



Council of the European Union
General Secretariat

Brussels, 23 March 2020

Interinstitutional files:
2018/0328(COD)

WK 3133/2020 REV 1

LIMITE

**CYBER
TELECOM
CODEC
COPEN
COPS
COSI**

**CSC
CSCI
IND
JAI
RECH
ESPACE**

WORKING PAPER

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

WORKING DOCUMENT

From:	General Secretariat of the Council
To:	Delegations
Subject:	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 - Comments from CZ, DK, DE, EE, IE, EL, ES, FR, LU, HU, NL, AT, PL, PT, SK, FI and SE

Delegations will find in Annex comments from CZ, DK, DE, EE, IE, EL, ES, FR, LU, HU, NL, AT, PL, PT, SK, FI and SE on the above-mentioned subject.

TABLE OF CONTENT

	Page
CZECH REPUBLIC	2
DENMARK	4
GERMANY	9
ESTONIA	22
IRELAND	38
GREECE	42
SPAIN	44
FRANCE	53
LUXEMBOURG	74
HUNGARY	75
NETHERLANDS	76
AUSTRIA	77
POLAND	79
PORTUGAL	82
SLOVAK REPUBLIC	93
FINLAND	95
SWEDEN	118

CZECH REPUBLIC

COMMENTS OF THE CZECH REPUBLIC ON DRAFT REGULATION 5341/3/20 REV 3

- (14) (...) They should also support the deployment of cybersecurity products and solutions ~~and to the extent~~ while promoting where possible, ~~rely~~ the implementation of the European cybersecurity certification framework as defined by Regulation (EU) 2019/881 of the European Parliament and of the Council¹ ~~the Cybersecurity Act~~.

Article 4a

1. (...)

(a) strategic tasks, consisting of:

- (2) (...)

(i) defining priorities for its work on:

(...)

- the reinforcement of cybersecurity ~~industrial, technological and research skills and training and~~

(...)

- (3) ensuring synergies and cooperation ~~while avoiding duplication of activities~~ with relevant Union institutions, agencies and bodies such as ENISA ~~while avoiding any duplication of activities with such Union institutions, agencies and bodies~~;

Article 15

(...)

- 2. The Governing Board shall take its decisions by a majority of at least 75% of all its members, ~~with voting rights, the representatives of the Commission constituting a single member for this purpose~~. An absent member of the Governing Board may delegate his or her vote to his or her alternate or, in the absence of his or her alternate, to another member. Any member ~~of the Governing Board may represent not more than one other member. [For decisions related to the usage of Union funds in Article 13(3) except point (cb), the Union should hold 50% of the voting rights]~~.

Commented [A1]: We welcome this change of the text, it makes the wording more flexible and reasonable. We would like to keep it as it is now proposed.

Commented [A2]: We appreciate the way the changes have been made here and we suggest to keep the text as it is now.

Commented [A3]: We cannot agree with the Union holding 50% of the voting rights in described cases. It is still Member States who contribute to Union funds. Therefore, we suggest to delete this proposed sentence.

Article 38

(...)

2. Once there is sufficient information available about the implementation of this Regulation, but no later than ~~two three and a half years~~ **the date referred to in Article 45 paragraph 4 of this Regulation** ~~after the start of the implementation of this Regulation~~, the Commission shall carry out an interim evaluation of the ~~Competence Centre~~ **on the basis of terms of reference agreed with the Governing Board**. The Commission shall prepare a report on that evaluation and shall submit that report to the European Parliament and to the Council by 31 ~~July 2023~~ **December 2024**. The ~~Competence Centre~~ and Member States shall provide the Commission with the information necessary for the preparation of that report.

Commented [A4]: We would appreciate to know what was the original purpose of the change. There is probably some mistake, the logical binding of the text is missing. We suppose that there should be „two years **after** the date referred“ or „no later than the date referred“.

Article 46

(...)

2. At the end of the period referred to in paragraph 1 of this Article, ~~unless decided otherwise through a review of this Regulation~~ **the mandate of the Centre is extended in accordance with the second subparagraph of Article 38(3)**, the winding-up procedure shall be triggered. ~~The winding-up procedure shall be automatically triggered if the Union or all participating Member States withdraw from the Competence Centre.~~

Commented [A5]: We ask for the clarification here too – we assume there could be a mistake in the text. It is not possible to extend the mandate of the Centre and in the same time trigger the winding-up procedure. Maybe the word “unless” should not be deleted. Moreover, we would like to note we do not consider appropriate to extend the mandate of the Centre solely based on the Commission’s decision.

DENMARK

- (8) The ~~Competence~~ Centre should be the Union's main instrument to pool investment in cybersecurity research, technology and industrial development and to implement relevant projects and initiatives together with ~~the a Cybersecurity Competence~~ **Network of National Coordination Centre ("the Network")**. ~~The Centre~~ **It** should deliver cybersecurity-related financial support from ~~the~~ Horizon Europe - **the Framework Programme for Research and Innovation established by Regulation 2020/... of the European Parliament and of the Council² ('the Horizon Europe programme')** and the Digital Europe programme established by Regulation 2020/... of the European Parliament and of the Council³ ('the Digital Europe programmes'), and should be open to the European Regional Development Fund and other programmes where appropriate. This approach should contribute to creating synergies and coordinating financial support related to cybersecurity research, innovation, technology and industrial development and avoiding unnecessary duplication. **The Centre should not play an operational role or a technical assistance role. Upon request from a Member State the Centre should be able to provide expert cybersecurity industrial, technological, and research advice to that Member State.**

Commented [A6]: It is unclear what kind of expert advice the Centre should be able to provide to Member States. "Cybersecurity industrial, technological, and research" has been added to delineate the tasks of the Centre from the tasks of ENISA and to align the text with recital 9c, 12 and article 3 in general.

² Regulation 2020/... of the European Parliament and of the Council, of ..., establishing Horizon Europe - the Framework Programme for Research and Innovation, laying down its rules for participation and dissemination (OJ ...) [2018/0224(COD)].

³ Regulation 2020/... of the European Parliament and of the Council, of ..., establishing the Digital Europe programme for the period 2021-2027 (OJ ...) [2018/0227(COD)].

- (8a) The Competence Centre **would** benefit from the ~~particular expertise~~ experience and the broad and relevant stakeholders' representation built through the contractual public-private partnership on cybersecurity between the Commission and European Cyber Security Organisation ECSO Association during the duration of the Framework Programme for Research and Innovation (2014-2020) ("Horizon 2020"), established by Regulation (EU) No 1291/2013 of the European Parliament and of the Council⁴, and the lessons learned from four pilot projects⁵ launched in early 2019 under Horizon 2020, ~~thereby building on the existing experience that has been set up by the contractual public-private partnership on cybersecurity,~~ for the management of the Cybersecurity Competence Community, and the representation of the Cybersecurity Competence Community in the Centre.
- (9) The Centre should develop and monitor the implementation of a comprehensive and sustainable Cybersecurity Industrial, Technology and Research Agenda ~~Strategy~~ which will set out strategic recommendations and priorities for development and growth of the European cybersecurity ~~ecosystem~~ industrial, technological and research sector (the "Agenda"). The Agenda **should provide the basis for the annual and multi-annual work programme of the Centre. Furthermore, the Agenda** should be taken duly into account in particular within the ~~bi-annual and annual~~ planning and implementation of the Horizon Europe programme and the Digital Europe programme in the area of cybersecurity. The Agenda **could also serve** ~~be able to provide as~~ cybersecurity ~~industrial, technological, and research~~ specific advice, where relevant, **for** the implementation of other Union programmes.

Commented [A7]: "Industrial, technological, and research" has been added to align the text with recital 9c, 12 and article 3 in general.

⁴ Regulation (EU) No 1291/2013 of the European Parliament and of the Council of 11 December 2013 establishing Horizon 2020 - the Framework Programme for Research and Innovation (2014-2020) and repealing Decision No 1982/2006/EC (OJ L 347, 20.12.2013, p. 104).

⁵ CONCORDIA, ECHO, SPARTA and CyberSec4Europe are the four winning pilot projects of the 2018 Horizon 2020 cybersecurity call "establishing and operating a pilot for a European Cybersecurity Competence Network and developing a common European Cybersecurity Research & Innovation Roadmap".

Article 4a

Tasks of the Centre

1. In order to fulfill the mission laid out in Article 3 and the objectives laid out in Article 4, the Centre shall, in close cooperation with the Network, have the following ~~strategic and implementation~~ tasks:

(a) strategic tasks, consisting of:

(1) developing and monitoring the implementation of a comprehensive and sustainable Cybersecurity Industrial, Technology and Research Agenda, which ~~will~~ shall set out strategic recommendations and goals for the development and growth of the European cybersecurity industrial, technological and research ~~sectorecosystem~~ (the “Agenda”);

(2) through the Agenda and the multiannual work programme, while avoiding any duplication of ~~efforts~~ activities with ENISA:

(i) defining priorities for its work on:

- ~~for its work on~~ the enhancement of cybersecurity research and innovation and its deployment,
- the development of cybersecurity industrial, technological and research capacities ~~and~~ capabilities, ~~skills~~ and infrastructure,
- the reinforcement of cybersecurity **industrial, technological and research skills and training and**
- the deployment of cybersecurity products and solutions, and

(ii) supporting cybersecurity industry, with a view to strengthening Union excellence, capacities and competitiveness on cybersecurity;

Commented [A8]: Great addition

- (3) ensuring synergies and cooperation ~~while avoiding duplication of activities~~ with relevant Union institutions, agencies and bodies such as ENISA ~~while avoiding any duplication of activities with such Union institutions, agencies and bodies;~~
- (4) coordinating National Coordination Centres through the Network and ensuring regular exchange of expertise;
- (5) providing expert **cybersecurity industrial, technological, and research** advice upon request from a Member State to that Member State;
- (6) facilitating collaboration and sharing of expertise among relevant stakeholders, in particular members of the **Cybersecurity Competence Community**; ~~this may include financially supporting education, training, exercises and building up cybersecurity skills;~~
- (7) facilitating the use of results from research and innovation projects in actions related to the development of cybersecurity products and solutions, seeking to avoid fragmentation and duplication of efforts and ~~to replicating~~ good cybersecurity practices and **cybersecurity** products and solutions, including those developed by **small and medium enterprises (SMEs)** and those based on open-source software; ~~Support to the deployment of cybersecurity products and solutions should to the extent possible rely on the European cybersecurity certification framework as defined by the Cybersecurity Act.~~
- (b) implementation tasks, consisting of:
- (1) coordinating ~~and administrating~~ the work of the Network and the Cybersecurity Competence Community in order to achieve the mission set out in Article 3, in particular supporting cybersecurity start-ups and SMEs in the ~~European~~ Union and facilitating their access to expertise, funding, investment and to markets;

Commented [A9]: It is unclear what kind of expert advice the Centre should be able to provide to Member States. "Cybersecurity industrial, technological, and research" has been added to delineate the tasks of the Centre from the tasks of ENISA and to align the text with recital 9c, 12 and article 3 in general.

- (2)** establishing and implementing the Centre's annual work programme, ~~by managing all the phases in the lifetime of the project,~~ in accordance with the Agenda and the multiannual work programme, for the cybersecurity parts of:
- (i) the Digital Europe programme ~~established by Regulation No XXX and in particular actions related to Article 6 of Regulation (EU) No XXX [Digital Europe Programme],~~
 - (ii) joint actions receiving support from the cybersecurity parts of the Horizon Europe programme ~~established by Regulation (EU) No XXX established by Regulation No XXX and in particular Section 2.2.6 of Pillar II of Annex I. of Decision No XXX on establishing the specific programme implementing Horizon Europe – the Framework Programme for Research and Innovation [ref. number of the Specific Programme], and in accordance with the multiannual strategic work programme of the Centre, and the strategic planning process of the Horizon Europe programme, and~~
 - (iii) other Union programmes when provided for in legal acts of the Union;
- (3)** providing expert advice on cyber security industry, technology, and research to the Commission when it prepares ~~its the draft annual work programmes pursuant to Article 11 of Council Decision (XXXX)⁶ of the Council on establishing the specific programme implementing Horizon Europe for other than joint actions in the area of cybersecurity research and innovation;~~

Commented [A10]: "Industry, technology, and research" has been added to delineate the tasks of the Centre from the tasks of ENISA and to align the text with recital 9c, 12 and article 3 in general.

⁶- Council Decision ..., of ..., on establishing the specific programme implementing Horizon Europe – the Framework Programme for Research and Innovation (OJ ...) [2018/0225(COD)].

GERMANY

- (9) ~~Taking into account that the objectives of this initiative can be best achieved if all Member States or as many Member States as possible participate, and as an incentive for Member States to take part, only Member States who contribute financially to the administrative and operational costs of the Competence Centre should hold voting rights.~~
- (10) ~~The participating Member States' financial participation should be commensurate to the Union's financial contribution to this initiative.~~
- (11) The ~~Competence~~ Centre should facilitate and ~~help~~-coordinate the work of the ~~Cybersecurity Competence~~ Network (~~“the Network”~~), which should be made up of National Coordination Centres, **one in from** each Member State. National Coordination Centres should receive direct Union financial support, including grants awarded without a call for proposals, in order to carry out **their** activities related to this Regulation.
- (12) National Coordination Centres should be **public sector entities, or entities with a majority of public participation, performing public administrative functions under national law, or upon general** including by means of delegation, **subject to public law obligations** and they should be selected by Member States. **The functions of a National Coordination Centre in a given Member State can be carried out by the same an entity that carries out also fulfilling other functions arising created under Union law, such as those of a national competent authority, and/or a single point of contact in the meaning of the NIS Directive (EU) 2016/1148 any other Union Regulation or a digital innovation hub in the meaning of the Digital Europe programme. Other public sector entities or entities performing public administrative functions in a Member State could assist the National Coordination Centre in that Member State, in carrying out its functions.**

Commented [A11]: Which rules will apply for grants without a call for proposal?

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

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

~~(18a) This Regulation should not utilise resources from Horizon Europe to fund projects which have a focus on military applications.~~

(18b) The enhancement of dual use application of cybersecurity technologies for cybersecurity purposes is without prejudice to the civilian nature of this Regulation and should therefore reflect specificities of Member States in cases when cybersecurity policy is pursued by civil-military or military authorities, and ensure complementarity but not overlap to the cyber defence related funding instruments.

(19) ~~In order to ensure structured and sustainable collaboration, the relation between the Competence Centre and the National Coordination Centres should be based on a contractual agreement.~~

(20) Appropriate provisions should be made to guarantee the liability and transparency of the ~~Competence Centre~~.

