



2018/0328(COD)

7.12.2018

*****I**

DRAFT REPORT

on the proposal for a regulation of the European Parliament and of the Council establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres (COM(2018)0630 – C8-0404/2018 – 2018/0328(COD))

Committee on Industry, Research and Energy

Rapporteur: Julia Reda

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.....	5
EXPLANATORY STATEMENT.....	54

DRAFT EUROPEAN PARLIAMENT LEGISLATIVE RESOLUTION

on the proposal for a regulation of the European Parliament and of the Council establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres (COM(2018)0630 – C8-0404/2018 – 2018/0328(COD))

(Ordinary legislative procedure: first reading)

The European Parliament,

- having regard to the Commission proposal to Parliament and the Council (COM(2018)0630),
 - having regard to Article 294(2) and Articles 173(3) and 188(1) of the Treaty on the Functioning of the European Union, pursuant to which the Commission submitted the proposal to Parliament (C8-0404/2018),
 - having regard to Article 294(3) of the Treaty on the Functioning of the European Union,
 - having regard to the opinion of the European Economic and Social Committee of ...¹,
 - having regard to Rule 59 of its Rules of Procedure,
 - having regard to the report of the Committee on Industry, Research and Energy and the opinion of the Committee on the Internal Market and Consumer Protection (A8-0000/2019),
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.

Amendment 1

Proposal for a regulation

Recital 1

Text proposed by the Commission

(1) Our daily lives and economies become increasingly dependent on digital technologies, citizens become more and more exposed to serious cyber incidents.

Amendment

(1) Our daily lives and economies become increasingly dependent on digital technologies, citizens become more and more exposed to serious cyber incidents.

¹Not yet published in the Official Journal

Future security depends, among others, on enhancing technological and industrial ability to protect the Union against cyber threats, as both *civilian* infrastructure and *military* capacities rely on secure digital systems.

Future security depends, among others, on enhancing technological and industrial ability to protect the Union against cyber threats as both infrastructure and *security* capacities rely on secure digital systems.

Or. en

Amendment 2

Proposal for a regulation Recital 3 a (new)

Text proposed by the Commission

Amendment

(3 a) Article 41(2) of the Treaty on European Union states that the Union budget is not to be used for expenditure arising from operations having military or defence implications. Therefore the Cybersecurity Industrial, Technology, and Research Centre and its actions should be provided purely for civilian purposes.

Or. en

Amendment 3

Proposal for a regulation Recital 4 a (new)

Text proposed by the Commission

Amendment

(4a) The Competence Centre and its actions should take into account the implementation of Regulation (EU) 2019/XXX [recast of Regulation (EC) No 428/2009 as proposed by COM(2016)616].^{1a}

^{1a} Regulation (EU) 2019/... of the European Parliament and of the Council of ... setting up a Union regime for the

control of exports, transfer, brokering, technical assistance and transit of dual-use items (OJ L ..., ..., p. ...).

Or. en

Amendment 4

Proposal for a regulation

Recital 5

Text proposed by the Commission

(5) Substantial disruption of network and information systems can affect individual Member States and the Union as a whole. The security of network and information systems is therefore essential ***for the smooth functioning of the internal market***. At the moment, the Union depends on non-European cybersecurity providers. However, it is in the Union's strategic interest to ensure that it retains and develops essential cybersecurity technological capacities ***to secure its Digital Single Market***, and in particular to protect critical networks and information systems and to provide key cybersecurity services.

Amendment

(5) Substantial disruption of network and information systems can affect individual Member States and the Union as a whole. The security of network and information systems is therefore essential. At the moment, the Union depends on non-European cybersecurity providers. However, it is in the Union's strategic interest to ensure that it retains and develops essential cybersecurity technological capacities ***and capabilities*** in particular to protect critical networks and information systems and to provide key cybersecurity services.

Or. en

Amendment 5

Proposal for a regulation

Recital 5 a (new)

Text proposed by the Commission

Amendment

(5a) The resilience of ICT infrastructure like the Internet is critical to society, industry and research throughout the Union. That infrastructure relies heavily on components developed as Free and Open

Source Software. Society, industry, businesses with diverse business models, as well as research and development build on them to create products and provide services.

Or. en

Amendment 6

Proposal for a regulation Recital 6 a (new)

Text proposed by the Commission

Amendment

(6a) Cybersecurity experts often start their education in non-formal contexts, for example Free and Open Source Software projects and civic tech projects. Civic tech projects make use of open standards, Open Data, and Free and Open Source Software to develop products and services in the interest of society and the public good. They can be of non-commercial or pre-commercial nature and can as such be a precursor for start-ups, or academic and research projects.

Or. en

Amendment 7

Proposal for a regulation Recital 8 a (new)

Text proposed by the Commission

Amendment

(8a) The Competence Centre should contribute to the security of ICT technology that is challenged by a constant evolution of threats and by the advancement of the technology itself. That is why security cannot simply be established, but should be understood as a process, incorporating the principle of

“security by design” in the development of ICT technology. “Security by design” as established in Commission Joint Communication of 13 September 2017 entitled “Resilience, Deterrence and Defence: Building strong cybersecurity for the EU” includes state-of-the-art methods to increase security, at all stages of the lifecycle of a product or service, starting with secure design and development methods, reducing the attack surface, and incorporating adequate security testing and security audits. For the duration of operation and maintenance, producers or providers need to make available updates remedying new vulnerabilities or threats without delay, for the estimated lifetime of a product and beyond. This can also be achieved by enabling third parties to create and provide such updates. The provision of updates is especially necessary in the case of commonly used infrastructures, products and processes.

Or. en

Amendment 8

Proposal for a regulation Recital 8 b (new)

Text proposed by the Commission

Amendment

(8b) “Security by design” as a principle should also influence formal as well as non-formal standardisation processes, where a common practice in non-formal standardisation is the creation of reference implementations, published under free and open licences. The secure design of, in particular, reference implementations is crucial for the overall reliability and resilience of commonly used network and information system infrastructure like the internet.

Amendment 9**Proposal for a regulation****Recital 12***Text proposed by the Commission*

(12) National Coordination Centres should be selected by Member States. In addition to the necessary administrative capacity, Centres should either possess or have direct access to cybersecurity technological expertise in cybersecurity, notably in domains such as cryptography, ICT security services, intrusion detection, system security, network security, software and application security, or human and societal aspects of security and privacy. They should also have the capacity to effectively engage and coordinate with the industry, the public sector, including authorities designated pursuant to the Directive (EU) 2016/1148 of the European Parliament and of the Council²³, and the research community.

²³ Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194, 19.7.2016, p. 1).

Amendment

(12) National Coordination Centres should be selected by Member States. In addition to the necessary administrative capacity, Centres should either possess or have direct access to cybersecurity technological expertise in cybersecurity, notably in domains such as cryptography, ICT security services, intrusion detection, system security, network security, software and application security, or human, *ethical* and societal aspects of security and privacy. They should also have the capacity to effectively engage and coordinate with the industry, the public sector, including authorities designated pursuant to the Directive (EU) 2016/1148 of the European Parliament and of the Council²³, and the research community.

²³ Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194, 19.7.2016, p. 1).

