on compliance and penal measures, but also on positive incentives, such as providing guidance and assistance to SMEs, who have specific needs and interests, or on freely offered services to check email-server and website configuration. Such proposals are also meant to illustrate, in this respect, that governments need to be service-orientated.

Incident reporting is critical to cybersecurity: it can prevent others from becoming victims of a cyberattack. The Rapporteur wishes to mention that in his former capacity in the cybersecurity field, he often found it impossible to report an incident within 24 hours. Usually at this early stage an incident is still unclear until later on. To the Rapporteur, the proposed timeframe of 24 hours seems unreasonable, also due to the fact that the experts efforts are invested in mitigating the problem; reporting at this stage is of secondary interest. The cyber incident and its implications are rarely understood well within 24 hours, and notifications

within 24 hours could lead to incorrect reporting, over-reporting and further confusion. Moreover, these incidents often happen over the weekend. Therefore, the Rapporteur proposes to align this Directive with other Union law, such as the GDPR, thus increasing the timeline to within 72 hours.

The Rapporteur does not find it desirable to make the **reporting of potential incidents** mandatory. Voluntary sharing of potential incidents or near misses should be encouraged, but medium and large entities can potentially have tens or even hundreds of significant cyber threats in a single day. Reporting these potential incidents would be burdensome and would inhibit the effectiveness of the response. It could also harm the efficacy of the authorities that have to deal with these notifications, undermining the confidence of the reporting system and their ability to act upon actual incidents.

Reporting potential cyber threats to CSIRTs or competent authorities should also not be mandatory. Compliance and liability will discourage the activities of threat hunters; an essential part of the cyber security ecosystem. Furthermore, there are (serious) occasions where it would be better to report a threat to the intelligence community, when it is in their area of competence, instead of to the NIS authorities.

Cybersecurity measures should be appropriate to the size of the entity and the cybersecurity risks it faces. **Supervision and enforcement** should therefore be proportionate. The fines and penal measures are essential if the NIS2 legislation is to be effective, but the Rapporteur believes legislators should emphasize that there is an escalation-ladder, and only after demonstrable negligence of repeated warnings, should senior management be prepared to feel the force of the law. **Preventing double oversight** trough sector-specific legislation is also important for entities who fall in the scope of both NIS2 and a sector-specific one, such as DORA.

The Rapporteur encourages every member state to formulate a **national cybersecurity strategy on active cyber defence**. In Europe, we have become good at coordinating after an incident has occurred, but the increase of knowledge (public and private) about cyberattacks before they occur, also entails a responsibility. Merely passively sharing that knowledge is not sufficient; citizens and entities expect an active posture from their governments on cybersecurity protection. Member States must initiate capabilities to thwart attacks and actively prevent them from occurring.

The core of the internet needs attention too. DNS services need to offer secure and privacy minded services to customers. This is not commonly accepted yet. The Rapporteur is concerned that citizens who have their own DNS service on a laptop or small server at home, fall in scope in the proposal of the Commission. The Rapporteur wishes that these persons, often tech-savvy individuals, to be excluded from this Directive. Another problem is that operators of root name servers are included in the scope of the NIS2. Since the Internet grew in the 1970s, 1980s and further, these services are operated by good expert-volunteers. As this service is not monetised, and as it can be argued that governments should not regulate it, the Rapporteur believes that root servers should be **excluded from the scope**.

The Rapporteur finds it of great importance to strengthen the overall security of electronic communication networks and services and improve the integrity of the internet. This means that throughout Europe inter-operable trust-techniques should be used. European DNS resolvers with extra focus on privacy and security are greatly encouraged, as well as the physical protection of internet backbones and submarine communication cables. This Directive should therefore be seen in light of the full package of the cybersecurity strategy as

was launched by the Commission: we need a more secure core of the internet.

The NIS2 further provides the legal basis for **coordinated security risk assessments** by the Cooperation Group. The 5G toolbox has served as an excellent example. The Rapporteur believes that these risk assessments could widely improve the security and strategic sovereignty of the Union and believes that these risk assessments should be done on a wide-range of ICT services, systems or products. Cargo-scanners at airports and ports is an explicit example he wishes to mention in this regard.

Unintendedly, essential information sharing has been severely hampered and should be improved. An example: in the past years, police forces discovered and decrypted servers from ransomware gangs, containing sometimes millions of victims, in the EU and outside the EU. The police's job is to work on new cases, so they enable CSIRTs to reach out to targets and mitigate the cyber threats with the uncovered information on those servers. Unfortunately, due to unjustified perceived legal hurdles hardly any victim has been notified or assisted. Therefore, it is essential that the NIS2 creates a clear legal basis to mitigate such threats and to share information not only inside the EU, but also with partners outside the EU.

With the enhancement of the scope, CSIRTs must prepare to offer **scalable and automated solutions** for the swift and secure distribution of coordinated vulnerability disclosure, incident reporting and threat intelligence. The automation of information sharing is not just a derivative of this Directive: it is at the core of it. Providing the **legal basis for CSIRTs and companies to share data**, with their customers, peers, and authorities, both in and outside the EU, is a prerequisite of all good intentions of the NIS2.

Using **standards and certification schemes** is another positive feature from the Commission's proposal. Certification should be possible through specific European- and internationally recognized schemes, preferable over national schemes. Harmonization should be the aim; rules in one Member State should be similar to rules in other Member States.

The NIS2 proposal requires ENISA to develop and maintain a European vulnerability registry. The Rapporteur believes that a **European vulnerability database** should be preferred over a registry. There is little reason to double what is already in place and used by the cybersecurity community as a common standard in all parts of the world. Doubling will sow discord and confusion within the expert community. A European database, not a registry, should leverage the CVE registry; the list of records of international publicly known cybersecurity vulnerabilities used throughout the world. The Rapporteur believes that ENISA should have a prominent new role within the CVE registry, which is now mainly US based. Duplication of efforts should furthermore be prevented; the desirable outcome should be a database with unique challenges for European organisations. Finally yet importantly, the Rapporteur stresses it is of utmost importance for ENISA to have the infrastructure and procedures in place to deal with classified information. Cybersecurity should be handled from the unclassified level up to the (top) secret level.

WHOIS data, the authoritative record of domain ownership, is the only viable means to obtain the information necessary to identify criminal actors, track threat actors, prevent harms and protect the online ecosystem. The cybersecurity community relies on it, and it enables threat researchers to hunt adversaries, so that citizens and entities can protect themselves against upcoming threats. It is the only reliable accountability mechanism in an otherwise anonymous internet. However, over the past three years, following the entry into force of the GDPR, WHOIS data is regarded by some as a liability issue. The standing practise of WHOIS data has been halted, unfortunately and unjustified. The Rapporteur therefore reiterates in his

report the lawfulness of processing data for cybersecurity reasons under the GDPR, in the explicit legislative wish for WHOIS data to be shared again.

Overall, the Rapporteur believes that the NIS2 is the necessary step to take to harmonise our internal market and improve cybersecurity throughout the EU.