Commented [A12]: In contradiction to the “enhancement of dual use application of cybersecurity technologies for cybersecurity purposes is without prejudice...”, the use of “exclusive” implies deletion of para 18b, because it excludes all civilian technologies, which could potentially be used for military purposes as well

- (21) In view of its expertise in cybersecurity and its mandate as a reference point for advice and expertise on cybersecurity for Union institutions, agencies and bodies, as well as for relevant Union stakeholders, ~~as well as~~ **and in view of** its collection of input through its tasks, ~~for instance on cybersecurity certification and standardisation~~ the European Union **Agency** for Cybersecurity (**ENISA**) **as established by Regulation (EU) 2019/881 ("ENISA")** should play an active part in the activities of the Centre including the development of the Agenda, avoiding any duplication of their tasks in particular through its role as permanent observer in the Governing Board of the Centre (**"Governing Board"**). **Regarding the drafting of the Agenda, and the annual work programme and the multiannual work programme of the Centre, the Executive Director of the Centre ("Executive Director") and the Governing Board of the Centre should take into account any relevant strategic advice and input provided by ENISA, according to the rules of procedure within deadlines set by the Governing Board of the Centre.**
- (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 this ~~present initiative~~ **Regulation**.
- (23) ~~The Union contribution to the Competence Centre should finance half of the costs arising from the establishment, administrative and coordination activities of the Competence Centre. In order to avoid double funding, those activities should not benefit simultaneously from a contribution from other Union programmes.~~
- (24) The Governing Board **of the Competence Centre**, composed of **representatives from** the Member States and the Commission, should define the general direction of the ~~Competence~~ Centre's operations, and ensure that **the Centre** ~~it~~ carries out its tasks in accordance with this Regulation. **The Governing Board should adopt the Agenda consisting of strategic goals that have to be fulfilled by the Centre.**

Commented [A13]: It makes sense that ENISA's "input" will also be taken into account.

HAVE ADOPTED THIS REGULATION:

CHAPTER I

GENERAL PROVISIONS AND PRINCIPLES OF THE COMPETENCE CENTRE AND THE NETWORK

Article 1

Subject matter

1. This Regulation establishes the European Cybersecurity Industrial, Technology and Research Competence Centre (the ‘Competence Centre’), as well as the Network of National Coordination Centres (the “Network”), and lays down rules for the nomination of National Coordination Centres, as well as for the establishment of the Cybersecurity Competence Community (the “Community”).
2. The Competence Centre shall contribute have an important role in to the implementation of the cybersecurity part of the Digital Europe programme established by Regulation No XXX and in particular actions related to Article 6 of Regulation (EU) No XXX [Digital Europe Programme] thereof and of the Horizon Europe programme established by Regulation No XXX and in particular Section 2.2.6 of Pillar II of Annex I. of Decision No XXX on establishing the specific programme implementing Horizon Europe – the Framework Programme for Research and Innovation [ref. number of the Specific Programme].
3. The seat of the Competence Centre shall be located in [XXXBrussels, Belgium].

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.

4a The seat of the Competence Centre shall be located in [XXXBrussels, Belgium].

5. **This Regulation is without prejudice to the competences of the Member States regarding activities concerning public security, defence, national security and the activities of the state in areas of criminal law.**

Commented [A14]: Is Art. 1(4a) in accordance with recital 7a. When will the seat be decided by the governments of the MS? Will the method be discussed in COREPER?
See also our detailed questions sent last Friday via e-mail!

Article 2

Definitions

For the purpose of this Regulation, the following definitions ~~shall~~ apply:

- (1) 'cybersecurity' means ~~the protection~~ **the activities necessary to protect** network and information systems, ~~the-users~~ **of such systems**, and other persons **affected by** ~~against~~ cyber threats;
- (1a) **'network and information system' means a network and information system as defined in point (1) of Article 4 of Directive (EU) 2016/1148;**
- (2) 'cybersecurity products and solutions' means ICT products, services or processes with the specific purpose of protecting network and information systems, ~~their~~ users **of such systems** and ~~other affected~~ persons **affected by** ~~from~~ cyber threats;
- (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;~~

Article 4a

Tasks of the Centre

1. In order to fulfill the mission laid out in Article 3 and the objectives laid out in Article 4, the Centre shall, in close cooperation with the Network, have the following ~~strategic and implementation~~ tasks:
 - (a) strategic tasks, consisting of:
 - (1) developing and monitoring the implementation of a comprehensive and sustainable Cybersecurity Industrial, Technology and Research Agenda, which ~~will~~ shall set out strategic recommendations and goals for the development and growth of the European cybersecurity industrial, technological and research ~~sectorecosystem~~ (the “Agenda”);
 - (2) through the Agenda and the multiannual work programme, while avoiding any duplication of ~~efforts~~ activities with ENISA:
 - (i) defining priorities for its work on:
 - ~~for its work on~~ the enhancement of cybersecurity research and innovation and its deployment,
 - the development of cybersecurity industrial, technological and research capacities ~~and~~ capabilities, ~~skills~~ and infrastructure,
 - the reinforcement of cybersecurity **industrial, technological and research** skills and training and
 - the deployment of cybersecurity products and solutions, and
 - (ii) supporting cybersecurity industry, with a view to strengthening Union excellence, capacities and competitiveness on cybersecurity;

- (3)** ensuring synergies and cooperation ~~while avoiding duplication of activities~~ with relevant Union institutions, agencies and bodies such as ENISA ~~while avoiding any duplication of activities with such Union institutions, agencies and bodies;~~
- (4)** coordinating National Coordination Centres through the Network and ensuring regular exchange of expertise;
- (5)** ~~providing expert advice upon request from a Member State to that Member State;~~
- (6)** facilitating collaboration and sharing of expertise among relevant stakeholders, in particular members of the **Cybersecurity Competence Community**; ~~this may include financially supporting education, training, exercises and building up cybersecurity skills;~~
- (7)** facilitating the use of results from research and innovation projects in actions related to the development of cybersecurity products and solutions, seeking to avoid fragmentation and duplication of efforts and ~~to replicating~~ good cybersecurity practices and **cybersecurity** products and solutions, including those developed by **small and medium enterprises (SMEs)** and those based on open-source software; ~~Support to the deployment of cybersecurity products and solutions should to the extent possible rely on the European cybersecurity certification framework as defined by the Cybersecurity Act.~~

(b) implementation tasks, consisting of:

- (1)** ~~coordinating and administering~~ the work of the Network and the Cybersecurity Competence Community in order to achieve the mission set out in Article 3, in particular supporting cybersecurity start-ups and SMEs in the ~~European~~ Union and facilitating their access to expertise, funding, investment and to markets;

Commented [A15]: Would „coordinating“ not be sufficient? What is the added value of including „administering“?

Article 7

Tasks of the National Coordination Centres

1. The National Coordination Centres shall have the following tasks:

- (a) **acting as contact points at the national level for the Cybersecurity Competence Community** to supporting the Competence Centre in achieving its objective and missions, and in particular in coordinating the Cybersecurity Competence Community **through the coordination of its national members;**
- (aa) **providing expertise and actively contributing to the strategic planning of the activities according to tasks referred to in Article 4a, taking into account relevant national and regional challenges for cybersecurity in different sectors;**
- (b) facilitating the participation of industry, **research institutions** and other actors at the Member State level in cross-border projects;
- ~~e) contributing, together with the Competence Centre, to identifying and addressing sector specific cyber security industrial challenges;~~
- ~~d) acting as contact point at the national level for the Cybersecurity Competence Community and the Competence Centre;~~
- (e) seeking to establish synergies with relevant activities at the national and regional level, **such as including national policies on research, development and innovation in the area of cybersecurity, and in particular those policies stated in the national cybersecurity strategies;**
- (f) implementing specific actions for which grants have been awarded by the Competence Centre, including through provision of financial support to third parties in **line accordance** with Article 204 of Regulation **(EU, Euratom) 2018/1046** under conditions specified in the ~~concerned~~ grant agreements **concerned;**

- (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;
- (h) assessing requests by entities established in the same Member State as the **National** Coordination Centre for becoming part of the Cybersecurity Competence Community;
- (i) **advocating and promoting involvement by relevant entities in the activities arising from the Centre, Network and Community, and monitoring, as appropriate, the level of engagement with and grant actions awarded for cybersecurity research, developments and deployments, with particular reference to the entities regulated under Directive (EU) 2016/1148.**
2. For the purposes of point (f) of **paragraph 1 of this Article**, the financial support to third parties may be provided in any of the forms specified in Article 125 of Regulation (EU, Euratom) 2018/1046~~XXX [new Financial Regulation]~~, including in the form of lump sums.

Commented [A16]: Why was this deleted?

Article 15

Voting rules of the Governing Board

- 1. A vote shall be held if the members of the Governing Board failed to achieve consensus.
- 2. The Governing Board shall take its decisions by a majority of at least 75% of all its members, **with voting rights, the representatives of the Commission constituting a single member for this purpose**. An absent member of the Governing Board may delegate his or her vote to his or her alternate or, in the absence of his or her alternate, to another member. Any member of the Governing Board may represent not more than one other member. **[For decisions related to the usage of Union funds in Article 13(3) except point (cb), the Union should hold 50% of the voting rights].**
- 2a. For decisions related to the task laid down in point (cb) of Article 13(3), contributing Member States and the Commission shall ~~hold~~ votes in a manner that is proportional to their relevant contribution on a specific joint action in line with the methodology adopted pursuant to point (s) of Article 13(3).
 - 1. ~~For any other decisions other than those referred to in paragraph -2a, every~~ each Member States and the Union shall hold 50 % of the voting rights shall have one vote. The vote ~~ing rights~~ of the Union shall be **indivisible cast jointly by the two representatives of the Commission** ~~[or unanimous]~~.
 - ~~2. Every participating Member State shall hold one vote.~~
 - ~~3. The Governing Board shall take its decisions by a majority of at least 75% of all votes, including the votes of the members who are absent, representing at least 75% of the total financial contributions to the Competence Centre. The financial contribution will be calculated based on the estimated expenditures proposed by the Member States referred to in point c of Article 17(2) and based on the report on the value of the contributions of the participating Member States referred to in Article 22(5).~~

Commented [A17]: It has to be ensured that COM only holds 50% of the voting rights in those exceptional cases.

CHAPTER III

FINANCIAL PROVISIONS

Article 21

Union and Member States' financial contribution

-1. The Centre shall be funded by the Union.

1. The Union's contribution to the ~~Competence~~ Centre to cover administrative costs and operational costs shall comprise the following:
 - a) [EUR 1 981 668 000] from the Digital Europe programme, including up to [EUR 23 746 000] for administrative costs;
 - b) an amount from the Horizon Europe programme, including for administrative costs, **for joint actions, which shall be equal to the amount contributed voluntary** ~~voluntary by Member States pursuant to paragraph 5 of this Article 21(5) and but not exceed [the amount determined in the strategic planning process of the Horizon Europe programme] to be determined by taking into account the strategic planning process~~ to be carried out pursuant to Article 6(6) of Regulation XXX [Horizon Europe Regulation] **and the multiannual work programme and the annual work programmes of the Centre.**
2. The maximum Union contribution shall be paid from the appropriations in the general budget of the Union allocated to [Digital Europe Programme] and to the specific programme implementing Horizon Europe, established by Decision XXX.
3. The ~~Competence~~ Centre shall implement cybersecurity actions of [Digital Europe Programme] and [Horizon Europe Programme] in accordance with point (c)(iv) **of the first subparagraph** of Article 62 **(1)** of Regulation (EU, Euratom) ~~XXX²³ [the Financial Regulation] 2018/1046.~~

Commented [A18]: Why was "voluntary" deleted here?
Is the reference to paragraph 5 here sufficient to ensure that MS only voluntarily participate financially in joint actions.

Article 38

Monitoring, evaluation and review

1. The ~~Competence~~ Centre shall ensure that its activities, including those managed through the National Coordination Centres and the Network, shall be subject to continuous and systematic monitoring and periodic evaluation. The ~~Competence~~ Centre shall ensure that the data for monitoring programme implementation and results are collected efficiently, effectively, and in a timely manner and proportionate reporting requirements shall be imposed on recipients of Union funds and Member States. The ~~outcomes~~ **conclusions** of that evaluation shall be made public.
2. Once there is sufficient information available about the implementation of this Regulation, but no later than ~~two three and a half~~ years **the date referred to in Article 45 paragraph 4 of this Regulation** ~~after the start of the implementation of this Regulation,~~ the Commission shall carry out an interim evaluation of the ~~Competence~~ Centre **on the basis of terms of reference agreed with the Governing Board.** The Commission shall prepare a report on that evaluation and shall submit that report to the European Parliament and to the Council by 31 **July 2023.** ~~December 2024.~~ The ~~Competence~~ Centre and Member States shall provide the Commission with the information necessary for the preparation of that report.
3. The evaluation referred to in paragraph 2 shall include:
 - (a) an assessment of the working capacity of the Centre regarding objectives, mandate and tasks and the cooperation and coordination with other relevant actors, particularly National Coordination Centres, the **Cybersecurity Competence** Community and ENISA;
 - (b) an assessment of the results achieved by the ~~Competence~~ Centre, having regard to its **mission**, objectives, mandate and tasks, **and in particular the efficiency of the Centre in coordinating Union funds and pooling expertise;**

Commented [A19]: The criteria for the evaluation shall be defined by the governing board. The final evaluation has to be developed in accordance with the governing board.

(c) an assessment of the coherence of implementation tasks in accordance with the Agenda and the multiannual work programme ~~of the Centre~~;

(d) an assessment of the coordination and cooperation of the Centre with the Program Committee of the Horizon Europe programme and the Digital Europe programme, especially **with a view to increasing** coherence and synergy with the strategic planning of the Centre, ~~the~~ Horizon Europe programme and ~~the~~ Digital Europe programme;

(e) an assessment on joint actions;

(f) an assessment to determine whether the duration of the Centre should be extended beyond the period specified in Article 46(1). ~~That~~ assessment shall include legal and administrative considerations whether the mandate of the Centre could be transferred to a different Union body to create synergies and reduce fragmentation.

If the Commission considers that the continuation of the ~~Competence~~ Centre is justified with regard to its assigned objectives, mandate and tasks, it may propose that the duration of the mandate of the ~~Competence~~ Centre set out in Article 46 be extended. The Council and European Parliament have to decide upon the continuation of the Centre.

Commented [A20]: An assessment of the duration of the Centre (8year duration) after only 2 years is not feasible.

Commented [A21]: Council and EP have to decide on the continuation of the Centre.

4. On the basis of the conclusions of the interim evaluation referred to in paragraph 2, the Commission may ~~act in accordance with [Article 22(54)] or~~ take any other appropriate actions.
5. The monitoring, evaluation, phasing out and renewal of the contribution from Horizon Europe will follow the provisions of Articles 8, 45 and 47 and ~~Annex III~~ of the Horizon Europe Regulation and agreed implementation ~~modalities~~ arrangements.

ESTONIA

- (8a) The ~~Competence~~ Centre **would** benefit from the ~~particular expertise~~ experience and the broad and relevant stakeholders' representation built through the contractual public-private partnership on cybersecurity between the Commission and European Cyber Security Organisation ECSO Association during the duration of the Framework Programme for Research and Innovation (2014-2020) ("Horizon 2020"), established by Regulation (EU) No 1291/2013 of the European Parliament and of the Council⁷, and the lessons learned from four pilot projects⁸ launched in early 2019 under Horizon 2020, **thereby building on the existing experience that has been set up by the contractual public-private partnership on cybersecurity**, for the management of the Cybersecurity Competence Community, and the representation of the Cybersecurity Competence Community in the Centre.
- (9) The Centre should develop and monitor the implementation of a comprehensive and sustainable Cybersecurity Industrial, Technology and Research Agenda ~~Strategy~~ which will set out strategic recommendations and priorities for development and growth of the European cybersecurity **ecosystem industrial, technological and research sector** (the "Agenda"). The Agenda **should provide the basis for the annual and multi-annual work programme of the Centre**. Furthermore, the Agenda should be taken duly into account in particular within the ~~bi-annual and annual~~ planning and implementation of the Horizon Europe programme and the Digital Europe programme in the area of cybersecurity. The Agenda **could also serve** ~~be able to provide as~~ cybersecurity specific advice, where relevant, **for** the implementation of other Union programmes.