Amendment 10**Proposal for a regulation****Recital 14***Text proposed by the Commission*

(14) Emerging technologies such as

Amendment

(14) Emerging technologies such as

artificial intelligence, Internet of Things, high-performance computing (HPC) and quantum computing, **blockchain and** concepts such as secure digital identities create at the same time new challenges for cybersecurity as well as offer **solutions**. Assessing and validating the robustness of existing or future ICT systems will require testing security **solutions** against attacks run on HPC and quantum machines. The Competence Centre, the Network and the Cybersecurity Competence Community should help advance and disseminate the latest cybersecurity **solutions**. At the same time the Competence Centre and the Network should be at the service of developers and operators in critical sectors such as transport, energy, health, financial, government, telecom, manufacturing, **defence**, and space to help them solve their cybersecurity challenges.

artificial intelligence, Internet of Things, high-performance computing (HPC) and quantum computing, **as well as** concepts such as secure digital identities create at the same time new challenges for cybersecurity as well as offer **products and processes**. Assessing and validating the robustness of existing or future ICT systems will require testing security **products and processes** against attacks run on HPC and quantum machines. The Competence Centre, the Network and the Cybersecurity Competence Community should help advance and disseminate the latest cybersecurity **products and processes**. At the same time the Competence Centre and the Network should be at the service of developers and operators in critical sectors such as transport, energy, health, financial, government, telecom, manufacturing, and space to help them solve their cybersecurity challenges.

Or. en

Justification

"solutions" should be replaced with "products and processes" across the text.

Amendment 11

Proposal for a regulation

Recital 17

Text proposed by the Commission

(17) In order to respond to the needs of both demand and supply side industries, the Competence Centre's task to provide cybersecurity knowledge and technical assistance to industries should refer to both ICT products and services and all other industrial and technological products and **solutions** in which cybersecurity is to be embedded.

Amendment

(17) In order to respond to the needs of both demand and supply side industries, the Competence Centre's task to provide cybersecurity knowledge and technical assistance to industries should refer to both ICT products and services and all other industrial and technological products and **processes** in which cybersecurity is to be embedded.

(This amendment, replacing “solutions” with “products and processes”, applies throughout the text. Adopting it will necessitate corresponding changes throughout.)

Or. en

Amendment 12

Proposal for a regulation

Recital 18

Text proposed by the Commission

(18) *Whereas the Competence Centre and the Network should strive to achieve synergies between the cybersecurity civilian and defence spheres*, projects financed by the Horizon Europe Programme will be implemented in line with Regulation XXX [Horizon Europe Regulation], which provides that research and innovation activities carried out under Horizon Europe shall have a focus on civil applications.

Amendment

(18) Projects financed by the Horizon Europe Programme will be implemented in line with Regulation XXX [Horizon Europe Regulation], which provides that research and innovation activities carried out under Horizon Europe shall have a focus on civil applications.

Or. en

Amendment 13

Proposal for a regulation

Recital 18 a (new)

Text proposed by the Commission

(18 a) Where an applicant for funding under Horizon Europe excludes non-civil applications in development, research, education or other activities, this should not lead to a disadvantage.

Amendment

Or. en

Amendment 14

Proposal for a regulation Recital 22

Text proposed by the Commission

(22) Where they receive a financial contribution from the general budget of the Union, the National Coordination Centres and the entities which are part of the Cybersecurity Competence Community should publicise the fact that the respective activities are undertaken in the context of the present initiative.

Amendment

(22) Where they receive a financial contribution from the general budget of the Union, the National Coordination Centres and the entities which are part of the Cybersecurity Competence Community should publicise the fact that the respective activities are undertaken in the context of the present initiative **and are of civilian nature**.

Or. en

Amendment 15

Proposal for a regulation Recital 29

Text proposed by the Commission

(29) The Competence Centre should have in place rules regarding the prevention **and the management of conflict** of interest. The Competence Centre should also apply the relevant Union provisions concerning public access to documents as set out in Regulation (EC) No 1049/2001 of the European Parliament and of the Council²⁴. Processing of personal data by the Competence Centre will be subject to Regulation (EU) No XXX/2018 of the European Parliament and of the Council. The Competence Centre should comply with the provisions applicable to the Union institutions, and with national legislation regarding the handling of information, in particular sensitive non classified information and EU classified information.

Amendment

(29) The Competence Centre should have in place rules regarding the prevention, **identification and resolution of conflicts** of interest **in respect of its members, bodies and staff, the Governing Board, as well as the Scientific and Industrial Advisory Board, and the Community. Member States should ensure the prevention, identification, and resolution of conflicts of interest in respect of the National Coordination Centres**. The Competence Centre should also apply the relevant Union provisions concerning public access to documents as set out in Regulation (EC) No 1049/2001 of the European Parliament and of the Council²⁴. Processing of personal data by the Competence Centre will be subject to Regulation (EU) No XXX/2018 of the European Parliament and of the Council. The Competence Centre should comply

with the provisions applicable to the Union institutions, and with national legislation regarding the handling of information, in particular sensitive non classified information and EU classified information.

²⁴ Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents (OJ L 145, 31.5.2001, p. 43).

²⁴ Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents (OJ L 145, 31.5.2001, p. 43).

Or. en

Amendment 16

Proposal for a regulation

Recital 31

Text proposed by the Commission

(31) The Competence Centre should operate in an open and transparent way providing ***all relevant*** information in a timely manner as well as promoting its activities, including information and dissemination activities to the wider public. The rules of procedure of the bodies of the Competence Centre should be made publicly available.

Amendment

(31) The Competence Centre should operate in an open and transparent way ***comprehensively*** providing information in a timely manner as well as promoting its activities, including information and dissemination activities to the wider public. ***It should provide the public and any interested parties with a list of the Cybersecurity Competence Community members and should make public the declarations of interest made by them in accordance with Article 42.*** The rules of procedure of the bodies of the Competence Centre should be made publicly available.

Or. en

Amendment 17

Proposal for a regulation

Recital 31 a (new)

Text proposed by the Commission

Amendment

(31a) The European Cybersecurity Community can benefit from representing the diversity of society at large, and should achieve a balanced representation of genders, ethnic diversity, and disabled persons.

Or. en

Amendment 18

Proposal for a regulation

Article 1 – paragraph 2 a (new)

Text proposed by the Commission

Amendment

2 a. The Competence Centre shall contribute to the overall resilience in the Union towards cybersecurity threats. This can be achieved by raising the awareness for cybersecurity threats, by developing competences, capacities, capabilities throughout the Union, thoroughly taking into account the interplay of hardware and software infrastructure, networks, products and processes, and the societal and ethical implications and concerns.

Or. en

Amendment 19

Proposal for a regulation

Article 1 – paragraph 3

Text proposed by the Commission

Amendment

3. The seat of the Competence Centre shall be located in [Brussels, Belgium.] ***deleted***

Or. en

Justification

The amendment is of technical nature, sentence is moved into Article 44.

Amendment 20

**Proposal for a regulation
Article 1 – paragraph 4**

Text proposed by the Commission

Amendment

4. The Competence Centre shall have legal personality. In each Member State, it shall enjoy the most extensive legal capacity accorded to legal persons under the laws of that Member State. It may, in particular, acquire or dispose of movable and immovable property and may be a party to legal proceedings. **deleted**

Or. en

Justification

This amendment is of technical nature. The paragraph is moved into Article 38a (new).

Amendment 21

**Proposal for a regulation
Article 2 – paragraph 1 – point 1**

Text proposed by the Commission

Amendment

(1) 'cybersecurity' means the protection of network and information systems, their users, and other persons against **cyber** threats;

(1) 'cybersecurity' means **the process of** the protection of network and information systems, their users, and other persons against threats **from network and information systems and their users**;

Or. en

Amendment 22

**Proposal for a regulation
Article 2 – paragraph 1 – point 2**

Text proposed by the Commission

(2) '**cybersecurity** products and **solutions**' means ICT products, services or **process** with the specific purpose of protecting network and information systems, their users and **affected** persons from **cyber** threats;

Amendment

(2) 'products and **processes**' means **commercial and non-commercial** ICT products, services or **processes** with the specific purpose of protecting network and information systems, their users and **other** persons from **cybersecurity** threats, **including Free and Open Source Software products, services or processes**;

Or. en

Amendment 23

Proposal for a regulation

Article 2 – paragraph 1 – point 3

Text proposed by the Commission

(3) 'public authority' means any government or other public administration, including public advisory bodies, at national, regional or local level or any natural or legal person performing public administrative functions under national law, including specific duties;

Amendment

(3) 'public authority' means any government or other public administration, including public advisory bodies, at national, regional or local level or any natural or legal person performing public administrative functions under **Union and national** law, including specific duties;

Or. en

Amendment 24

Proposal for a regulation

Article 2 – paragraph 1 – point 4 a (new)

Text proposed by the Commission

Amendment

(4a) 'industry' means the industry providing products, processes, and services addressing cybersecurity demands and requirements, including SMEs, microenterprises, and individual experts.

Amendment 25

Proposal for a regulation

Article 2 – paragraph 1 – point 4 b (new)

Text proposed by the Commission

Amendment

(4b) ‘stakeholders’ mean the industry, public entities and other entities dealing with operational and technical matters in the area of cybersecurity; civil society, in particular consumer associations, and the Free and Open Source Software community; the academic and research community;

Or. en

Amendment 26

Proposal for a regulation

Article 2 – paragraph 1 – point 4 c (new)

Text proposed by the Commission

Amendment

(4c) ‘civic tech projects’ means non-commercial and pre-commercial projects making use of open standards, Open Data, and Free and Open Source Software, in the interest of society and the public good, in particular where they do not have access to sufficient, steady financial support;

Or. en

Amendment 27

Proposal for a regulation

Article 3 – paragraph 1 – point a

Text proposed by the Commission

Amendment

(a) ***retain and*** develop the cybersecurity technological ***and*** industrial capacities ***necessary to secure its Digital Single Market;***

(a) develop the ***civilian*** cybersecurity technological, industrial, ***societal, academic and research*** capacities ***and capabilities;***

Or. en

Amendment 28

Proposal for a regulation

Article 3 – paragraph 1 – point a a (new)

Text proposed by the Commission

Amendment

(a a) increase the resilience and reliability of the civilian infrastructure of network and information systems, the Internet and commonly used hardware and software in the Union;

Or. en

Amendment 29

Proposal for a regulation

Article 3 – paragraph 1 – point b

Text proposed by the Commission

Amendment

(b) increase the competitiveness of the Union's cybersecurity industry and turn cybersecurity into competitive advantage of other Union industries.

(b) increase the competitiveness of the Union's ***civilian*** cybersecurity industry and turn cybersecurity into ***a*** competitive advantage of other Union industries;

Or. en

Amendment 30

Proposal for a regulation

Article 3 – paragraph 1 – point b a (new)

Text proposed by the Commission

Amendment

(b a) raise the awareness for cybersecurity threats, and related societal and ethical implications and concerns in the Union.

Or. en

Amendment 31

Proposal for a regulation

Article 4 – paragraph 1 – point 1

Text proposed by the Commission

Amendment

1. facilitate **and help coordinate the work of** the National Coordination Centres Network ('the Network') referred to in Article 6 and the Cybersecurity Competence Community referred to in Article 8;

1. **create, manage, and** facilitate the National Coordination Centres Network ('the Network') referred to in Article 6 and the Cybersecurity Competence Community (**'the Community'**) referred to in Article 8;

(The term "Cybersecurity Competence Community" can be shortened to "the Community" throughout the text.)

Or. en

Amendment 32

Proposal for a regulation

Article 4 – paragraph 1 – point 3 – introductory part

Text proposed by the Commission

Amendment

3. enhance cybersecurity capabilities, knowledge and infrastructures at the service of industries, the public sector and research communities, by carrying out the following tasks:

3. enhance cybersecurity **resilience**, capabilities, knowledge and infrastructures at the service of **society**, industries, the public sector and research communities, by carrying out the following tasks, **having regard to the state-of-the-art cybersecurity industrial and research infrastructures and related services**:

Amendment 33

Proposal for a regulation

Article 4 – paragraph 1 – point 3 – point a

Text proposed by the Commission

(a) ***having regard to the state-of-the-art cybersecurity industrial and research infrastructures and related services***, acquiring, upgrading, operating and making available ***such infrastructures*** and related services to a wide range of users ***across the Union from industry including SMEs, the public sector and the research and scientific community***;

Amendment

(a) acquiring, upgrading, operating and making available ***own facilities*** and related services to a wide range of users ***and stakeholders***;

Or. en

Amendment 34

Proposal for a regulation

Article 4 – paragraph 1 – point 3 – point a a (new)

Text proposed by the Commission

(a a) facilitating access to facilities and related services other than its own to a wide range of users and stakeholders, where these are made available;

Amendment

Or. en

Amendment 35

Proposal for a regulation

Article 4 – paragraph 1 – point 3 – point b

Text proposed by the Commission

(b) ***having regard to the state-of-the-art cybersecurity industrial and research***

Amendment

(b) providing support to other entities, including financially, to acquiring,

*infrastructures and related services, providing support to other entities, including financially, to acquiring, upgrading, operating and making available such **infrastructures** and related services to a wide range of users **across the Union from industry including SMEs, the public sector and the research and scientific community**;*

upgrading, operating and making available such *facilities* and related services to a wide range of users **and stakeholders**;

Or. en

Amendment 36

Proposal for a regulation

Article 4 – paragraph 1 – point 3 – point b a (new)

Text proposed by the Commission

Amendment

(ba) providing financial support and technical assistance to cybersecurity start-ups, SMEs, micro-enterprises, individual experts; to Free and Open Source Software projects, commonly used for infrastructure, products and processes; and to civic tech projects;

Or. en

Amendment 37

Proposal for a regulation

Article 4 – paragraph 1 – point 3 – point b b (new)

Text proposed by the Commission

Amendment

(bb) providing software security code audits and improvements for Free and Open Source Software projects, commonly used for infrastructure, products and processes;

Or. en

Amendment 38

Proposal for a regulation

Article 4 – paragraph 1 – point 3 – point c

Text proposed by the Commission

(c) **providing** cybersecurity knowledge and technical assistance **to** industry **and** public authorities, in particular by supporting actions aimed at facilitating access to the expertise available in the Network and the Cybersecurity Competence Community;

Amendment

(c) **facilitating the sharing of** cybersecurity knowledge and technical assistance **among others to civil society, the** industry, public authorities, **and the academic and research community**, in particular by supporting actions aimed at facilitating access to the expertise available in the Network and the Cybersecurity Competence Community;

Or. en

Amendment 39

Proposal for a regulation

Article 4 – paragraph 1 – point 3 – point c a (new)

Text proposed by the Commission

Amendment

(c a) promoting “security by design” as principle in the process of developing, maintaining, operating, and updating infrastructures, products and services; in particular by supporting state-of-the-art secure development methods, adequate security testing, security audits; including the commitment of producer or provider to make available updates remedying new vulnerabilities or threats, without delay, and beyond the estimated product lifetime, or enabling a third party to create and provide such updates;