Commented [A22]: EE: As the reference for Horizon Europe is already made in the recital 9b, we propose deleting it from this recital.

⁷ Regulation (EU) No 1291/2013 of the European Parliament and of the Council of 11 December 2013 establishing Horizon 2020 - the Framework Programme for Research and Innovation (2014-2020) and repealing Decision No 1982/2006/EC (OJ L 347, 20.12.2013, p. 104).

⁸ CONCORDIA, ECHO, SPARTA and CyberSec4Europe are the four winning pilot projects of the 2018 Horizon 2020 cybersecurity call "establishing and operating a pilot for a European Cybersecurity Competence Network and developing a common European Cybersecurity Research & Innovation Roadmap".

- (9a) When the Centre is preparing its annual work programme ("annual work programme"), it should inform the Commission on its co-funding needs based on the Member States' planned co-funding contributions to joint actions, in order for the Commission to take into account the Union matching contribution in the preparation of the draft general budget for the following year.
- (9b) Where the Commission prepares the ~~Horizon Europe W~~ work programme of the ~~Horizon Europe~~ programme for matters related to cyber security, including in the context of its stakeholder consultation process and particularly before the adoption of that work programme, the Commission should take into due account the input of the ~~Centre Governing Board and Executive Director~~ and share its such input with the ~~Horizon Europe~~ Programme Committee of the Horizon Europe programme.
- (9c) In order to support its role in the area of cybersecurity and the involvement of the Network and to provide a strong governance role for the Member States of National Coordination Centres, the Centre should be established as a Union body with legal personality. ~~To achieve its role, it should manage funding.~~ The Centre should perform a dual role by undertaking specific tasks in the area of cybersecurity industry, technology and research as laid down in Art 4 and 4a this Regulation and by managing cybersecurity related funding from several programmes at the same time – notably the Horizon Europe programme and the Digital Europe programme, and possibly even further Union programmes. Such management should be in line accordance with their regulations rules applicable to those programmes. ~~The Centre will therefore have a special nature~~ Nevertheless, considering that the funding for the functioning of the Centre would originate primarily from the ~~{DEP}~~ Digital Europe programme and the ~~{Horizon Europe}~~ funding programmes and in view of the absence of appropriate funding alternatives in those funding programmes, it is necessary that the Centre is considered as a partnership for the purpose of budget implementation, including the programming phase.

Commented [A23]: EE: As the necessary minimum requirements for Horizon partnership are not defined for the Centre (ie. the Centre does not possess rights for deciding for all calls and projects in the area of cyber security, since those are decided in the Horizon framework/strategic planning), it cannot be considered as a partnership. How the financing from Horizon for the activities of the Centre would be synchronised with the financing for projects already decided in the Horizon strategic planning?

- (9) Taking into account that the objectives of this initiative can be best achieved if all Member States or as many Member States as possible participate, and as an incentive for Member States to take part, only Member States who contribute financially to the administrative and operational costs of the Competence Centre should hold voting rights.
- (10) The participating Member States' financial participation should be commensurate to the Union's financial contribution to this initiative.
- (11) The Competence Centre should facilitate and help coordinate the work of the **Cybersecurity Competence Network ("the Network")**, which should be made up of National Coordination Centres, **one in from** each Member State. National Coordination Centres should receive direct Union financial support, including grants awarded without a call for proposals, in order to carry out **their** activities related to this Regulation.
- (12) National Coordination Centres should be **public sector entities, or entities with a majority of public participation, performing public administrative functions under national law, or upon general** including by means of delegation, **subject to public law obligations** and they should be selected by Member States. **The functions of a National Coordination Centre in a given Member State can be carried out by the same an entity that carries out also fulfilling other functions arising created under Union law, such as those of a national competent authority, and/or a single point of contact in the meaning of the NIS Directive (EU) 2016/1148 any other Union Regulation or a digital innovation hub in the meaning of the Digital Europe programme. Other public sector entities or entities performing public administrative functions in a Member State could assist the National Coordination Centre in that Member State, in carrying out its functions.**

Commented [A24]: EE: According to our understanding this is not allowed in Horizon Europe. Could the COM or CLS clarify this?

- (15) The Competence Centre should have several key functions. First, the Competence Centre should facilitate and help coordinate the work of the European Cybersecurity Competence Network and nurture support the Cybersecurity Competence Community. The Centre should drive implement cybersecurity relevant parts of the Digital Europe programme and the Horizon Europe programme in accordance with its the Centre's multiannual work programme ("multiannual work programme") and the annual strategic work programme and the strategic planning process of the Horizon Europe programme by allocating grants, typically following a competitive call for proposals the cybersecurity technological agenda in accordance with its multiannual work programme, and facilitate transfer of access to the expertise gathered in the Network and the Cybersecurity Competence Community and . Secondly, it should implement relevant parts of Digital Europe and Horizon Europe programmes by allocating grants, typically following a competitive call for proposals. Thirdly, the Competence Centre should facilitate support joint investment by the Union, Member States and/or industry.
- (16) The Competence Centre and the National Coordination Centres should stimulate and support the cooperation and coordination of the activities of the Cybersecurity Competence Community, which would involve a large, open, and diverse group of actors involved in cybersecurity technology. That Community should include in particular research entities, supply-side industries, demand-side industries, civil society groups in the area of cybersecurity and the public sector. The Cybersecurity Competence Community should provide input to the activities and multiannual work programme and the annual work programme of the Competence Centre and it should also benefit from the community-building activities of the Competence Centre and the Network, but otherwise should not be privileged with regard to calls for proposals or calls for tender.

Commented [A25]: EE: This should go without prejudice to the open calls for scientists and enterprises, who are not connected to the activities of the Centre and conduct research activities related to cyber.

HAVE ADOPTED THIS REGULATION:

CHAPTER I

GENERAL PROVISIONS AND PRINCIPLES OF THE COMPETENCE CENTRE AND THE NETWORK

Article 1

Subject matter

1. This Regulation establishes the European Cybersecurity Industrial, Technology and Research ~~Competence~~ Centre (the ‘~~Competence~~-Centre’), as well as the Network of National Coordination Centres (the “Network”), and lays down rules for the nomination of National Coordination Centres, as well as for the establishment of the Cybersecurity Competence Community (the “Community”).
2. The ~~Competence~~ Centre shall **contribute have an important role in** to the implementation of the cybersecurity part of the Digital Europe programme **established by Regulation No XXX** and in particular actions related to Article 6 of Regulation (EU) No XXX [Digital Europe Programme] **thereof** and of the Horizon Europe programme **established by Regulation No XXX** and in particular Section 2.2.6 of Pillar II of Annex I of Decision No XXX on establishing the specific programme implementing Horizon Europe – the Framework Programme for Research and Innovation [ref. number of the Specific Programme].
3. **The seat of the Competence Centre shall be located in [XXXBrussels, Belgium].**

Commented [A26]: EE: New reference should be added, which is now in the Horizon regulation Section 3.1.3.
https://www.europarl.europa.eu/doceo/document/TA-8-2019-0396_EN.html#title2

- (4) ~~participating Member State contributing Member State~~ means a Member State which voluntarily contributes financially to the administrative and operational costs of the Competence Centre.
- (3) **"joint actions"** means an actions included in the **Centre's annual work programme** receiving Union financial support from the Horizon Europe programme and/or Digital Europe programme, as well as financial or in-kind support by one or more Member States, ~~to be~~ which are implemented via projects involving beneficiaries established in the Member States which provide financial or in-kind support to those beneficiaries ~~entities~~ stemming from those Member States.
- (4) **"in-kind contribution by Member States"** means those eligible costs, incurred by National Coordination Centres and other public entities when participating in projects funded through this Regulation, which are not financed by a Union contribution. ~~In the case of projects funded through Horizon Europe, eligible costs shall be calculated in line with Article 32 of the Regulation establishing Horizon Europe. In the case of projects funded through Digital Europe, eligible costs shall be calculated in line with the Financial Regulation.⁹~~

Commented [A27]: EE: we should bear in mind the Horizon conditions that a consortium for joint actions requires the participation of more than one Member State. Furthermore, Associated countries are also involved in Horizon activities. See article 18 https://www.europarl.europa.eu/doceo/document/TA-8-2019-0395_EN.html#title2

Article 3

Mission of the Competence Centre and the Network

1. The ~~Competence~~ Centre and the Network shall help the Union to:
 - (a) retain and develop, **in an autonomous manner, the Union's the** cybersecurity **research**, technological and industrial capacities **and capabilities** necessary to **strengthen trust and security in secure** the Digital Single Market;
 - (b) increase the **global** competitiveness of the Union's cybersecurity industry and turn cybersecurity into a competitive advantage of other Union industries.

⁹ **Reference to the Financial Regulation and other legislative acts.**

Article 4a

Tasks of the Centre

1. In order to fulfill the mission laid out in Article 3 and the objectives laid out in Article 4, the Centre shall, in close cooperation with the Network, have the following ~~strategic and implementation~~ tasks:

(a) strategic tasks, consisting of:

(1) developing and monitoring the implementation of a comprehensive and sustainable Cybersecurity Industrial, Technology and Research Agenda, which ~~will~~ shall set out strategic recommendations and goals for the development and growth of the European cybersecurity industrial, technological and research ~~sectorecosystem~~ (the “Agenda”);

(2) through the Agenda and the multiannual work programme, while avoiding any duplication of ~~efforts~~ activities with ENISA:

(i) defining priorities for its work on:

- ~~for its work on~~ the enhancement of cybersecurity research and innovation and its deployment,
- the development of cybersecurity industrial, technological and research capacities ~~and~~ capabilities, ~~skills~~ and infrastructure,
- the reinforcement of cybersecurity **industrial, technological and research** skills and training and
- the deployment of cybersecurity products and solutions, and

(ii) supporting cybersecurity industry, with a view to strengthening Union excellence, capacities and competitiveness on cybersecurity;

- (3)** ensuring synergies and cooperation ~~while avoiding duplication of activities~~ with relevant Union institutions, agencies and bodies such as ENISA ~~while avoiding any duplication of activities with such Union institutions, agencies and bodies;~~
- (4)** coordinating National Coordination Centres through the Network and ensuring regular exchange of expertise;
- (5)** ~~providing expert advice upon request from a Member State to that Member State;~~
- (6)** facilitating collaboration and sharing of expertise among relevant stakeholders, in particular members of the **Cybersecurity Competence Community**; ~~this may include financially supporting education, training, exercises and building up cybersecurity skills;~~
- (7)** facilitating the use of results from research and innovation projects in actions related to the development of cybersecurity products and solutions, seeking to avoid fragmentation and duplication of efforts and ~~to replicating~~ good cybersecurity practices and **cybersecurity** products and solutions, including those developed by **small and medium enterprises (SMEs)** and those based on open-source software; ~~Support to the deployment of cybersecurity products and solutions should to the extent possible rely on the European cybersecurity certification framework as defined by the Cybersecurity Act.~~
- (b)** implementation tasks, consisting of:
- (1)** coordinating ~~and administrating~~ the work of the Network and the **Cybersecurity Competence Community** in order to achieve the mission set out in Article 3, in particular supporting cybersecurity start-ups and SMEs in the ~~European~~ Union and facilitating their access to expertise, funding, investment and to markets;

Commented [A28]: EE: We should not limit it to providing advice to a single Member State. We would propose a new wording: "providing expert advice upon request through the Network".

- (2)** establishing and implementing the Centre's annual work programme, ~~by managing all the phases in the lifetime of the project,~~ in accordance with the Agenda and the multiannual work programme, for the cybersecurity parts of:
- (i) the Digital Europe programme ~~established by Regulation No XXX and in particular actions related to Article 6 of Regulation (EU) No XXX [Digital Europe Programme],~~
 - (ii) joint actions receiving support from the cybersecurity parts of the Horizon Europe programme ~~established by Regulation (EU) No XXX established by Regulation No XXX and in particular Section 2.2.6 of Pillar II of Annex I. of Decision No XXX on establishing the specific programme implementing Horizon Europe – the Framework Programme for Research and Innovation [ref. number of the Specific Programme], and in accordance with the multiannual strategic work programme of the Centre, and the strategic planning process of the Horizon Europe programme, and~~
 - (iii) other Union programmes when provided for in legal acts of the Union;
- (3)** providing expert advice on cyber security to the Commission when it prepares ~~its the~~ draft ~~annual~~ work programmes pursuant to Article 11 of Council Decision (XXXX)¹⁰ ~~of the Council on establishing the specific programme implementing Horizon Europe for other than joint actions in the area of cybersecurity research and innovation;~~

Commented [A29]: EE: As the recital 15, this should go without prejudice to the open calls for scientists and enterprises, who are not connected to the activities of the Centre and conduct research activities related to cyber. It should furthermore be in line with the strategic planning process of the Horizon Europe programme.

¹⁰ Council Decision ..., of ..., on establishing the specific programme implementing Horizon Europe – the Framework Programme for Research and Innovation (OJ ...) [2018/0225(COD)].

Article 8

The Cybersecurity Competence Community

1. The Cybersecurity Competence Community shall contribute to the mission of the ~~Competence Centre~~ **and the Network** as laid down in Article 3 and enhance and disseminate cybersecurity expertise across the Union.
2. The Cybersecurity Competence Community shall, **on the one hand**, consist of industry, academic and non-profit research organisations, **other relevant civil society** ~~and~~ associations as well as public entities and other entities dealing with **cybersecurity** operational and technical matters **and, on the other hand, where relevant, actors of sectors having an interest in cybersecurity and facing cybersecurity challenges**. It shall bring together the main stakeholders with regard to cybersecurity **research**, technological and industrial capacities in the Union. It shall involve National Coordination Centres as well as Union institutions and bodies with relevant expertise, **such as ENISA**.

3. Only entities which are established within the Union may be ~~accredited~~ **registered** as members of the Cybersecurity Competence Community. They shall demonstrate that they **can contribute to the missions as set out in Article 3 and shall** have cybersecurity expertise with regard to at least one of the following domains:
- (a) research **and innovation**;
 - (b) industrial **or product** development;
 - (c) training and education;
 - (d) **information security and/or incident response operations**;
 - (e) **scientific or technical partnerships or cooperation with academic and/or public authorities as defined under Article 2(3).**

~~Furthermore they should comply with the relevant national security regulations.~~

4. The ~~Competence~~ Centre shall ~~accredit~~ **register** 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, **including an assessment on security grounds**, of whether that entity meets the criteria provided for in paragraph 3 of this Article. **That assessment shall also take into account, where relevant, any national assessment on security grounds made by the national competent authorities.** ~~An registration accreditation~~ shall not be limited in time but may be revoked by the ~~Competence~~ Centre at any time if ~~the Centre it~~ or the relevant National Coordination Centre considers that the entity does not fulfil the criteria set out in paragraph 3 of this Article or ~~it~~ falls under the relevant provisions set out in Article 136 of Regulation **(EU, Euratom) 2018/1046XXX [new financial regulation]**, or for justified security reasons.