Or. en

Amendment 40

Proposal for a regulation

Article 4 – paragraph 1 – point 3 – point c b (new)

Text proposed by the Commission

Amendment

(c b) promoting the development of source code contribution policies, in particular where Free and Open Source Software projects are used, modified, and enhanced in public authorities; and especially where the Free and Open Source Software is commonly used for infrastructure, products and processes;

Or. en

Amendment 41

Proposal for a regulation

Article 4 – paragraph 1 – point 4 – introductory part

Text proposed by the Commission

Amendment

4. contribute to the wide deployment of state-of-the-art **cyber security** products and **solutions** across the **economy**, by carrying out the following tasks:

4. contribute to the wide deployment of state-of-the-art **and sustainable cybersecurity** products and **processes** across the **Union**, by carrying out the following tasks:

Or. en

Amendment 42

Proposal for a regulation

Article 4 – paragraph 1 – point 4 – point a

Text proposed by the Commission

Amendment

(a) stimulating cybersecurity research, development and the uptake of Union cybersecurity products and **solutions** by public authorities and **user industries**;

(a) stimulating cybersecurity research, development and the uptake of Union cybersecurity products and **processes**, **including** by public authorities and **industry**;

Amendment 43

Proposal for a regulation

Article 4 – paragraph 1 – point 4 – point b

Text proposed by the Commission

(b) assisting public authorities, demand side industries and other users in adopting and integrating *the latest cyber security solutions*;

Amendment

(b) assisting public authorities, demand side industries and other users in adopting and integrating *commonly used, state-of-the-art cybersecurity products and processes*;

Or. en

Amendment 44

Proposal for a regulation

Article 4 – paragraph 1 – point 4 – point c

Text proposed by the Commission

(c) supporting in particular public authorities in organising their public procurement, or carrying out procurement of state-of-the-art cybersecurity products and *solutions* on behalf of public authorities;

Amendment

(c) supporting in particular public authorities in organising their public procurement, or carrying out procurement of state-of-the-art cybersecurity products and *processes* on behalf of public authorities, *including by providing support for sustainable procurement*;

Or. en

Amendment 45

Proposal for a regulation

Article 4 – paragraph 1 – point 4 – point d

Text proposed by the Commission

(d) providing financial support and technical assistance to cybersecurity start-ups *and SMEs* to connect to potential

Amendment

(d) providing financial support and technical assistance to cybersecurity start-ups, *SMEs, micro-enterprises, individual*

markets and to attract investment;

experts, commonly used Free and Open Source Software projects, and civic tech projects, to connect to potential markets, deployment opportunities, and to attract investment;

Or. en

Amendment 46

Proposal for a regulation

Article 4 – paragraph 1 – point 5 – introductory part

Text proposed by the Commission

Amendment

5. improve the understanding of cybersecurity *and* contribute to reducing skills gaps in the Union related to cybersecurity by carrying out the following tasks:

5. improve the understanding of cybersecurity, contribute to reducing skills gaps *and strengthening the level of skills* in the Union related to cybersecurity by carrying out the following tasks:

Or. en

Amendment 47

Proposal for a regulation

Article 4 – paragraph 1 – point 5 – point -a (new)

Text proposed by the Commission

Amendment

(-a) raising awareness for the infrastructure-relevance of some commonly used Free and Open Source Software projects, products and processes in coordination with relevant Union agencies and bodies including ENISA, as well as the Network and the Community;

Or. en

Amendment 48

Proposal for a regulation

Article 4 – paragraph 1 – point 5 – point a

Text proposed by the Commission

(a) supporting further development of cybersecurity skills, ***where appropriate together*** with relevant EU agencies and bodies including ENISA.

Amendment

(a) supporting further development of cybersecurity ***processes, skills, and competences; facilitating a common high level of cybersecurity knowledge; and contributing to the resilience of users and infrastructures in the Union in coordination*** with relevant EU agencies and bodies including ENISA, ***as well as the Network.***

Or. en

Amendment 49

Proposal for a regulation

Article 4 – paragraph 1 – point 6 – point a

Text proposed by the Commission

(a) providing financial support to cybersecurity research efforts based on a common, continuously evaluated and improved multiannual strategic, industrial, technology and research ***agenda***;

Amendment

(a) providing financial support to cybersecurity research efforts based on a common, continuously evaluated and improved multiannual strategic, industrial, technology and research ***plan***;

Or. en

Justification

Aligning wording with Art. 13

Amendment 50

Proposal for a regulation

Article 4 – paragraph 1 – point 6 – point b

Text proposed by the Commission

(b) ***support*** large-scale research and

Amendment

(b) ***supporting*** large-scale research and

demonstration projects in next generation cybersecurity technological capabilities, in collaboration with the industry *and* the Network;

demonstration projects in next generation cybersecurity technological capabilities, in collaboration with the industry, the Network, *and the Community*;

Or. en

Amendment 51

Proposal for a regulation

Article 4 – paragraph 1 – point 6 – point c

Text proposed by the Commission

(c) *support* research and innovation for standardisation in cybersecurity *technology*

Amendment

(c) *supporting* research and innovation for *formal and non-formal* standardisation in cybersecurity, *where appropriate in close cooperation with the European Standardisation Organisations*;

Or. en

Amendment 52

Proposal for a regulation

Article 4 – paragraph 1 – point 6 – point c a (new)

Text proposed by the Commission

Amendment

(ca) *supporting the development of independent products and processes that can be freely studied, shared, and built upon, in close cooperation with the industry, the Network and the Community.*

Or. en

Amendment 53

Proposal for a regulation

Article 4 – paragraph 1 – point 7

Text proposed by the Commission

Amendment

- 7. *enhance cooperation between the civil and defence spheres with regard to dual use technologies and applications in cybersecurity, by carrying out the following tasks:*** ***deleted***
- (a) supporting Member States and industrial and research stakeholders with regard to research, development and deployment;***
 - (b) contributing to cooperation between Member States by supporting education, training and exercises ;***
 - (c) bringing together stakeholders, to foster synergies between civil and defence cyber security research and markets;***

Or. en

Amendment 54

Proposal for a regulation Article 4 – paragraph 1 – point 8

Text proposed by the Commission

Amendment

- 8. *enhance synergies between the civil and defence dimensions of cybersecurity in relation to the European Defence Fund by carrying out the following tasks:*** ***deleted***
- (a) providing advice, sharing expertise and facilitating collaboration among relevant stakeholders;***
 - (b) managing multinational cyber defence projects, when requested by Member States, and thus acting as a project manager within the meaning of Regulation XXX [Regulation establishing the European Defence Fund].***

Or. en

Amendment 55

Proposal for a regulation

Article 4 – paragraph 1 – point 8 a (new)

Text proposed by the Commission

Amendment

8 a. contribute to the Union's efforts to enhance cooperation with regard to cybersecurity by:

(a) facilitating the participation of the Network and the Community in international conferences;

(b) facilitating the contribution of the Network and the Community to standardisation organisations;

(c) cooperating with third countries and international organisations within relevant international cooperation frameworks;

(d) facilitating the participation of the Governing Board in international governmental organisations;

(e) assisting and providing advice to the Commission with regard to the implementation of Regulation (EU) 2019/XXX [recast of Regulation (EC) No 428/2009 as proposed by COM(2016)616]^{1a};

^{1a} Regulation (EU) 2019/XXX of the European Parliament and the Council of ... setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items, and EU restrictive measures in force, in particular as regards the export of cybersurveillance and intrusion technology (OJ L ..., ..., p. ...).