Commented [A30]: EE: If the National Coordination Centre decides who should be part of the Community, they should decide who needs to leave the Community. It should not be the decision of the Centre.

Article 13

Tasks of the Governing Board

1. The Governing Board shall have the overall responsibility for the strategic orientation and the operations of the ~~Competence Centre~~, and shall supervise the implementation of its activities **and shall be responsible for any task that is not specifically allocated to the Executive Director.**
2. The Governing Board shall adopt its rules of procedure. Those rules shall include specific procedures for identifying and avoiding conflicts of interest and ensure the confidentiality of any sensitive information.
3. The Governing Board shall take the necessary strategic decisions, in particular:
 - (a) **develop and adopt the Agenda encompassing strategic goals and priorities for a sustainable development of the European cybersecurity research, technological and industrial sector and monitor its implementation;**
 - (aa) **based on the Agenda, adopt the multiannual work programme, containing the development of a common, industrial, technology and research strategic priorities roadmap, which are based on the basis of the needs identified by Member States in cooperation with the Cybersecurity Competence Community and which require the focus of Union's financial support. Such priorities shall include key technologies and domains for developing the Union's own capabilities in cybersecurity strategic autonomy; a statement of the major priorities and planned initiatives of the Competence Centre, including an estimate of financing needs and sources;**

- (aaa) adopt the annual work ~~plan~~ programme for implementing the relevant Union funds, notably the cybersecurity parts of the Horizon Europe **programme** and **the** Digital Europe programme, in accordance with the Centre's multi annual work programme and the strategic planning process of **the** Horizon Europe **programme** including an estimation of ~~thee~~ of financing needs and sources; Where appropriate, proposals and in particular the annual work programme shall assess the need to apply security rules as set out in Article 34 of this Regulation, including in particular the security self-assessment procedure in accordance with Article 16 of the [XXXX Horizon Europe Regulation];
- (b) adopt the ~~Competence~~ Centre's ~~work plan~~, annual accounts and balance sheet and annual activity report, on the basis of a proposal from the Executive Director;
- (c) adopt the specific financial rules of the ~~Competence~~ Centre in accordance with [Article 70 of **Regulation (EU, Euratom) 2018/1046 the —FRFinancial Regulation**];
- (ca) ~~in the line with the Centre's~~ as part of the **Centre's annual work programme** adopt decisions ~~to dedicate~~ allocate funds from the Union budget to joint actions between the Union and Member States;
- (cb) as part of the annual work programme and in accordance with the decisions referred to in point (ca) ~~of this paragraph~~, and without prejudice to the regulations establishing Horizon Europe and the Digital Europe Programme, adopt decisions relating to the description the joint actions referred to in point (ca) and lay down conditions for their implementation;
- (d) adopt a procedure for appointing the Executive Director;

Commented [A31]: EE: There is a slight discrepancy here, as if the actions are carried out with the means from the Horizon Europe programme and its regulation, how then the Governing Board can lay down conditions for their implementation?

Article 14

Chairperson and Meetings of the Governing Board

1. The Governing Board shall elect a Chairperson and a Deputy Chairperson from among the ~~its members with voting rights~~, for a period of ~~two~~ **three** years. The mandate of the Chairperson and the Deputy Chairperson may be extended once, following a decision by the Governing Board. If, however, their membership of the Governing Board ends at any time during their term of office, their term of office shall automatically expire on that date. The Deputy Chairperson shall *ex officio* replace the Chairperson if the latter is unable to attend to his or her duties. The Chairperson shall take part in the voting.
2. The Governing Board shall hold its ordinary meetings at least three times a year. It may hold extraordinary meetings at the request of the Commission, at the request of one third of all its members, at the request of the **Chairperson**, or at the request of the Executive Director in the fulfilment of his/her tasks.
3. The Executive Director shall take part in the deliberations, unless decided otherwise by the Governing Board, but shall have no voting rights.

- 3a. The Governing Board may invite, on a case-by-case basis, other persons to attend its meetings as observers, including additional representatives of the Commission, for ensuring coordination and synergies between different Union activities involving cybersecurity.
4. **Representatives of the Cybersecurity Competence Community** ~~Members of the Industrial and Scientific Advisory Board~~ may take part, upon invitation from the Chairperson, in the meetings of the Governing Board, without voting rights.
5. The members of the Governing Board and their alternates may, subject to its rules of procedure, be assisted at the meetings by advisers or experts.
6. The ~~Competence~~ Centre shall provide the secretariat for the Governing Board.

Article 15

Voting rules of the Governing Board

- 1. A vote shall be held if the members of the Governing Board failed to achieve consensus.
- 2. The Governing Board shall take its decisions by a majority of at least 75% of all its members, **with voting rights, the representatives of the Commission constituting a single member for this purpose.** An absent member of the Governing Board may delegate his or her vote to his or her alternate or, in the absence of his or her alternate, to another member. Any member of the Governing Board may represent not more than one other member. **[For decisions related to the usage of Union funds in Article 13(3) except point (cb), the Union should hold 50% of the voting rights].**

Commented [A32]: EE: We do not support this addition.

CHAPTER III

FINANCIAL PROVISIONS

Article 21

Union and Member States' financial contribution

-1. The Centre shall be funded by the Union.

1. The Union's contribution to the ~~Competence~~ Centre to cover administrative costs and operational costs shall comprise the following:
 - a) [EUR 1 981 668 000] from the Digital Europe programme, including up to [EUR 23 746 000] for administrative costs;
 - b) an amount from the Horizon Europe programme, including for administrative costs, **for joint actions, which shall be equal to the amount contributed voluntary by Member States pursuant to paragraph 5 of this Article 21(5) and but not exceed [the amount determined in the strategic planning process of the Horizon Europe programme]** ~~to be determined by taking into account the strategic planning process~~ to be carried out pursuant to Article 6(6) of Regulation XXX [Horizon Europe Regulation] **and the multiannual work programme and the annual work programmes of the Centre.**
2. The maximum Union contribution shall be paid from the appropriations in the general budget of the Union allocated to [Digital Europe Programme] and to the specific programme implementing Horizon Europe, established by Decision XXX.
3. The ~~Competence~~ Centre shall implement cybersecurity actions of [Digital Europe Programme] and [Horizon Europe Programme] in accordance with point (c)(iv) **of the first subparagraph** of Article 62 **(1)** of Regulation (EU, Euratom) ~~XXX²³ [the Financial Regulation] 2018/1046.~~

Commented [A33]: EE: According to our understanding the strategic planning for HE is close to being finalised and there is no specific amount allocated to the Centre. How does this affect this para?

IRELAND

Third Country Engagement

A global approach to cybersecurity technological and industrial development, thereby maximising the opportunities for European firms globally, rather than solely the Internal Market, which constitutes approx. only 20% of the world marketplace.

The consequent need for reciprocity in regard to market access for European cybersecurity products and services.

The need for continued operational cooperation on cybersecurity with third countries in the interests of national and public security of the Member States.

Firstly the Irish proposal argues for international cooperation between not only the Centre but more importantly the Network and the Cybersecurity Competence Community.

- The Community consists of cybersecurity professionals. For the Community to be truly competent it has to be outward focused and engaging with likeminded entities in the rest of the world. International agreements would be necessary to underpin positive relationships with third country firms in Europe. For example if Member States wanted US companies to be involved in collaborative activities such as awareness raising, skills development and on cyber education then there needs to be provision for such international cooperation.
- It should also be possible for association agreements with third countries to be in place for their designated National Coordination Centres to engage with the EU Network of National Coordination Centres as guests or observers for example. There needs to be space for not only dialogue by also joint or parallel initiatives between EU Member States and specified third countries. For example if the National Coordination Centre of Switzerland wishes to have some interaction, potentially attending some meetings, with the Network of National Coordination Centres there would have to be provision for such international cooperation.
- The role of the Centre would be in regard to mere facilitation and administration of any international agreement. The primary actors would be both the Network and Cybersecurity Competence Community.

Secondly, the Irish proposal is about **legal provision** for international agreements with third countries. Whether international agreements and their scope with specified third countries take place is a subsequent political decision for Member States to make. The Irish argument is about having the enabling power in law for such agreements. Article 13 of the NIS Directive (2016/1148) has such a provision for third country involvement with the NIS Cooperation Group. We know that third countries such as Norway and accession candidates in the Western Balkans have sought such involvement and Article 13 provided the enabling legal power. Why therefore is such provision not in the current draft legislative text?

Thirdly there is a need for the legislation to make provision for international agreements as otherwise EU technological sovereignty could be perceived as not only inward, insular and protectionist but even hostile by others. As the European Union does not yet possess technological sovereignty in regard to cybersecurity and is dependent on others, provision for international co-operation in the legal text could help others interpret the legislation in a less provocative and more benign manner. The pursuit of technological sovereignty needs to be undertaken on an incremental basis with great sensitivity.

Fourthly, security cooperation is at risk with the text of this draft legislative proposal as is. This absence of provision for international cooperation may well be perceived as a retrograde and even hostile step by others with adverse geopolitical consequences. It sends out a dangerous message that Europe is not interested in international cooperation on cybersecurity. It may also have the unintended consequence of weakening of cooperation between Member States on cybersecurity. Secure information sharing on cyber threats could become highly selective or even cease. Collaboration and even dialogue with US multinational cybersecurity firms, on whom Europe is greatly dependent, could be disrupted.

Proposed Text

Article 10

Cooperation of the Competence Centre with Union institutions, bodies, offices and agencies and other international cooperation

1. **To ensure coherence and complementarity, avoiding any duplication of efforts** the Competence Centre shall cooperate with relevant Union institutions, bodies, offices and agencies including **the European Union Agency for Cybersecurity-ENISA 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 established by Commission Implementing Decision 2013/778/EU¹¹, the Innovation and Networks Executive Agency established by Commission Implementing Decision 2013/801/EU¹², the European Cybercrime Centre at Europol, as well as the European Defence Agency and other relevant Union entities.**
The Centre may also cooperate with international organisations, where relevant.

¹¹ **Commission Implementing Decision 2013/778/EU of 13 December 2013 establishing the Research Executive Agency and repealing Decision 2008/46/EC (OJ 346, 20.12.2013, p. 54).**

¹² **Commission Implementing Decision 2013/801/EU of 23 December 2013 establishing the Innovation and Networks Executive Agency and repealing Decision 2007/60/EC as amended by Decision 2008/593/EC (OJ 352, 24.12.2013, p. 65).**

Commented [A34]: What international organisations is the Centre going to be cooperating with?

Focus here should be international agreements with third countries.

Commented [A35]: "International organisations" is a very narrow term limited to inter-governmental entities.

2. Such cooperation shall take place within the framework of working arrangements. Those arrangements shall be submitted to the ~~prior~~ approval of the ~~Commission~~ **Governing Board**.
3. The Union may conclude international agreements, in accordance with TFEU Article 218, with third countries or international organisations, allowing and organising their participation as appropriate with the Centre, the Network and the Cybersecurity Competence Community.

Commented [A36]: Legal provision is needed for international cooperation. The legislation should not be protectionist, closing off options that politically MS may wish to explore with particular third countries, similar to concept of association agreements that exist in Horizon 2020.

MS Sovereign Right to Manage National Coordination Centre Membership

Ireland has several times drawn attention to the provision in Article 8.4 in regard to the Centre revoking an entity's membership of the Cybersecurity Competence Community. If a National Coordination Centre has approved an entity for membership, then it should only be for that same National Coordination Centre to revoke such membership.

The EU Centre should have no such role as it detracts from the competence of Member States. As a compromise, Ireland had suggested that the Network of National Coordination Centres could be consulted before a National Coordination Centre would decide to revoke membership. In principle, National Coordination Centres would have regard to the views of their peers before deciding on revocation. Conflict between the Member State based National Coordination Centre and the Commission oriented Centre should be avoided. A Member State whose National Coordination Centre has been undermined by the Centre will not be inclined to cooperate with the EU structures leading in turn to fragmentation of effort as regards development of research, innovation, industrial and technological capabilities on cybersecurity.

Proposed Text

Article 8

The Cybersecurity Competence Community

4.

The ~~Competence~~ Centre shall ~~accredit-register~~ 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, **including, where appropriate, an assessment on security grounds,** of whether that entity meets the criteria provided for in paragraph 3 **of this Article**. ~~An registration-accreditation~~ shall not be limited in time but may be revoked by the ~~Competence~~ Centre at any time if ~~the Centre~~ it or the relevant

Commented [A37]: It is not clear whether many entities who are designated as National Coordination Centres would have the administrative capability to undertake a generic security assessment. NCCs are about research and innovation promotion not State or public security.

Commented [A38]: If the NCC decides who should be part of the Community, then that same NCC should decide who needs to leave the Community. The Centre itself should have no role. However the Network could be consulted by the NCC before decisions on admission and revocation are taken.

National Coordination Centre considers that the entity does not fulfil the criteria set out in paragraph 3 **of this Article or** ~~or it~~ falls under the relevant provisions set out in Article 136 of Regulation XXX [new financial regulation], **or for justified security reasons.**

MS Sovereign Right to Independently undertake Cybersecurity Cooperation on Research, Innovation, Industrial and Technological Developments in the interests of their economic wellbeing.

The establishment and operation of the proposed Centre, Network and Community should be without prejudice to the rights of Member States to pursue their own agendas in regard to capabilities development on the matter of cybersecurity.

Nothing in this draft Regulation should restrict or impede Member States resourcing and or incentivising collaborations and partnerships with entities from third countries. Ireland's recently published National Cyber Security Strategy 2019-2024 provides for such partnerships. We would therefore welcome an explicit assurance in the text that Member States are free to pursue and resource from their own public resources collaborations on research, innovation, technological and industrial development with entities from third countries. Otherwise this draft legislation can become a strait jacket that restricts the ability and autonomy of Member States to take actions that they consider important in the field of cybersecurity research, innovation, industrial and technological development. Decisions by the Centre are taken by qualified majority rather than by unanimity so dissenting Member States who are outvoted need flexibility to pursue their public interest agendas.

Proposed text

Article 1

Subject matter

5. **This Regulation is without prejudice to the competences of the Member States regarding activities concerning public security, defence, national security (including the economic well-being of the state when issues refer to national security matters) and the activities of the state in areas of criminal law.**
6. **This Regulation is without prejudice to the competences of the Member States to independently resource, fund and otherwise incentivise research, innovation, technological, industrial developments on cybersecurity with interests from third countries.**

Commented [A39]: This text is needed. It existed in previous EU Regulations, notably 526/2013. The economic well being of Member States must be of relevance.

Commented [A40]: Member States must retain the capacity to independently develop and encourage relations with economic interests from third countries. Some Member States want to maintain an open global approach to industrial development on cybersecurity.

GREECE

First of all we would like to thank the Presidency for all the efforts and hard work on the draft Regulation and for taking on board and into account our comments and concerns regarding the wording of recital 21 and articles 4a and 13 par. 4.

You will find below some additional comments.

RECITAL 21

- (21) In view of its expertise in cybersecurity and its mandate as a reference point for advice and expertise on cybersecurity for Union institutions, agencies and bodies, as well as ~~for~~ relevant Union stakeholders, ~~as well as~~ **and in view of** its collection of input through its tasks, ~~for instance on cybersecurity certification and standardisation~~ the European Union **Agency** for Cybersecurity (**ENISA**) ~~as~~ **established by Regulation (EU) 2019/881 ("ENISA")** should play an active part in the activities of the Centre including the development of the Agenda, avoiding any duplication of their tasks in particular through its role as permanent observer in the Governing Board **of the Centre ("Governing Board")**. **Regarding the drafting of the Agenda, and the annual work programme and the multiannual work programme of the Centre, the Executive Director of the Centre ("Executive Director") and the Governing Board of the Centre should take into account any relevant strategic advice and input provided by ENISA, according to the rules of procedure with deadlines set by the Governing Board of the Centre.**¹³

Commented [A41]: We suggest the addition of the following wording : «Both ENISA, as regards the provision of support to the formulation and implementation of the European cybersecurity policy, and the Centre, as regards the coordination of the research, innovation and deployment in the field of cybersecurity, should fulfill their objectives and tasks provided in the Regulation (EU) 2019/881 and the current Regulation on the basis of complementarity». This is to better clarify the operational scope of the two entities instead of make a vague reference to a "structured cooperation" between them.

Article 3

Mission of the Competence Centre and the Network

1. The ~~Competence~~ Centre and the Network shall help the Union to:
 - (a) retain and develop, **in an autonomous manner, the Union's** ~~the~~ cybersecurity **research**, technological and industrial capacities **and capabilities** necessary to **strengthen trust and security in secure** the Digital Single Market;
 - (b) increase the **global** competitiveness of the Union's cybersecurity industry and turn cybersecurity into ~~a~~ competitive advantage of other Union industries.

2. The ~~Competence Centre and the Network~~ shall undertake ~~their~~ tasks, where appropriate, in collaboration with ~~ENISA and the Network of National Coordination Centres and a~~ the Cybersecurity Competence Community.

- 2a. **Only** actions contributing to the missions set out in paragraph 1 shall be eligible for support through Union financial assistance in accordance with **the legal acts establishing relevant programmes notably** Horizon Europe and Digital Europe **regulations.**

Commented [A42]: We suggest the addition of the following wording "as regards the formulation and implementation of the European Cybersecurity policy" in order to be aligned with our comments on recital 21.

SPAIN

- (9a) When the Centre is preparing its annual work programme ("annual work programme"), it should inform the Commission on its co-funding needs based on the Member States' planned voluntary co-funding contributions to joint actions, in order for the Commission to take into account the Union matching contribution in the preparation of the draft general budget for the following year. During the first four years of Horizon Europe, a maximum of [XX %] of the annual budget of Cluster [Y] shall be programmed through joint actions. For the remaining part of the programme, and in accordance with the strategic Planning process of Horizon Europe, this percentage may be increased. The Horizon Europe Programme Committee shall communicate the total budgetary share of each work programme dedicated to joint actions.
- (9b) Where the Commission prepares the Horizon Europe Work programme of the Horizon Europe programme for matters related to cyber security, including in the context of its stakeholder consultation process and particularly before the adoption of that work programme, the Commission should take into due account the input of the Centre Governing Board and Executive Director and share its such input with the Horizon Europe Programme Committee of the Horizon Europe programme.
- (9c) In order to support its role in the area of cybersecurity and the involvement of the Network and to provide a strong governance role for the Member States ~~of National Coordination Centres~~, the Centre should be established as a Union body with legal personality. ~~To achieve its role, it should manage funding.~~ The Centre should perform a dual role by undertaking specific tasks in the area of cybersecurity industry, technology and research as laid down ~~in Art 4 and 4a~~ this Regulation and by managing cybersecurity related funding from several programmes at the same time – notably the Horizon Europe programme and the Digital Europe programme, and possibly even further Union programmes. Such management should be in line accordance with their ~~regulations~~ rules applicable to those programmes. ~~The Centre will therefore have a special nature~~ Nevertheless, considering that the funding for the functioning of the Centre would originate primarily from the ~~{DEP}~~ Digital Europe programme and the ~~{Horizon Europe}~~ funding programmes ~~and in view of the absence of appropriate funding alternatives in those funding programmes~~, it is necessary that the Centre is considered as a partnership for the purpose of budget implementation, including the programming phase.

Commented [A43]: Clarify whether this coordination (to share) exercise implies decision making or opinion

(12a) In addition to the necessary administrative capacity, The National Coordination

Centres **should have the necessary administrative capacity and should either possess or have direct access to cybersecurity industrial, technological and research 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 and be in a position 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 Council⁴⁴, and the research community.**

- (13) Where financial support is provided to National Coordination Centres in order to support third parties at the national level, **this that financial support should** be passed on to relevant **stakeholders beneficiaries** through cascading grant agreements.

Commented [A44]: The implementation of actions may not be delegated in cascade to the coordination centres, but must be managed entirely by the Centre.

⁴⁴ 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).

- (15) The Competence Centre should have several key functions. First, the Competence Centre should facilitate and help coordinate the work of the European Cybersecurity Competence Network and nurture support the Cybersecurity Competence Community. The Centre should drive implement cybersecurity relevant parts of the Digital Europe programme and the Horizon Europe programme in accordance with its the Centre's multiannual work programme ("multiannual work programme") and the annual strategic work programme and the strategic planning process of the Horizon Europe programme , which will by allocating grants, typically following a competitive call for proposals the cybersecurity technological agenda in accordance with its multiannual work programme, and facilitate transfer of access to the expertise gathered in the Network and the Cybersecurity Competence Community and . Secondly, it should implement relevant parts of Digital Europe and Horizon Europe programmes by allocating grants, typically following a competitive call for proposals. Thirdly, the Competence Centre should facilitate support joint investment by the Union, Member States and/or industry.
- (16) The Competence Centre and the National Coordination Centres should stimulate and support the cooperation and coordination of the activities of the Cybersecurity Competence Community, which would involve a large, open, and diverse group of actors involved in cybersecurity technology. That Community should include in particular research entities, supply-side industries, demand-side industries, civil society groups in the area of cybersecurity and the public sector. The Cybersecurity Competence Community should provide input to the activities and multiannual work programme and the annual work programme of the Competence Centre and it should also benefit from the community-building activities of the Competence Centre and the Network, but otherwise should not be privileged with regard to calls for proposals or calls for tender.

Formatted: Font: Times New Roman (Theme Headings, Strikethrough, Kern at 12 pt

Article 4a

Tasks of the Centre

1. In order to fulfill the mission laid out in Article 3 and the objectives laid out in Article 4, the Centre shall, in close cooperation with the Network, have the following ~~strategic and implementation~~ tasks:

(a) strategic tasks, consisting of:

(1) developing and monitoring the implementation of a comprehensive and sustainable Cybersecurity Industrial, Technology and Research Agenda, which ~~will~~ shall set out strategic recommendations and goals for the development and growth of the European cybersecurity industrial, technological and research ~~sectorecosystem~~ (the “Agenda”);

(2) through the Agenda and the multiannual work programme, while avoiding any duplication of ~~efforts~~ activities with ENISA:

(i) defining priorities for its work on:

- ~~for its work on~~ the enhancement of cybersecurity research and innovation and its deployment,
- the development of cybersecurity industrial, technological and research capacities ~~and~~ capabilities, ~~skills~~ and infrastructure,
- the reinforcement of cybersecurity **industrial, technological and research** skills and training and
- the deployment of cybersecurity products and solutions, and

(ii) supporting cybersecurity industry, with a view to strengthening Union excellence, capacities and competitiveness on cybersecurity;

- (3)** ensuring synergies and cooperation ~~while avoiding duplication of activities~~ with relevant Union institutions, agencies and bodies such as ENISA ~~while avoiding any duplication of activities with such Union institutions, agencies and bodies;~~
- (4)** coordinating National Coordination Centres through the Network and ensuring regular exchange of expertise;
- (5)** ~~providing expert advice upon request from a Member State to that Member State;~~
- (6)** facilitating collaboration and sharing of expertise among relevant stakeholders, in particular members of the **Cybersecurity Competence Community**; ~~this may include financially supporting education, training, exercises and building up cybersecurity skills;~~
- (7)** facilitating the use of results from research and innovation projects in actions related to the development of cybersecurity products and solutions, seeking to avoid fragmentation and duplication of efforts and ~~to replicating~~ good cybersecurity practices and **cybersecurity** products and solutions, including those developed by **small and medium enterprises (SMEs)** and those based on open-source software; ~~Support to the deployment of cybersecurity products and solutions should to the extent possible rely on the European cybersecurity certification framework as defined by the Cybersecurity Act.~~
- (8)** The design of the Center's agenda and the multiannual work programme should be aligned with the corresponding Horizon Europe cluster in order to avoid inefficiencies

Formatted: Indent: Left: 2 cm, Hanging: 0.99 cm

(b) implementation tasks, consisting of:

- (1)** coordinating ~~and administrating~~ the work of the Network and the Cybersecurity Competence Community in order to achieve the mission set out in Article 3, in particular supporting cybersecurity start-ups and SMEs in the **European Union** and facilitating their access to expertise, funding, investment and to markets;

Article 7

Tasks of the National Coordination Centres

1. The National Coordination Centres shall have the following tasks:
 - (a) **acting as contact points at the national level for the Cybersecurity Competence Community** to supporting the Competence Centre in achieving its objective and missions, and in particular in coordinating the Cybersecurity Competence Community **through the coordination of its national members;**
 - (aa) **providing expertise and actively contributing to the strategic planning of the activities according to tasks referred to in Article 4a, taking into account relevant national and regional challenges for cybersecurity in different sectors;**
 - (b) facilitating the participation of industry, **research institutions** and other actors at the Member State level in cross-border projects;

- e) ~~contributing, together with the Competence Centre, to identifying and addressing sector specific cyber security industrial challenges;~~
- d) ~~acting as contact point at the national level for the Cybersecurity Competence Community and the Competence Centre;~~
- (e) seeking to establish synergies with relevant activities at the national and regional level, **such as including national policies on research, development and innovation in the area of cybersecurity, and in particular those policies stated in the national cybersecurity strategies;**
- (f) **implementing specific actions for which grants have been awarded by the Competence Centre, including through provision of financial support to third parties in line accordance with Article 204 of Regulation (EU, Euratom) 2018/1046 under conditions specified in the concerned grant agreements concerned;**
- (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;
- (h) assessing requests by entities established in the same Member State as the **National** Coordination Centre for becoming part of the Cybersecurity Competence Community;
- (i) **advocating and promoting involvement by relevant entities in the activities arising from the Centre, Network and Community, and monitoring, as appropriate, the level of engagement with and grant actions awarded for cybersecurity research, developments and deployments, with particular reference to the entities regulated under Directive (EU) 2016/1148.**

2. For the purposes of point (f) **of paragraph 1 of this Article**, the financial support to third parties may be provided in any of the forms specified in Article 125 of Regulation **(EU, Euratom) 2018/1046XXX [new Financial Regulation]**, including in the form of lump sums.

Commented [A45]: In accordance to recital 13, implementation of specific actions may not be delegated in cascade to the coordination centres, but must be managed entirely by the Centre.

3. National Coordination Centres may receive a grant from the Union in accordance with **point (d) of the first paragraph of** Article 195 (d) of Regulation **(EU, Euratom) 2018/1046XXX [new Financial Regulation]** in relation to carrying out the tasks laid down in this Article.
4. National Coordination Centres shall, where relevant, cooperate through the Network for the purpose of implementing tasks referred to in points (a), (b), (c), (e) and (g) of paragraph 1.

Article 8

The Cybersecurity Competence Community

1. The Cybersecurity Competence Community shall contribute to the mission of the ~~Competence Centre and the Network~~ as laid down in Article 3 and enhance and disseminate cybersecurity expertise across the Union.
2. The Cybersecurity Competence Community shall, **on the one hand**, consist of industry, academic and non-profit research organisations, **other relevant civil society and** associations as well as public entities and other entities dealing with cybersecurity operational and technical matters , such as ECSO, **and, on the other hand, where relevant, actors of sectors having an interest in cybersecurity and facing cybersecurity challenges.** It shall bring together the main stakeholders with regard to cybersecurity **research**, technological and industrial capacities in the Union. It shall involve National Coordination Centres as well as Union institutions and bodies with relevant expertise, **such as ENISA.**

Commented [A46]: "We'd like to insist in mentioning ECSO in this article as an association that has performed an outstanding role during the development of the cPPP in Cybersecurity"

- 3a. The Governing Board may invite, on a case-by-case basis, other persons to attend its meetings as observers, including additional representatives of the Commission, for ensuring coordination and synergies between different Union activities involving cybersecurity.
4. **Representatives of the Cybersecurity Competence Community** ~~Members of the Industrial and Scientific Advisory Board~~ may take part, upon invitation from the Chairperson, in the meetings of the Governing Board, without voting rights.
5. The members of the Governing Board and their alternates may, subject to its rules of procedure, be assisted at the meetings by advisers or experts.
6. The ~~Competence~~ Centre shall provide the secretariat for the Governing Board.

Article 15

Voting rules of the Governing Board

- 1. A vote shall be held if the members of the Governing Board failed to achieve consensus.
- 2. The Governing Board shall take its decisions by a majority of at least 75% of all its members, **with voting rights, the representatives of the Commission constituting a single member for this purpose.** An absent member of the Governing Board may delegate his or her vote to his or her alternate or, in the absence of his or her alternate, to another member. Any member of the Governing Board may represent not more than one other member. **[For decisions related to the usage of Union funds in Article 13(3) except point (cb), the Union should hold 50% of the voting rights].**

Commented [A47]: The risk in this new version is that the voting system may favor certain Member states that would Foster JAs and, since the COM holds 50% of the voting rights the decision-making process would be much easier to deblock the funding for those JAs. In this sense, we agree with the NL that All Member States should have voting rights in the Governing Board, independent of the financial contribution.

FRANCE

- (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 **research and technological capacities** to secure its Digital Single Market **as outlined by the Commission in its Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions entitled "A Digital Single Market Strategy for Europe"**, and in particular to protect critical networks and information systems and to provide key cybersecurity services.
- (6) A wealth of expertise and experience in cybersecurity research, technology and industrial development exists in the Union, but the efforts of industrial and research communities are fragmented, lacking alignment and a common mission, which hinders competitiveness in this domain. These efforts and expertise need to be pooled, networked and used in an efficient manner to reinforce and complement existing research, technology and industrial capacities at Union and national levels.
- (7) The Council Conclusions adopted in November 2017 called on the Commission to provide rapidly an impact assessment on the possible options to create a **Network of Cybersecurity Competence Centres, together with ~~the~~ a European Cybersecurity Research and Competence Centre** and propose by mid-2018 the relevant legal instrument.