Or. en

Amendment 56

Proposal for a regulation

Article 4 – paragraph 1 – point 8 b (new)

Text proposed by the Commission

Amendment

8 b. contributing to the fundamental rights and ethics assessment of cybersecurity research funded by the Competence Centre.

Or. en

Amendment 57

Proposal for a regulation

Article 5 – title

Text proposed by the Commission

Amendment

Investment in and use of infrastructures, capabilities, products or **solutions**

Investment in and use of infrastructures, capabilities, products or **processes**

Or. en

Amendment 58

Proposal for a regulation

Article 5 – paragraph 1 – introductory part

Text proposed by the Commission

Amendment

1. Where the Competence Centre provides funding for infrastructures, capabilities, products or **solutions** pursuant to Article 4(3) and (4) in the form of a grant or a prize, the work plan of the Competence Centre may specify in particular:

1. Where the Competence Centre provides funding for infrastructures, capabilities, products or **processes** pursuant to Article 4(3) and (4) in the form of a grant or a prize, the work plan of the Competence Centre may specify in particular:

Or. en

Amendment 59

Proposal for a regulation

Article 5 – paragraph 1 – point a a (new)

Text proposed by the Commission

Amendment

(a a) ensure that as a result of Union contribution, access is open by default and re-use is possible;

Or. en

Amendment 60

Proposal for a regulation

Article 5 – paragraph 1 – point b

Text proposed by the Commission

Amendment

(b) rules governing access to and use of an infrastructure or capability.

(b) **additional** rules governing access to and use of an infrastructure or capability.

Or. en

Amendment 61

Proposal for a regulation

Article 5 – paragraph 2

Text proposed by the Commission

Amendment

2. The Competence Centre may be responsible for the overall execution of relevant joint procurement actions including pre-commercial procurements on behalf of members of the Network, **members of the cybersecurity Competence Community, or other third parties representing the users of cybersecurity products and solutions**. For this purpose, the Competence Centre may be assisted by one or more National Coordination Centres or members of the Cybersecurity

2. The Competence Centre may be responsible for the overall execution of relevant joint procurement actions including pre-commercial procurements on behalf of members of the Network. For this purpose, the Competence Centre may be assisted by one or more National Coordination Centres or members of the Cybersecurity Competence Community.

Amendment 62

Proposal for a regulation Article 6 – paragraph 4

Text proposed by the Commission

4. The nominated National Coordination Centre shall have the capability to support the Competence Centre and the Network in fulfilling their mission laid out in Article 3 of this Regulation. They shall possess or have direct access to technological expertise in cybersecurity and be in a position to effectively engage and coordinate with industry, the public sector and the research community.

Amendment

4. The nominated National Coordination Centre shall have the capability to support the Competence Centre and the Network in fulfilling their mission laid out in Article 3 of this Regulation. They shall possess or have direct access to technological expertise in cybersecurity and be in a position to effectively engage and coordinate with industry, the public sector and the ***academic and*** research community. ***The Commission shall issue guidelines further detailing the assessment procedure and explaining the application of the criteria.***

Amendment 63

Proposal for a regulation Article 6 – paragraph 5

Text proposed by the Commission

5. The relationship between the Competence Centre and the National Coordination Centres shall be based on a contractual agreement signed between the Competence Centre and each of the National Coordination Centres. The agreement shall ***provide for*** the rules governing the relationship and division of tasks between the Competence Centre and each National Coordination Centre.

Amendment

5. The relationship between the Competence Centre and the National Coordination Centres shall be based on a contractual agreement signed between the Competence Centre and each of the National Coordination Centres. The agreement shall ***consist of the same set of general conditions providing*** the rules governing the relationship and division of tasks between the Competence Centre and

each National Coordination Centre *and special conditions tailored on the particular National Coordination Centre.*

Or. en

Amendment 64

Proposal for a regulation Article 7 – paragraph 1 – point a

Text proposed by the Commission

(a) supporting the Competence Centre in achieving its objectives and in particular in coordinating the Cybersecurity Competence Community;

Amendment

(a) supporting the Competence Centre in achieving its objectives and in particular in ***establishing and*** coordinating the Cybersecurity Competence Community;

Or. en

Amendment 65

Proposal for a regulation Article 7 – paragraph 1 – point b

Text proposed by the Commission

(b) facilitating the participation of industry and other actors at the Member State level in cross-border projects;

Amendment

(b) ***promoting, encouraging and*** facilitating the participation of ***civil society, industry, in particular start-ups and SMEs, academic and research community,*** and other actors at the Member State level in cross-border projects;

Or. en

Amendment 66

Proposal for a regulation Article 7 – paragraph 1 – point c

Text proposed by the Commission

(c) contributing, together with the Competence Centre, to identifying and addressing sector-specific **cyber security industrial** challenges;

Amendment

(c) contributing, together with the Competence Centre, to identifying and addressing sector-specific **cybersecurity** challenges;

Or. en

Amendment 67

Proposal for a regulation

Article 7 – paragraph 1 – point e

Text proposed by the Commission

(e) seeking to establish synergies with relevant activities at the national **and** regional level;

Amendment

(e) seeking to establish synergies with relevant activities at the national, regional **and local** level;

Or. en

Amendment 68

Proposal for a regulation

Article 7 – paragraph 1 – point f a (new)

Text proposed by the Commission

Amendment

(f a) promoting and disseminating a common minimal cybersecurity educational curricula in cooperation with the relevant bodies in the Member States;

Or. en

Amendment 69

Proposal for a regulation

Article 7 – paragraph 1 – point g

Text proposed by the Commission

(g) promoting and disseminating the relevant outcomes of the work by the Network, the Cybersecurity Competence Community and the Competence Centre at national *or* regional level;

Amendment

(g) promoting and disseminating the relevant outcomes of the work by the Network, the Cybersecurity Competence Community and the Competence Centre at national, regional, *or local* level;

Or. en

Amendment 70

**Proposal for a regulation
Article 7 – paragraph 1 – point h**

Text proposed by the Commission

(h) assessing requests by entities established in the same Member State as the Coordination Centre for becoming part of the Cybersecurity Competence Community.

Amendment

(h) assessing requests by entities *and individuals* established in the same Member State as the Coordination Centre for becoming part of the Cybersecurity Competence Community.

Or. en

Amendment 71

**Proposal for a regulation
Article 8 – paragraph 1**

Text proposed by the Commission

1. The Cybersecurity Competence Community *shall contribute* to the mission of the Competence Centre as laid down in Article 3 and *enhance and disseminate* cybersecurity expertise across the Union.

Amendment

1. The Cybersecurity Competence Community *contributes* to the mission of the Competence Centre as laid down in Article 3 and *enhances and disseminates* cybersecurity expertise across the Union *and provides technical expertise*.

Or. en

Amendment 72

Proposal for a regulation

Article 8 – paragraph 2

Text proposed by the Commission

2. The Cybersecurity Competence Community shall consist of industry, academic and **non-profit** research organisations, **and associations** as well as public entities and other entities dealing with operational and technical matters. It shall bring together the main stakeholders with regard to cybersecurity technological **and** industrial capacities in the Union. **It** shall involve National Coordination Centres as well as Union institutions and bodies with relevant expertise..