Commented [A48]: -FR/ Nous proposons de mentionner également la communication sur la stratégie numérique du 19/02 « Façonner l'avenir numérique de l'Europe » qui couvre la stratégie de cybersécurité

programme established by Regulation 2020/... of the European Parliament and of the Council¹⁵ ('the Digital Europe programmes'), and should be open to the European Regional Development Fund and other programmes where appropriate. This approach should contribute to creating synergies and coordinating financial support related to cybersecurity research, innovation, technology and industrial development and avoiding unnecessary duplication. **The Centre should not play an operational role or a technical assistance role. Upon request from a Member State the Centre should be able to provide expert advice to that Member State.**

Commented [A49]: FR/this addition does not seem necessary

- (8a) The ~~Competence~~ Centre **would** benefit from the ~~particular expertise~~ experience and the broad and relevant stakeholders' representation built through the contractual public-private partnership on cybersecurity between the Commission and European Cyber Security Organisation ECSO Association during the duration of the Framework Programme for Research and Innovation (2014-2020) ("Horizon 2020"), established by Regulation (EU) No 1291/2013 of the European Parliament and of the Council¹⁶, and the lessons learned from four pilot projects¹⁷ launched in early 2019 under Horizon 2020, **thereby building on the existing experience that has been set up by the contractual public-private partnership on cybersecurity,** for the management of the Cybersecurity Competence Community, and the representation of the Cybersecurity Competence Community in the Centre.
- (9) The Centre should develop and monitor the implementation of a comprehensive and sustainable Cybersecurity Industrial, Technology and Research Agenda ~~Strategy~~ which will set out strategic recommendations and priorities for development and growth of the European cybersecurity ~~ecosystem~~ **industrial, technological and research sector** (the "Agenda"). The Agenda **should provide the basis for the annual and multi-annual work programme of the Centre. Furthermore, the Agenda** should be taken duly

15

Regulation 2020/... of the European Parliament and of the Council, of ..., establishing the Digital Europe programme for the period 2021-2027 (OJ ...) [2018/0227(COD)].

16

Regulation (EU) No 1291/2013 of the European Parliament and of the Council of 11 December 2013 establishing Horizon 2020 - the Framework Programme for Research and Innovation (2014-2020) and repealing Decision No 1982/2006/EC (OJ L 347, 20.12.2013, p. 104).

17

CONCORDIA, ECHO, SPARTA and CyberSec4Europe are the four winning pilot projects of the 2018 Horizon 2020 cybersecurity call "establishing and operating a pilot for a European Cybersecurity Competence Network and developing a common European Cybersecurity Research & Innovation Roadmap".

into account in particular within the ~~bi-annual and annual~~ planning and implementation of the Horizon Europe programme and the Digital Europe programme in the area of cybersecurity. The Agenda could also ~~serve~~ ~~be able to provide as~~ cybersecurity specific advice, where relevant, ~~for~~ the implementation of other Union programmes.

~~activities supporting~~ 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, for example in order to achieve security-by-design. They should also support the deployment of cybersecurity products and solutions ~~and to the extent while~~ promoting where possible, ~~rely the implementation of~~ the European cybersecurity certification framework as defined by Regulation (EU) 2019/881 of the European Parliament and of the Council¹⁸ ~~the Cybersecurity Act~~.

Commented [A50]: FR/the term "promoting" is already a much weaker wording than what was previously agreed, therefore we would like to delete "where possible". We would like to remind the considerable weakening of this sentence since it was moved from an article to a recital, which is not in line with what was proposed as a compromise by the presidency at the HWP meeting

- (21) In view of its expertise in cybersecurity and its mandate as a reference point for advice and expertise on cybersecurity for Union institutions, agencies and bodies, as well as for relevant Union stakeholders, ~~as well as~~ and in view of its collection of input through its tasks, ~~for instance on cybersecurity certification and standardisation~~ the European Union Agency for Cybersecurity (ENISA) as established by Regulation (EU) 2019/881 ("ENISA") should play an active part in the activities of the Centre including the development of the Agenda, avoiding any duplication of their tasks in particular through its role as permanent observer in the Governing Board of the Centre ("Governing Board"). Regarding the drafting of the Agenda, and the annual work programme and the multiannual work programme of the Centre, the Executive Director of the Centre ("Executive Director") and the Governing Board of the Centre should take into account any relevant strategic advice and input provided by ENISA, according to the rules of procedure within deadlines set by the Governing Board of the Centre.
- (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 this ~~present initiative~~ Regulation.
- (23) ~~The Union contribution to the Competence Centre should finance half of the costs arising from the establishment, administrative and coordination activities of the Competence Centre. In order to avoid double funding, those activities should not benefit simultaneously from a contribution from other Union programmes.~~

HAVE ADOPTED THIS REGULATION:

CHAPTER I

GENERAL PROVISIONS AND PRINCIPLES OF THE COMPETENCE CENTRE AND THE NETWORK

Article 1

Subject matter

1. This Regulation establishes the European Cybersecurity Industrial, Technology and Research Competence Centre (the 'Competence Centre'), as well as the Network of National Coordination Centres (the "Network"), and lays down rules for the nomination

Commented [A51]: FR/we welcome the addition of "relevant"; we would not support any change to that sentence that would make the advice of ENISA binding on the governing board as it would reduce the influence of the governing board, and by that, Member states, regarding strategic decisions

of National Coordination Centres, as well as for the establishment of the Cybersecurity Competence Community ~~(the “Community”)~~.

2. The ~~Competence~~ Centre shall **contribute have an important role in** ~~to~~ the implementation of the cybersecurity part of the Digital Europe programme **established by Regulation No XXX** and in particular actions related to Article 6 of Regulation (EU) No XXX [Digital Europe Programme] ~~thereof~~ and of the Horizon Europe programme **established by Regulation No XXX** and in particular Section 2.2.6 of Pillar II of Annex I. of Decision No XXX on establishing the specific programme implementing Horizon Europe – the Framework Programme for Research and Innovation [ref. number of the Specific Programme].
3. ~~The seat of the Competence Centre shall be located in [XXXBrussels, Belgium].~~

Commented [A52]: FR/we strongly disagree with this modification which creates further confusion on the role of the Centre and has already been the subject of lengthy discussions at the Council ; We would suggest either to revert to “contribute to the implementation” or to delete “contribute” and to simply use the term “shall implement”

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.

~~4a The seat of the Competence Centre shall be located in [XXXBrussels, Belgium].~~

Commented [A53]: Suppression en lien avec les articles 1.3 et 44

Article 2

Definitions

For the purpose of this Regulation, the following definitions ~~shall~~ apply:

- (1) 'cybersecurity' means ~~the protection~~ **the activities necessary to protect** network and information systems, ~~the-users of such systems~~, and other persons **affected by** ~~against~~ cyber threats;
- (1a) **'network and information system' means a network and information system as defined in point (1) of Article 4 of Directive (EU) 2016/1148;**
- (2) 'cybersecurity products and solutions' means ICT products, services or processes with the specific purpose of protecting network and information systems, ~~their~~ users **of such** systems and ~~other affected~~ persons **affected by** ~~from~~ cyber threats;
- (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;**

- (4) ~~participating Member State contributing Member State~~ means a Member State which voluntarily contributes financially to the administrative and operational costs of the Competence Centre.
- (3) "joint actions" means an actions included in the **Centre's annual work programme** receiving Union financial support from the Horizon Europe programme and/or Digital Europe programme, as well as financial or in-kind support by one or more Member States, ~~to be~~ which are implemented via projects involving beneficiaries established in the Member States which provide financial or in-kind support to those beneficiaries ~~entities~~ stemming from those Member States.
- (4) "in-kind contribution **by Member States**" means those eligible costs, incurred by National Coordination Centres and other public entities when participating in projects funded through this Regulation, which are not financed by a Union contribution. ~~In the case of projects funded through Horizon Europe, eligible costs shall be calculated in line with Article 32 of the Regulation establishing Horizon Europe. In the case of projects funded through Digital Europe, eligible costs shall be calculated in line with the Financial Regulation.~~¹⁹

Article 3

Mission of the Competence Centre and the Network

1. The ~~Competence~~ Centre and the Network shall help the Union to:
 - (a) **retain and develop, in an autonomous manner, the Union's the cybersecurity research,** technological and industrial capacities **and capabilities** necessary to **strengthen trust and security in secure the Digital Single Market;**
 - (b) increase the **global** competitiveness of the Union's cybersecurity industry and turn cybersecurity into a competitive advantage of other Union industries.
2. The ~~Competence~~ Centre **and the Network** shall undertake ~~their~~ its tasks, where appropriate, in collaboration with **ENISA and the Network of National Coordination Centres and a the Cybersecurity Competence Community.**
- 2a. **Only actions contributing to the missions set out in paragraph 1 shall be eligible for support through Union financial assistance in accordance with the legal acts establishing relevant programmes notably Horizon Europe and Digital Europe regulations.**

Commented [A54]: FR/this is very important for us to maintain this text as it is

Commented [A55]: FR/we welcome the reintroduction of the word "only"; we would still prefer to delete the part from "in accordance " onwards as it has been stated that it is already clear that the Centre should comply with both regulations

¹⁹

Reference to the Financial Regulation and other legislative acts.

Article 4

Objectives and Tasks of the Centre

The Competence Centre shall **enhance the coordination of research, innovation and deployment in the field of cybersecurity in order to fulfil the missions as described in Article 3 and strengthen the competitiveness of the European Union and its Digital Single Market**, by:

- (1) defining strategic orientations and priorities for research, innovation and deployment in cybersecurity in line with Union law;
- (2) implementing actions under relevant Union funding programmes in line with the defined Union's strategic orientations; and
- (3) ~~and by stimulating cooperation and coordination within National Coordination Centres and the Cybersecurity Competence Community.~~ have the following objectives and related tasks:
 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;~~
 2. ~~contribute to the implementation of the cybersecurity part of the Digital Europe Programme established by Regulation No XXX²⁰ and in particular actions related to Article 6 of Regulation (EU) No XXX [Digital Europe Programme] and of the Horizon Europe Programme established by Regulation No XXX²¹ and in particular Section 2.2.6 of Pillar II of Annex I. of Decision No XXX on establishing the specific programme implementing Horizon Europe — the Framework Programme for Research and Innovation [ref. number of the Specific Programme]. and of other Union programmes when provided for in legal acts of the Union];~~
 3. ~~enhance cybersecurity capabilities, knowledge and infrastructures at the service of industries, the public sector and research communities, by carrying out the following tasks:~~
 - (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;~~
 - (b) ~~having regard to the state of the art cybersecurity industrial and research infrastructures and related services, providing support to other entities, including financially, to acquiring, upgrading, operating and making available~~

²⁰[add full title and OJ reference]

²¹[add full title and OJ reference]

- 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;
- (e) ~~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;~~

Article 4a

Tasks of the Centre

1. In order to fulfill the mission laid out in Article 3 and the objectives laid out in Article 4, the Centre shall, in close cooperation with the Network, have the following ~~strategic and implementation~~ tasks:

(a) strategic tasks, consisting of:

(1) developing and monitoring the implementation of a comprehensive and sustainable Cybersecurity Industrial, Technology and Research Agenda, which ~~will~~ shall set out strategic recommendations and goals for the development and growth of the European cybersecurity industrial, technological and research ~~sectorecosystem~~ (the “Agenda”);

(2) through the Agenda and the multiannual work programme, while avoiding any duplication of ~~efforts~~ activities with ENISA:

(i) defining priorities for its work on:

- ~~for its work on~~ the enhancement of cybersecurity research and innovation and its deployment,
- the development of cybersecurity industrial, technological and research capacities ~~and~~ capabilities, ~~skills~~ and infrastructure,
- the reinforcement of cybersecurity **industrial, technological and research** skills and training and
- the deployment of cybersecurity products and solutions, and

(ii) supporting cybersecurity industry, with a view to strengthening Union excellence, capacities and competitiveness on cybersecurity;

(3) ensuring synergies and cooperation ~~while avoiding duplication of activities~~ with relevant Union institutions, agencies and bodies such as ENISA **while avoiding any duplication of activities with such Union institutions, agencies and bodies;**

(4) coordinating National Coordination Centres through the Network and ensuring regular exchange of expertise;

Commented [A56]: FR/ as previously stated, we see a contradiction in this sentence : ensuring synergies and cooperation in our opinion cannot possibly create duplication of activities as the whole point of creating synergies and cooperation is to avoid duplication ; we would like to delete the addition from “while” onwards, as otherwise the sentence does not make any sense

(5) providing expert advice upon request from a Member State to that Member State;

(6) facilitating collaboration and sharing of expertise among relevant stakeholders, in particular members of the Cybersecurity Competence Community; ~~this may include financially supporting education, training, exercises and building up cyber security skills;~~

(7) facilitating the use of results from research and innovation projects in actions related to the development of cybersecurity products and solutions, seeking to avoid fragmentation and duplication of efforts and ~~to replicating~~ good cybersecurity practices and cybersecurity products and solutions, including those developed by small and medium enterprises (SMEs) and those based on open-source software; ~~Support to the deployment of cybersecurity products and solutions should to the extent possible rely on the European cybersecurity certification framework as defined by the Cybersecurity Act.~~

Commented [A57]: FR/this addition is too vague and broad ; we do not understand the purpose of this addition and would prefer to delete

(b) implementation tasks, consisting of:

(1) coordinating and administrating the work of the Network and the Cybersecurity Competence Community in order to achieve the mission set out in Article 3, in particular supporting cybersecurity start-ups and SMEs in the European Union and facilitating their access to expertise, funding, investment and to markets;

Article 13

Tasks of the Governing Board

1. The Governing Board shall have the overall responsibility for the strategic orientation and the operations of the Competence Centre, and shall supervise the implementation of its activities **and shall be responsible for any task that is not specifically allocated to the Executive Director.**
2. The Governing Board shall adopt its rules of procedure. Those rules shall include specific procedures for identifying and avoiding conflicts of interest and ensure the confidentiality of any sensitive information.
3. The Governing Board shall take the necessary strategic decisions, in particular:
 - (a) develop and adopt the Agenda encompassing strategic goals and priorities for a sustainable development of the European cybersecurity research, technological and industrial sector and monitor its implementation;**

(aa) based on the Agenda, adopt **the** multiannual work programme, containing the development of **a** common, industrial, technology and research **strategic priorities roadmap, which are based on the basis of** the needs identified by Member States in cooperation with the Cybersecurity Competence Community **and which** require the focus of Union's financial support. Such priorities shall include key technologies and domains for developing the Union's own capabilities in cybersecurity **strategie autonomy**; a statement of the major priorities and planned initiatives of the Competence Centre, including an estimate of financing needs and sources;

Commented [A58]: FR/this part is very important for us

- (aaa) adopt the annual work plan programme for implementing the relevant Union funds, notably the cybersecurity parts of the Horizon Europe programme and the Digital Europe programme, in accordance with the Centre's multi annual work programme and the strategic planning process of the Horizon Europe programme including an estimation of the of financing needs and sources; Where appropriate, proposals and in particular the annual work programme shall assess the need to apply security rules as set out in Article 34 of this Regulation, including in particular the security self-assessment procedure in accordance with Article 16 of the [XXXX Horizon Europe Regulation];**
- (b) adopt the ~~Competence~~ Centre's work plan, annual accounts and balance sheet and annual activity report, on the basis of a proposal from the Executive Director;
- (c) adopt the specific financial rules of the ~~Competence~~ Centre in accordance with [Article 70 of Regulation (EU, Euratom) 2018/1046 the ~~FR~~Financial Regulation];
- (ca) **in the line with the Centre's as part of the Centre's annual work programme adopt decisions to dedicate allocate funds from the Union budget to joint actions between the Union and Member States;**
- (cb) **as part of the annual work programme and in accordance with the decisions referred to in point (ca) of this paragraph, and without prejudice to the regulations establishing Horizon Europe and the Digital Europe Programme, adopt decisions relating to the description the joint actions referred to in point (ca) and lay down conditions for their implementation.**
- (d) adopt a procedure for appointing the Executive Director;
- ~~e) adopt the criteria and procedures for assessing and accrediting the entities as members of the Cybersecurity Competence Community;~~
- (f) appoint, dismiss, extend the term of office of, provide guidance to and monitor the performance of the Executive Director, and appoint the Accounting Officer;
- (g) adopt the annual budget of the ~~Competence~~ Centre, including the corresponding staff establishment plan indicating the number of temporary posts by function group and by grade and the number of contract staff and seconded national experts expressed in full-time equivalents;
- (h) adopt rules **for the prevention and management of conflicts of interest in respect of its members;** ~~regarding conflicts of interest;~~

- (i) **when appropriate, ~~provide~~ seek advice ~~to~~ from the Cybersecurity Competence Community with regard to the establishment of working groups and establish such groups with members of the Cybersecurity Competence Community;**
- j) ~~appoint members of the Industrial and Scientific Advisory Board;~~
- (k) set up an Internal Auditing Function in accordance with Commission Delegated Regulation (EU) No 1271/2013²²;
- (l) **set up a monitoring mechanism to ensure that the implementation of the respective funds is done in accordance with the Agenda, the missions and the multiannual work programme of the Centre;**
- (la) ~~to ensure a regular dialogue and establish an effective cooperation mechanism with the Cybersecurity Competence Community;~~
- l) ~~promote the Competence Centre globally, so as to raise its attractiveness and make it a world class body for excellence in cybersecurity;~~
- (m) establish the Competence Centre's communications policy upon recommendation by the Executive Director;
- (n) be responsible to monitor the adequate follow-up of the conclusions of retrospective evaluations;
- (o) where appropriate, establish implementing rules to the Staff Regulations and the Conditions of Employment in accordance with Article 31(3);
- (p) where appropriate, lay down rules on the secondment of national experts to the Competence Centre and on the use of trainees in accordance with Article 32(2);
- (q) adopt security rules for the Competence Centre;
- (r) adopt an anti-fraud strategy that is proportionate to the fraud risks having regard to a cost-benefit analysis of the measures to be implemented;
- (s) adopt the methodology to calculate the **voluntary financial and in-kind** contribution from **contributing Member States in accordance with Horizon Europe and Digital Europe Regulations;**
- (sa) **register entities nominated by Member States as their National Coordination Centres;**
- (sb) **in deciding on the annual work programme and the multiannual work programme, ensure coherence and synergies with those parts of the Digital**

Commented [A59]: FR/this was already discussed that to reduce the administrative burden of the Centre, the task of creating working groups should not be one of the Centre, but of the Community upon advice from the Centre. We do not understand why it was reverted back. We would like to go back to the previous version.

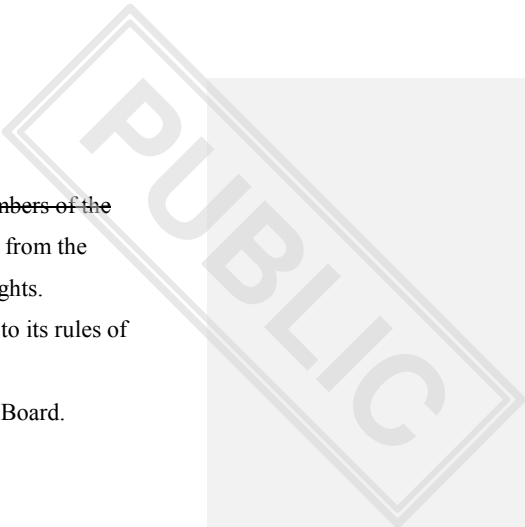
- Europe programme and the Horizon Europe programme which are not managed by the Centre, as well as with other Union programmes;
- t) be responsible for any task that is not specifically allocated to a particular body of the Competence Centre; it may assign such tasks to anybody of the Competence Centre;
 - (u) discuss and adopt the annual report on the implementation of the Centre's strategic goals and priorities with a recommendation, if necessary, for their better realisation
 - v) ~~specify an operational methodology for calculating the in-kind contributions of Member States.~~
4. Regarding the tasks laid down in points (a), (aa) and (aaa) of paragraph 3, the Executive Director and the Governing Board shall take into account any relevant strategic advice and input provided by ENISA, within deadlines according to the rules of procedure set by the Governing Board.

Commented [A60]: FR/ we welcome the addition of the word "relevant", we still believe however that "shall" is too strong, and we would prefer "should" or "may"

Article 14

Chairperson and Meetings of the Governing Board

1. The Governing Board shall elect a Chairperson and a Deputy Chairperson from among the its members with voting rights, for a period of ~~two~~ three years. The mandate of the Chairperson and the Deputy Chairperson may be extended once, following a decision by the Governing Board. If, however, their membership of the Governing Board ends at any time during their term of office, their term of office shall automatically expire on that date. The Deputy Chairperson shall *ex officio* replace the Chairperson if the latter is unable to attend to his or her duties. The Chairperson shall take part in the voting.
2. The Governing Board shall hold its ordinary meetings at least three times a year. It may hold extraordinary meetings at the request of the Commission, at the request of one third of all its members, at the request of the Chairperson, or at the request of the Executive Director in the fulfilment of his/her tasks.
3. The Executive Director shall take part in the deliberations, unless decided otherwise by the Governing Board, but shall have no voting rights.
- 3a. The Governing Board may invite, on a case-by-case basis, other persons to attend its meetings as observers, including additional representatives of the Commission, for ensuring coordination and synergies between different Union activities involving cybersecurity.

- 
4. **Representatives of the Cybersecurity Competence Community** ~~Members of the Industrial and Scientific Advisory Board~~ may take part, upon invitation from the Chairperson, in the meetings of the Governing Board, without voting rights.
 5. The members of the Governing Board and their alternates may, subject to its rules of procedure, be assisted at the meetings by advisers or experts.
 6. The ~~Competence~~ Centre shall provide the secretariat for the Governing Board.

Article 15

Voting rules of the Governing Board

- 1. **A vote shall be held if the members of the Governing Board failed to achieve consensus.**

- 2. The Governing Board shall take its decisions by a majority of at least 75% of all its members, **with voting rights, the representatives of the Commission constituting a single member for this purpose.** An absent member of the Governing Board may delegate his or her vote to his or her alternate or, in the absence of his or her alternate, to another member. Any member of the Governing Board may represent not more than one other member. **[For decisions related to the usage of Union funds in Article 13(3) except point (cb), the Union should hold 50% of the voting rights].**
- 2a. For decisions related to the task laid down in point (cb) of Article 13(3), contributing Member States and the Commission shall ~~hold~~ votes in a manner that is proportional to their relevant contribution on a specific joint action in line with the methodology adopted pursuant to point (s) of Article 13(3).
- 1- For ~~any other~~ decisions other than those referred to in paragraph -2a, ~~every~~ each Member States and the Union ~~shall hold 50 % of the voting rights shall have one vote.~~ **The vote ing rights of the Union shall be indivisible cast jointly by the two representatives of the Commission [or unanimous].**
2. ~~Every participating Member State shall hold one vote.~~
3. ~~The Governing Board shall take its decisions by a majority of at least 75% of all votes, including the votes of the members who are absent, representing at least 75% of the total financial contributions to the Competence Centre. The financial contribution will be calculated based on the estimated expenditures proposed by the Member States referred to in point c of Article 17(2) and based on the report on the value of the contributions of the participating Member States referred to in Article 22(5).~~
4. ~~Only the representatives of the Commission and the representatives of the participating Member States shall hold voting rights.~~
5. The Chairperson shall take part in the voting.

Commented [A61]: FR/ Nous comprenons que “*the Union should hold 50% of the voting rights*” revient à accorder un droit de veto à la Commission pour des décisions touchant à un domaine sensible qui est la cybersécurité. Nous réitérons notre opposition et notre demande de clarification de la base juridique retenue pour cette formulation.

Commented [A62]: FR/ we believe that the wording “the voting rights of the Union shall be indivisible” was clearer than the new wording “cast jointly” as casting a vote jointly does not mean in our understanding that the voting has to be the same

CHAPTER III

FINANCIAL PROVISIONS

Article 21

Union and Member States’ financial contribution

- 1. **The Centre shall be funded by the Union.**
1. The Union’s contribution to the ~~Competence~~ Centre to cover administrative costs and operational costs shall comprise the following:

- a) [EUR 1 981 668 000] from the Digital Europe programme, including up to [EUR 23 746 000] for administrative costs;
- b) an amount from the Horizon Europe programme, including for administrative costs, **for joint actions, which shall be equal to the amount contributed voluntary by Member States pursuant to paragraph 5 of this Article 21(5) and but not exceed [the amount determined in the strategic planning process of the Horizon Europe programme]** ~~to be determined by taking into account the strategic planning process~~ to be carried out pursuant to Article 6(6) of Regulation XXX [Horizon Europe Regulation] **and the multiannual work programme and the annual work programmes of the Centre.**

2. The maximum Union contribution shall be paid from the appropriations in the general budget of the Union allocated to [Digital Europe Programme] and to the specific programme implementing Horizon Europe, established by Decision XXX.
3. The ~~Competence~~ Centre shall implement cybersecurity actions of [Digital Europe Programme] and [Horizon Europe Programme] in accordance with point (c)(iv) **of the first subparagraph** of Article 62 **(1)** of Regulation (EU, Euratom) ~~XXX²³~~ **the Financial Regulation** 2018/1046.
54. ~~The Union financial contribution shall not cover the tasks referred to in Article 4(8)(b).~~ **Contributions from Union programmes other than those referred to in paragraphs 1 and 2 above that are part of a Union co-financing to a programme implemented by one of the Member States shall not be accounted for in the calculation of the Union maximum financial contribution referred to in paragraphs 1 and 2) above.**
65. ~~Member States can make voluntary financial contributions for joint action with the Union, paid in instalments and in kind contributions consisting of costs incurred by National Coordination Centres and beneficiaries in implementing actions that are not reimbursed by the Centre.~~

Voluntary contributions made by one or more Member States for joint actions with the Union may take the form of financial or in-kind contributions.

Financial contributions by Member States may take the form of support by Member States provided to participants in joint actions.

In-kind contributions by Member States shall consist of eligible costs incurred by National Coordination Centres and other public entities when participating in projects funded through this Regulation less any Union contribution to those costs. In the case of projects funded through Horizon Europe, eligible costs shall be calculated in line with Article 32 of the Regulation establishing Horizon Europe. In the case of projects funded through Digital Europe, eligible costs shall be calculated in line with the Financial Regulation (EU, Euratom) 2018/1046.

The envisaged amount of total Member State voluntary contributions, including for administrative costs, to joint actions under the Horizon Europe Framework programme shall be determined in order to be taken into account in as part of the strategic planning process of the Horizon Europe programme to be carried out pursuant to Article 6(6) of Regulation XXX [Horizon Europe Regulation], with input from the Governing Board of the Centre.

For actions under the Digital Europe programme, notwithstanding Article 15 of the [Regulation establishing the Digital Europe Programme], the Member States may make a contribution to the costs of the Competence Centre that are co-financed from the Digital Europe programme that is lower than the amounts specified in [Article 21(1)(ab) – reference to be checked] of this Regulation.

Commented [A63]: FR/ This part should be in square brackets in order to be consistent with the §1.1.b. Indeed, these 2 § are clearly linked on that subject and the final decision about this wording shall so be taken later and at the same time.

CHAPTER IV

COMPETENCE CENTRE STAFF

Article 31

Staff

1. The Staff Regulations of Officials and the Conditions of Employment of Other Servants of the European Union as laid down by Council Regulation (EEC, Euratom, ECSC) No 259/68²⁴ ('Staff Regulations' and 'Conditions of Employment') and the rules adopted jointly by the institutions of the Union for the purpose of applying the Staff Regulations and Conditions of Employment shall apply to the staff of the ~~Competence~~ Centre.
2. The Governing Board shall exercise, with respect to the staff of the ~~Competence~~ Centre, the powers conferred by the Staff Regulations on the Appointing Authority and the powers conferred by the Conditions of Employment on the authority empowered to conclude contract ('the appointing authority powers').
3. The Governing Board shall adopt, in accordance with Article 110 of the Staff Regulations, a decision based on Article 2(1) of the Staff Regulations and on Article 6 of the Conditions of Employment delegating the relevant appointing authority powers to the Executive Director and defining the conditions under which that delegation may be suspended. The Executive Director is authorised to sub-delegate those powers.

4. Where exceptional circumstances so require, the Governing Board may, **through a** decision, temporarily suspend the delegation of the appointing authority powers to the Executive Director and any sub-delegation made by the latter. In such a case the Governing Board shall exercise itself the appointing authority powers or delegate them to one of its members or to a member **of staff** of the ~~Competence~~ Centre other than the Executive Director.
5. The Governing Board shall adopt implementing rules as regards the Staff Regulations and the Conditions of Employment in accordance with Article 110 of the Staff Regulations.
6. The staff resources shall be determined in the **staff**-establishment plan **referred to in point (g) of Article 13(3) of the Competence Centre**, indicating the number of temporary posts by function group and by grade and the number of contract staff expressed in full-time equivalents, in line with its annual budget.
7. **The human resources required in the Centre shall be met inter alia by redeployment of staff posts from Union institutions, bodies, offices and agencies.** The staff of the ~~Competence~~ Centre ~~shall~~ **may** consist of temporary staff and contract staff.
8. All costs related to staff shall be borne by the ~~Competence~~ Centre.

Commented [A64]: FR/we are against this addition which is weakening the EC proposal of a neutral HR cost for the Union, although it was confirmed at the EC that the neutral cost would work with redeployment of posts. It seems strange that MS would ask for additional administrative costs than what was proposed by the EC. We would like to ask for a deletion of "inter alia".

Article 32

Seconded national experts and other staff

1. The ~~Competence~~ Centre may make use of seconded national experts or other staff not employed by the ~~Competence~~ Centre.
2. The Governing Board shall adopt a decision laying down rules on the secondment of national experts to the ~~Competence~~ Centre, in agreement with the Commission.

LUXEMBOURG

Article 3

Mission of the Competence Centre and the Network

1. The Competence Centre and the Network shall help the Union to:

- (a) retain and develop, in an autonomous manner, the Union's the cybersecurity research, innovation, technological and industrial capacities and capabilities necessary to strengthen trust and security in secure the Digital Single Market;
- (b) increase the global competitiveness of the Union's cybersecurity industry ecosystem and turn cybersecurity into a competitive advantage of other Union industries.

[...]

Article 8

The Cybersecurity Competence Community

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

2. The Cybersecurity Competence Community shall, on the one hand, consist of industry, academic and non-profit research organisations, other relevant civil society and associations as well as public entities and other entities dealing with cybersecurity operational and technical matters and, on the other hand, where relevant, actors of sectors having an interest in cybersecurity and facing cybersecurity challenges. It shall bring together the main stakeholders with regard to cybersecurity research, innovation, technological and industrial capacities in the Union. It shall involve National Coordination Centres as well as Union institutions and bodies with relevant expertise, such as ENISA.