Amendment

2. The Cybersecurity Competence Community shall consist of **civil society**, industry, academic and research **community, associations, individual experts, relevant European Standardisation** Organisations, as well as public entities and other entities dealing with operational and technical matters **in the area of cybersecurity**. It shall bring together the main stakeholders with regard to cybersecurity technological, industrial, **academic and research, and societal** capacities **and capabilities** in the Union **and** shall involve National Coordination Centres as well as Union institutions and bodies with relevant expertise.

Or. en

Amendment 73

Proposal for a regulation

Article 8 – paragraph 3 – introductory part

Text proposed by the Commission

3. Only entities which are established within the Union may be accredited as members of the Cybersecurity Competence Community. **They** shall demonstrate that they **have cybersecurity** expertise with regard to at least one of the following domains:

Amendment

3. Only entities which are established, **and individuals resident** within the Union may be accredited as members of the Cybersecurity Competence Community. **The Governing Board shall specify criteria for cybersecurity expertise and applicants** shall demonstrate that they **can provide such** expertise with regard to at least one of the following domains:

Or. en

Amendment 74

Proposal for a regulation Article 8 – paragraph 3 – point a

Text proposed by the Commission

(a) research;

Amendment

(a) ***academia or*** research;

Or. en

Amendment 75

Proposal for a regulation Article 8 – paragraph 3 – point a a (new)

Text proposed by the Commission

(aa) ***ethics;***

Amendment

Or. en

Amendment 76

Proposal for a regulation Article 8 – paragraph 3 – point b a (new)

Text proposed by the Commission

(ba) ***professional services or the
deployment thereof;***

Amendment

Or. en

Amendment 77

Proposal for a regulation Article 8 – paragraph 3 – point b b (new)

Text proposed by the Commission

(bb) ***formal and technical
standardisation and specifications;***

Amendment

Amendment 78**Proposal for a regulation
Article 8 – paragraph 4***Text proposed by the Commission*

4. The Competence Centre shall accredit entities established under national law as members of the Cybersecurity Competence Community after an assessment made by the National Coordination Centre of the Member State where the entity is established, on whether that entity meets the criteria provided for in paragraph 3. An accreditation shall not be limited in time but may be revoked by the Competence Centre at any time if it or the relevant National Coordination Centre considers that the entity does not fulfil the criteria set out in paragraph 3 or it falls under the relevant provisions set out in Article 136 of Regulation XXX [new financial regulation].

Amendment

4. The Competence Centre shall accredit entities established under national law, ***or individuals***, as members of the Cybersecurity Competence Community after an assessment made by the National Coordination Centre of the Member State where the entity is established, ***or the individual is a resident***, on whether that entity ***or individual*** meets the criteria provided for in paragraph 3. An accreditation shall not be limited in time but may be revoked by the Competence Centre at any time if it or the relevant National Coordination Centre considers that the entity does not fulfil the criteria set out in paragraph 3 or it falls under the relevant provisions set out in Article 136 of Regulation XXX [new financial regulation]. ***The National Coordination Centres of the Member States shall aim to achieve a balanced representation of stakeholders in the Community, actively stimulating participation from under-represented categories and groups of individuals.***

Or. en

Amendment 79**Proposal for a regulation
Article 10 – paragraph 1***Text proposed by the Commission*

1. The Competence Centre shall cooperate with relevant Union institutions,

Amendment

1. The Competence Centre shall cooperate with relevant Union institutions,

bodies, offices and agencies including the European Union Agency for Network and Information Security, the Computer Emergency Response Team (CERT-EU), *the European External Action Service*, the Joint Research Centre of the Commission, the Research Executive Agency, Innovation and Networks Executive Agency, European Cybercrime Centre at Europol *as well as the European Defence Agency*.

bodies, offices and agencies including the European Union Agency for Network and Information Security (*ENISA*), the Computer Emergency Response Team (CERT-EU), the Joint Research Centre of the Commission, the Research Executive Agency, *the* Innovation and Networks Executive Agency, *as well as the* European Cybercrime Centre at Europol.

Or. en

Amendment 80

Proposal for a regulation Article 10 – paragraph 2

Text proposed by the Commission

2. Such cooperation shall take place within the framework of working arrangements. Those arrangements shall be *submitted to the* prior approval of the Commission.

Amendment

2. Such cooperation shall take place within the framework of working arrangements. Those arrangements shall be *adopted by the Governing Board after* prior approval of the Commission.

Or. en

Amendment 81

Proposal for a regulation Article 12 – paragraph 1

Text proposed by the Commission

1. The Governing Board shall be composed of one representative of each Member State, and five representatives of the Commission, on behalf of the Union.

Amendment

1. The Governing Board shall be composed of one representative of each Member State, *five representatives from the European Parliament*, and five representatives of the Commission, on behalf of the Union.

Or. en

Amendment 82

Proposal for a regulation Article 12 – paragraph 3

Text proposed by the Commission

3. Members of the Governing Board and their alternates shall be appointed in light of their knowledge in the field of **technology** as well as of relevant managerial, administrative and budgetary skills. The Commission and the Member States shall make efforts to limit the turnover of their representatives in the Governing Board, in order to ensure continuity of the Board's work. The Commission and the Member States shall **aim to** achieve a balanced representation between men and women on the Governing Board.

Amendment

3. Members of the Governing Board and their alternates shall be appointed in light of their knowledge in the field of **cybersecurity** as well as of relevant managerial, administrative and budgetary skills. The Commission and the Member States shall make efforts to limit the turnover of their representatives in the Governing Board, in order to ensure continuity of the Board's work. The Commission and the Member States shall achieve a balanced representation between men and women on the Governing Board.

Or. en

Amendment 83

Proposal for a regulation Article 12 – paragraph 6

Text proposed by the Commission

6. The **Commission** may invite observers, including representatives of relevant Union bodies, offices and agencies, to take part in the meetings of the Governing Board as appropriate.

Amendment

6. The **Governing Board** may invite observers, including representatives of relevant Union bodies, offices and agencies, to take part in the meetings of the Governing Board as appropriate.

Or. en

Amendment 84

Proposal for a regulation Article 12 – paragraph 7

Text proposed by the Commission

7. The European Agency for Network and Information Security (ENISA) shall ***be a permanent observer in*** the Governing Board.

Amendment

7. The European Agency for Network and Information Security (ENISA) shall ***permanently take part in the deliberations of*** the Governing Board, ***in an advisory role without voting rights.***

Or. en

Amendment 85

Proposal for a regulation

Article 13 – paragraph 3 – point e a (new)

Text proposed by the Commission

Amendment

(ea) adopt the working arrangements referred to in Article 10(2);

Or. en

Amendment 86

Proposal for a regulation

Article 13 – paragraph 3 – point l

Text proposed by the Commission

Amendment

(l) promote the Competence Centre ***globally, so as to raise its attractiveness and make it a world-class body for excellence in cybersecurity;***

(l) promote ***the cooperation of*** the Competence Centre ***with global actors;***

Or. en

Amendment 87

Proposal for a regulation

Article 16 – paragraph 3

Text proposed by the Commission

3. The Executive Director shall be appointed by the Governing Board from a list of candidates proposed by the Commission, following an open *and* transparent selection procedure.

Amendment

3. The Executive Director shall be appointed by the Governing Board from a list of candidates proposed by the Commission, following an open, transparent *and non-discriminatory* selection procedure.

Or. en

Amendment 88

Proposal for a regulation

Article 16 – paragraph 3 a (new)

Text proposed by the Commission

Amendment

3a. Before appointment, the candidate selected by the Governing Board shall make a statement before the relevant committee of the European Parliament and answer Members' questions when invited to do so.

Or. en

Amendment 89

Proposal for a regulation

Article 16 – paragraph 5

Text proposed by the Commission

Amendment

5. The term of office of the Executive Director shall be *four* years. By the end of that period, the *Commission* shall carry out an assessment which takes into account the evaluation of the performance of the Executive Director and the Competence Centre's future tasks and challenges.

5. The term of office of the Executive Director shall be *five* years. By the end of that period, the *Governing Board* shall carry out an assessment which takes into account the evaluation of the performance of the Executive Director and the Competence Centre's future tasks and challenges.

Or. en

Amendment 90

Proposal for a regulation Article 16 – paragraph 6

Text proposed by the Commission

6. The Governing Board may, **acting on a proposal from the Commission which takes** into account the assessment referred to in paragraph 5, extend once the term of office of the Executive Director for no more than **four** years.

Amendment

6. The Governing Board may, **taking** into account the assessment referred to in paragraph 5, extend once the term of office of the Executive Director for no more than **five** years.

Or. en

Amendment 91

Proposal for a regulation Article 16 – paragraph 8

Text proposed by the Commission

8. The Executive Director shall be removed from office only by decision of the Governing Board, acting on a proposal from the Commission.

Amendment

8. The Executive Director shall be removed from office only by decision of the Governing Board, acting on **its own initiative or on** a proposal from the Commission.

Or. en

Amendment 92

Proposal for a regulation Article 17 – paragraph 2 – point h

Text proposed by the Commission

(h) prepare an action plan following-up on the conclusions of the retrospective evaluations and reporting on progress every two years to the Commission

Amendment

(h) prepare an action plan following-up on the conclusions of the retrospective evaluations and reporting on progress every two years to the Commission **and the European Parliament;**

Amendment 93

Proposal for a regulation

Article 17 – paragraph 2 – point s

Text proposed by the Commission

(s) prepare an action plan following-up conclusions of internal or external audit reports, as well as investigations by the European Anti-Fraud Office (OLAF) and reporting on progress twice a year to the Commission and regularly to the Governing Board;

Amendment

(s) prepare an action plan following-up conclusions of internal or external audit reports, as well as investigations by the European Anti-Fraud Office (OLAF) and reporting on progress twice a year to the Commission and ***the European Parliament and*** regularly to the Governing Board;

Or. en

Amendment 94

Proposal for a regulation

Article 17 – paragraph 2 – point v

Text proposed by the Commission

(v) ensure effective communication with the Union's institutions;

Amendment

(v) ensure effective communication with the Union's institutions ***and report to the European Parliament and to the Council annually or on invitation;***

Or. en

Amendment 95

Proposal for a regulation

Article 18 – paragraph 1

Text proposed by the Commission

1. The Industrial and Scientific Advisory Board shall consist of no more than 16 members. The members shall be

Amendment

1. The Industrial and Scientific Advisory Board shall consist of no more than 16 members. The members shall be

appointed by the Governing Board from among the representatives of the entities of the Cybersecurity Competence Community.

appointed by the Governing Board from among the representatives of the entities of the Cybersecurity Competence Community ***according to an open, transparent and non-discriminatory procedure. The Board shall include at least three members each from industry, academic community and civil society including consumer organisations.***

Or. en

Amendment 96

Proposal for a regulation Article 19 – paragraph 1

Text proposed by the Commission

1. The Industrial and Scientific Advisory Board shall meet at least ***twice*** a year.

Amendment

1. The Industrial and Scientific Advisory Board shall meet at least ***three times*** a year.

Or. en

Amendment 97

Proposal for a regulation Article 19 – paragraph 2

Text proposed by the Commission

2. ***The Industrial and Scientific Advisory Board may advise the Governing Board on the establishment of working groups on specific issues relevant to the work of the Competence Centre where necessary under the overall coordination of one or more members of the Industrial and Scientific Advisory Board.***

Amendment

deleted

Or. en

Amendment 98

Proposal for a regulation

Article 20 – paragraph 1 – point 1 a (new)

Text proposed by the Commission

Amendment

(1a) advise the Governing Board on the establishment of working groups on specific issues relevant to the work of the Competence Centre;

Or. en

Amendment 99

Proposal for a regulation

Article 21 – paragraph 4

Text proposed by the Commission

Amendment

4. The Union financial contribution shall not cover the tasks referred to in Article 4(8)(b) ***deleted***

Or. en

Amendment 100

Proposal for a regulation

Article 22 – paragraph 4

Text proposed by the Commission

Amendment

4. The Commission may terminate, proportionally reduce or suspend the Union's financial contribution to the Competence Centre if the participating Member States do not contribute, contribute only partially **or contribute late** with regard to the contributions referred to in paragraph 1. ***4. The Commission may terminate, proportionally reduce or suspend the Union's financial contribution to the Competence Centre if the participating Member States do not contribute, **or** contribute only partially with regard to the contributions referred to in paragraph 1.***

Or. en

Amendment 101

Proposal for a regulation

Article 23 – paragraph 4 – point a

Text proposed by the Commission

(a) participating Member States' financial contributions to the administrative costs;

Amendment

(a) **the Union's and** participating Member States' financial contributions to the administrative costs;

Or. en

Justification

Missing from the Commission proposal by accident

Amendment 102

Proposal for a regulation

Article 23 – paragraph 4 – point b

Text proposed by the Commission

(b) participating Member States' financial contributions to the operational costs;

Amendment

(b) **the Union's and** participating Member States' financial contributions to the operational costs;

Or. en

Justification

Missing from the Commission proposal by accident

Amendment 103

Proposal for a regulation

Article 23 – paragraph 8 a (new)

Text proposed by the Commission

Amendment

8a. The Competence Centre shall cooperate closely with other Union institutions, agencies, and bodies in order

to reduce administrative costs.

Or. en

Amendment 104

Proposal for a regulation Article 35 – paragraph 2

Text proposed by the Commission

2. The Competence Centre shall ensure that the public and any interested parties are *given appropriate*, objective, reliable and easily accessible information, in particular with regard to the results of *its work*. It shall also make public the declarations of interest made in accordance with Article 41.

Amendment

2. The Competence Centre shall ensure that the public and any interested parties are *provided with comprehensive*, objective, reliable and easily accessible information, in particular with regard to the results of *the work of the Competence Centre, the Network, the Industry and Scientific Advisory Board and the Community*. It shall also make public the declarations of interest made in accordance with Article 42.

Or. en

Justification

"Article 41" reference corrected to Article 42 as discussed with the Commission.

Amendment 105

Proposal for a regulation Article 35 – paragraph 2 a (new)

Text proposed by the Commission

Amendment

2a. The Competence Centre shall provide the public and any interested parties with a list of the Cybersecurity Competence Community members and shall make public the declarations of interest made by them in accordance with Article 42.

Or. en

Amendment 106

Proposal for a regulation Article 38 a (new)

Text proposed by the Commission

Amendment

Article 38a

Legal Personality of the Competence Centre

- 1. The Competence Centre shall have legal personality.*
- 2. In each Member State, the Competence Centre shall enjoy the most extensive legal capacity accorded to legal persons under the laws of that Member State. It may, in particular, acquire or dispose of movable and immovable property and may be a party to legal proceedings.*

Or. en

Justification

This is a technical amendment. The paragraph was moved here from Art. 1(4).

Amendment 107

Proposal for a regulation Article 42 – paragraph 1

Text proposed by the Commission

Amendment

The Competence Centre Governing Board shall adopt rules for the prevention ***and management*** of conflicts of interest in respect of its members, bodies and staff. ***Those rules shall contain the provisions intended to avoid a conflict of interest in respect of the representatives of the members serving in*** the Governing Board as well as the Scientific and Industrial Advisory Board ***in accordance with***

The Competence Centre Governing Board shall adopt rules for the prevention, ***identification, and resolution*** of conflicts of interest in respect of its members, bodies and staff, the Governing Board, as well as the Scientific and Industrial Advisory Board, ***and the Community.***

Regulation XXX [new Financial Regulation].

Or. en

Justification

Second part moved to paragraph 3.

Amendment 108

**Proposal for a regulation
Article 42 – paragraph 1 a (new)**

Text proposed by the Commission

Amendment

Member States shall ensure the prevention, identification, and resolution of conflicts of interest in respect of the National Coordination Centres.

Or. en

Amendment 109

**Proposal for a regulation
Article 42 – paragraph 1 b (new)**

Text proposed by the Commission

Amendment

The rules referred to in paragraph 1 shall comply with Regulation (EU, Euratom) 2018/1046.

Or. en

Justification

Second sentence from paragraph 1 moved and modified.

Amendment 110

**Proposal for a regulation
Article 44 – title**

Text proposed by the Commission

Amendment

Support from the host Member State

Seat and Support from the host Member State

Or. en

Amendment 111

Proposal for a regulation

Article 44 – paragraph -1 (new)

Text proposed by the Commission

Amendment

-1. The seat of the Competence Centre shall be located in [Brussels, Belgium].

Or. en

Justification

This is a technical amendment. Paragraph moved from Art. 1(3) here.

Amendment 112

Proposal for a regulation

Article 44 – paragraph -1 a (new)

Text proposed by the Commission

Amendment

-1 a The host Member State shall provide the best possible conditions to ensure the proper functioning of the Competence Centre, including a single location, the accessibility of the location, the existence of adequate education facilities for the children of staff members, appropriate access to the labour market, social security and medical care for both children and partners.

Or. en

Amendment 113

Proposal for a regulation Article 44 – paragraph 1

Text proposed by the Commission

An administrative agreement *may* be concluded between the Competence Centre and the Member State [Belgium] in which its seat is located concerning privileges and immunities and other support to be provided by that Member State to the Competence Centre.

Amendment

An administrative agreement *shall* be concluded between the Competence Centre and the Member State [Belgium] in which its seat is located concerning privileges and immunities and other support to be provided by that Member State to the Competence Centre.

Or. en

EXPLANATORY STATEMENT

The Commission proposal establishing a *Cybersecurity Industrial, Technology, and Research Competence Centre and the Network of National Coordination Centres* is a welcome opportunity to design the future of European cooperation on the issue of cybersecurity.

Similar to other parts of the European economy, cybersecurity innovation, products, processes and services are in large part created in small and medium size enterprises. Innovation, when it is not produced within these SMEs themselves, takes place in start-ups and the research community. These economically oriented communities are supported by individual entrepreneurs, and very often, important impulses come from civil-society, and non-commercial or pre-commercial civic tech projects that make use of open standards, open data, and Free and Open Source Software to contribute to the common good.

We need to make sure that the European Cybersecurity framework seizes the opportunities and makes use of the strengths that the sector, as it is currently structured in Europe, can provide.

The proposed set-up of the Centre links the activities of Horizon Europe for cybersecurity research and of Digital Europe for cybersecurity deployment, thereby ideally creating synergies and spill-over effects between both Union programmes. Furthermore the Centre should facilitate and coordinate the work of the Cybersecurity Competence Network and should drive the cybersecurity technological agenda and facilitate access to the expertise gathered in the Network and the Community. The Commission considered to best achieve these goals by creating a new Union body, comprising elements of a joint undertaking, an executive agency and a decentralised agency. Given that with ENISA there is already another dedicated EU cybersecurity agency, this proposal should ensure that ENISA is consulted on all the Centre's relevant activities, to create synergies.

Cybersecurity as a process

The IT industry has long used the term “solution” to describe products and services in public relations contexts and commercial endorsements. However, it is important to understand cybersecurity as a process. With ICT technology constantly evolving, so do the threats. The efforts to make our infrastructure, networks and information systems more secure do not end with the purchase of a certain product or a service.

That is why it is important to strengthen cybersecurity constantly, throughout the lifecycle of a product, and taking into account the interplay of products and actors in connected networks and infrastructures like the Internet. Throughout the lifecycle phases of a system, the design, implementation, maintenance, and update phases, security should be an overarching principle.

Security of the Common Infrastructure

The Internet is the common infrastructure that not only the European but the worldwide economy, more and more relies on. In addition, it is the common infrastructure for communication, culture, and information that individuals rely on, on a daily basis.

From the basic infrastructure layer up to the applications that users interact with, Free and Open Source Software plays an integral role in the functioning of the Internet. As with any commonly used component, if a security vulnerability is discovered in a Free and Open Source Software component, the vulnerability can threaten the functioning of the Internet and related services.

Vulnerable “Internet of Things” devices have already been known to be used to attack other infrastructures. On the Internet, a security vulnerability in a consumer device can affect a high performance computing facility.

Such components are commonly developed, used, and built upon by various industrial actors, in research and development, as well as by public bodies. Consequently, in order to enhance the overall reliability, resilience, and security of our common infrastructure, the Centre’s activities should realise the role of commonly used Free and Open Source Software, and contribute to its security.

Resilience rather than Defence and Dual-Use Technologies

Due to the functioning of networks and information systems like the Internet, it is usually not possible to invariably attribute the origin of an attack to an entity with absolute certainty. Quite to the opposite, evidence can be fabricated to disguise a source, or to lead to wrong conclusions. In this context especially, it is a worrying development that states and intergovernmental organisations have started considering to use conventional military force in the case of cyberattacks.

It is a priority of the European Union to promote democracy, the rule of law, human rights and fundamental freedoms worldwide. Therefore, the Centre should promote and invest into the resilience and integrity of networks and information systems. Cybersecurity products and processes can be equally useful in civilian and military contexts, therefore the Centre should support existing frameworks for the control of dual-use technologies. Offensive military applications such as backdoors, withheld vulnerabilities, or exploits bear an inherent security risk for society at large and would run counter to the Centre's goal of improving cybersecurity. It is therefore important to limit the Centre's activities to civilian purposes.

Financing the Centre's structures and operating costs from Union programmes that may not be used for military purposes means that the Centre shouldn't facilitate any defence research or other defence-related projects. The Treaties need to be respected and the Union budget not used for military purposes.

Society, Ethics and Representation

The Centre should thoroughly take into account the societal and ethical implications and concerns that its actions, the actions of its bodies and the outcomes of products, services, facilities, and research funded by it may have.

More than other industries, the ICT sector is struggling to fulfil the demand for skilled workers. At the same time, the representation of genders, ethnic diversity and disabled persons is extraordinarily imbalanced. That is why it is in the interest of the industry,

including academia, research and others, to achieve balanced representation.

More so, it is in the interest of equality.

Governance Structure

The Centre and its bodies should make sure that conflicts of interest are not only identified, but remedied and handled in a transparent, and accountable manner. The Member States should make sure that the same goes for the National Coordination Centres.

The European Parliament should be put on equal footing with the Member States when it comes to influencing the Centre's governance and actions.