3. Only entities which are established within the Union may be accredited registered as members of the Cybersecurity Competence Community. They shall demonstrate that they can contribute to the missions as set out in Article 3 and shall have cybersecurity expertise with regard to at least one of the following domains:

- (a) academic or industrial research and innovation;
- (b) industrial, services or product development and innovation;
- (c) training and education;
- (d) information security and/or incident response operations;
- (e) scientific or technical partnerships or cooperation with academic and/or public authorities as defined under Article 2(3).

Furthermore they should comply with the relevant national security regulations.

[...]

HUNGARY

Hungary's comment on the CCCN regulation (REV3):

The revised text offers an acceptable compromise. Our only suggestion is that you consider supplementing preamble (7b) with „sovereignty”. Achieving technological sovereignty would help to ensure trust in ICT products and services and it would be line with the Commission's previous statements.

We suggest the following wording:

“The Union still lacks sufficient technological **sovereignty** and industrial capacities and capabilities to autonomously secure its economy and critical infrastructures and to become a global leader in cybersecurity field.”

NETHERLANDS

Please find below the NL comments in addition to our comments on Rev2, which we sent on 6 March (WK 2598/2020 ADD 1).

In addition to our General Comments we would like to observe the following:

General comments

- policy to promote additional themes or to or disregard the European strategic themes put forward;
- The Netherlands supports the line the Presidency has taken regarding the seat of the Centre: the discussion should be held in CRP.
- At this moment the text mentions: Horizon Europe, Horizon Europe programme, Horizon Europe framework programme; and Framework Programme for Research and innovation; consistency in the text would be good; as for the terminology we would prefer: *Framework Programme for Research and innovation*, and/or *Horizon Europe*.

In addition to the comments:

With a view to Article 21, 22 and 23 of the Regulation, and order to assess the proposal, we would request an estimate of the costs for the Member States.

AUSTRIA

Written Comments – Austria **Regulation CCCN – Doc. 5341/3/2020 REV 3**

Art. 1 para 4a

- This para should be in square brackets. It would also be helpful if the text included all possible legal options for the selection of the seat.

Art. 4a para 1 lit. a subpara 5, Recital 8

- The merit of this provision is questionable as it is ENISA's task to provide advice and expertise in the field of cybersecurity according to the Cybersecurity Act. Any further explanation or limitation is welcome.

Art. 7 para 4

- This paragraph must be revised because the reference are either not relevant anymore or do not fit the tasks of the Network (see also our comments to REV 2). The Network shall be an informal structure, which exchanges information and best practises when necessary. We support a light structure which doesn't add another layer of bureaucracy.

Art. 10 para 1

- We recommend striking "European Cybercrime Centre at" to anticipate possible future developments within Europol in particular with regard to the EU Innovation Hub.

Art. 13

- Para 3 lit. a: As it stands now, we think that the Governing Board would develop and, thus, draft the Agenda [whereby the secretariat for the Governing Board is provided by the Centre (Art. 14.6) and the secretariat for the meetings of the Governing Board by the Executive Director (Art. 17.2.b)]. If the Executive Director shall prepare a draft of the Agenda this should be included in Art. 17 as it is a very important tasks.
- Para 3 lit. aa has to be aligned with Art 17 para 2 lit. c. While according to Art 17.2.c there needs to be an opinion of the Network and the Community for the draft multiannual work programme prepared by the Executive Director, Art 13.3.aa refers to the needs identified by Member States (instead of the Network) in cooperation with the Community (cooperation vs. and). If Art. 13.3.aa describes the same like Art. 17.2.c the wording should be aligned and consistent (by using the wording of Art. 17.2.c). On the other hand, if it describes something different, it should be clarified what MS are supposed to deliver in cooperation with the Community.

Art. 17 para 2

- Lit. i: It is still unclear what kind of agreements are meant here. It either can be deleted or should be rephrased. The question is whether the signing of grant agreements is not already covered by lit. q.

Art. 31 para 7

This is an important paragraph and shall be kept in the text. We cannot agree with the changes made and propose “primarily” instead. We thank the Presidency who already indicated that this would be changed accordingly in the HWPCI meeting on 11 March.

POLAND

- 1) Support for recital 7a and as a consequence deletion of art. 1 par 4a, as they contradict each other.
- 2) Recital 8 – the last added sentence – what kind of expert advice will the Centre provide. This is not clear. What’s the reason to add this sentence?;
- 3) Recital 9a – we should add work programmes „...in the preparation of the draft general budget **and work programmes** for the following year”
- 4) Recital 15 – phrase „in accordance with its multiannual work programme” is used twice. Is it necessary? We propose to add „other forms of funding” in the part: „the strategic planning process of the Horizon Europe programme by allocating grants and **other forms of funding**”
- 5) Support for recital 21
- 6) Recital 24 – what’s the purpose of adding second sentence „The Governing Board should adopt the Agenda consisting of **strategic goals** that have to be fulfilled by the Centre”. It’s not in line with recital 9 that states that Agenda will set out **strategic recommendations and priorities** for development and growth of the European cybersecurity ecosystem industrial, technological and research sector (the “Agenda”).
- 7) Recital 28a – question: what are the limits for project financing (HE foresees for 70% and 30% by the beneficiary). Wording of this recital states that 100% is covered by EU and national centres (50% each). The HE rules must be kept
- 8) art. 1 par. 4a should be deleted. The seat should be decided by the Council only.
- 9) Art. 2(4) – the definition may incline that MS can only put to the project in kind contributions, as is says „which are not financed by a Union contribution”. The definition needs rewording to be clear that in-kind contributions are those which are not financial (amount of money given by MS) and are not financed by the EU
- 10) Art.4a(a)(1) which states that Agenda shall set out strategic recommendations and **goals** for the development and growth of the European cybersecurity industrial, technological and research sector is not in line with recital 9 that states that Agenda will set out strategic recommendations and **priorities** for development and growth of the European cybersecurity **ecosystem** industrial, technological and research sector (the “Agenda”).
- 11) Art.4a(a)(2) support for phrase „avoiding any duplication of activities with ENISA”
- 12) Art.4a(a)(5) it should be clear what kind of expert advice is foreseen, in what field?

- 13) Art. 8 (4) the phrase „That assessment shall also take into account, where relevant, any national assessment on security grounds made by the national competent authorities” may not be suitable for achieving the foreseen goals. Maybe it would be a good idea to use wording from DEP Regulation – art. 12 – „Legal entities established established or deemed to be established in Member States and controlled by Member States and/or nationals of Member States”.
- 14) Art. 13 (3) (cb) the sentence „adopt decisions relating to the description the joint actions referred to in point (ca) and lay down conditions for their implementation” is not clear. What are decisions related to the description the joint actions? And „their implementation” means implementation of joint actions?
- 15) Art. 13 (3)(l) we propose to add the following wording: „set up a monitoring mechanism to ensure that the implementation of the respective funds is done in accordance with the Agenda, the missions and the multiannual work programme **and with the rules of programmes where funding originates from**”
- 16) Support for art. 13(4)
- 17) The sentence „[For decisions related to the usage of Union funds in Article 13(3) except point (cb), the Union should hold 50% of the voting rights].” should be deleted. EC should not have a right to veto decisions.
- 18) Art. 15 (2a) the decision if there should be a concrete action should be taken with the rule one MS one vote. Then in the implementation process of the already agreed, concrete joint action the decisions should be made with the rule that the vote corresponds to the amount of the contribution. It’s still not clear in the text, even more with current wording of art. 13(cb)
- 19) Art. 23 (7) what does in this case mean „without prejudice to Article 13(3)(cb)”. Art. 13 (3) (cb) states that „as part of the annual work programme and in accordance with the decisions referred to in point (ca) of this paragraph, and without prejudice to the regulations establishing Horizon Europe and the Digital Europe Programme, adopt decisions relating to the description the joint actions referred to in point (ca) and lay down conditions for their implementation.”. The Governing Board cannot change by its decisions the rule expressed in the Regulation that all assets shall be owned by the Centre, unless the Regulation foresees that and set conditions to make such a decision. Now it doesn’t. The phrase „without prejudice to Article 13(3)(cb)” makes only confusion as Article 13(3)(cb) states nothing about the ownership. The ownership of the assets should be clearly regulated in the Regulation.

- 20) General comment and question to the EC: it's seems that the draft doesn't cover some practical questions like: what will happen with the financing when the beneficiary withdraws in course of project – who will cover the costs? Will it be the national centre? What kind of agreements will be signed – the HE grant agreement?
- 21) General comment and question to EC, especially DG RTD – will there be no legal obstacles in Centre's activities and HE financing and implementation in line with HE Strategic planning, having in mind that the list of partnerships in the HE Strategic Plan does not include the Centre or does not mention a Centre as an implementing body.

PORTUGAL

Amendments (in red) by PT to document 5341/3/20 REV3

Recitals

(8) The ~~Competence~~ Centre should be the Union's main instrument to pool investment in cybersecurity research, technology and industrial development and to implement relevant projects and initiatives together with ~~the a Cybersecurity Competence Network of National Coordination Centre ("the Network")~~. The Centre ~~it~~ should deliver cybersecurity-related financial support from ~~the~~ Horizon Europe - the Framework Programme for Research and Innovation established by Regulation 2020/... of the European Parliament and of the Council²⁵ ('the Horizon Europe programme') and the Digital Europe programme established by Regulation 2020/... of the European Parliament and of the Council²⁶ ('the Digital Europe programmes'), and should be open to the European Regional Development Fund and other programmes where appropriate. This approach should contribute to creating synergies and coordinating financial support related to cybersecurity research, innovation, technology and industrial development and avoiding unnecessary duplication. The Centre should not play an operational role or a technical assistance role. Upon request from a Member State the Centre should be able to provide expert advice to that Member State, **within the limits of the Centre's mandate**.

Rationale: This clarifies that the Center only acts within its mandate. The center should not offer general advice on cybersecurity issues.

(9c) In order to support its role in the area of cybersecurity **and the involvement of the Network** and to provide a strong governance role for the Member States ~~of National Coordination Centres~~, the Centre should be established as a Union body with legal personality. ~~To achieve its role, it should manage funding~~. The Centre should perform a dual role by undertaking specific tasks in the area of cybersecurity industry, technology and research as laid down **in Art 4 and 4a** this Regulation and by managing cybersecurity related funding from several programmes at the same time – notably the Horizon Europe programme and the Digital Europe programme, and possibly even further Union programmes. **Such management should must be** in ~~line~~ accordance with

²⁵ Regulation 2020/... of the European Parliament and of the Council, of ..., establishing Horizon Europe - the Framework Programme for Research and Innovation, laying down its rules for participation and dissemination (OJ ...) [2018/0224(COD)].

²⁶ Regulation 2020/... of the European Parliament and of the Council, of ..., establishing the Digital Europe programme for the period 2021-2027 (OJ ...) [2018/0227(COD)].

~~their regulations~~ rules applicable to **those programmes**. ~~The Centre will therefore have a special nature~~ Nevertheless, considering that the funding for the functioning of the Centre would originate primarily from the ~~{DEP}~~ Digital Europe programme and the ~~{Horizon Europe}~~ funding programmes ~~and in view of the absence of appropriate funding alternatives in those funding programmes~~, it is necessary that the Centre is considered as a partnership for the purpose of budget implementation, including the programming phase.

Rationale: Self-evident. Management must be in accordance with rules applicable to Horizon Europe and Digital Europe Programme.

- (11) The ~~Competence~~ Centre should facilitate and ~~help~~ coordinate the work of the ~~Cybersecurity Competence~~ Network (~~"the Network"~~), **which should be** made up of National Coordination Centres, ~~one in~~ **from** each Member State. National Coordination Centres should receive direct Union financial support, including grants awarded without a call for proposals, ~~except from Horizon Europe funding~~, in order to carry out **their** activities related to this Regulation.

Rationale: Horizon Europe doesn't provide for institutional funding. The amendment is needed in order to comply with the Horizon Europe regulation.

- (15) The ~~Competence~~ Centre ~~should have several key functions~~. First, the Competence Centre should **facilitate and help coordinate the work of the** European Cybersecurity Competence Network **and nurture support** the Cybersecurity Competence Community. The Centre should ~~drive~~ implement **cybersecurity** relevant parts of the Digital Europe programme and the Horizon Europe programme in accordance with ~~its~~ **the Centre's** multiannual work programme ("**multiannual work programme**") and **the** annual strategic work programme and the strategic planning process of the Horizon Europe programme by allocating grants, ~~primarily typically~~ following a competitive call for proposals ~~the cybersecurity technological agenda in accordance with its multiannual work programme, and facilitate transfer of access to the expertise gathered in the Network and the Cybersecurity Competence Community and~~. Secondly, it should implement relevant parts of Digital Europe and Horizon Europe programmes by allocating grants, typically following a competitive call for proposals. Thirdly, the Competence Centre should **facilitate support** joint investment by the Union, Member States ~~and/or~~ industry.

Rationale: Calls need to be competitive and no financing from Horizon Europe should be allocated without a call.

Furthermore, as we have consistently said during HWP Ciber meetings, additional clarification is needed concerning the process on how the Centre will implement the cybersecurity part of Horizon Europe and, more specifically, the link between this recital and recital 9b.

(18b) The enhancement of dual use ~~application~~-deployment, specifically through the Digital Europe Programme, of cybersecurity technologies for cybersecurity purposes is without prejudice to the civilian nature of this Regulation and should therefore reflect specificities of Member States in cases when cybersecurity policy is pursued by civil-military or military authorities, and ensure complementarity but not overlap to the cyber defence related funding instruments.

Rationale: In Horizon Europe dual use is not accepted. Therefore, it should be clear that this recital applies only to deployment and, therefore, to the Digital Europe Programme.

(24a) The Governing Board should be entrusted, **through the adequate legal procedures and complying with the regulation of the programmes**, with the powers necessary to establish the budget **of the Centre**, verify its execution, adopt the appropriate financial rules, establish transparent working procedures for decision making by the ~~Competence~~ Centre, adopt the ~~Competence~~ **Centre's annual work programme** and the multiannual **work programme**, reflecting the priorities **set in the Agenda** in achieving the objectives and tasks of the ~~Competence~~ Centre, adopt its rules of procedure, appoint the Executive Director **of the Centre** and decide on the extension of the Executive Director's term of office and on the termination thereof.

Rationale: This recital should specify who entrusts the Centre with the aforementioned powers and through which procedure.

(28a) Contributions of the Member States to the resources of the Centre can be financial and/or in-kind. Financial contributions could for example consist of a grant given by a Member State to a beneficiary in that Member State complementing Union financial support to a project under the annual work programme, or the contribution of the Member State to the operational costs of the Centre. On the other hand, in-kind contributions would typically accrue where a Member State entity is itself the

beneficiary of a Union financial support. For example, if the Union subsidised an activity of a National Coordination Centre at the financing rate of 50%, the remaining cost ~~will~~ would be accounted for as in-kind contribution. In another example, where a Member State entity received Union financial support for creating or upgrading an infrastructure to be shared among stakeholders in line with the annual work programme, the related non-subsidised costs ~~are~~ would be accounted for as in-kind contributions.

Rationale: The expression “financial and/or in kind” used in this recital should be the expression used throughout the whole text of the regulation in order to ensure consistency. In general, when a MS is supporting a call through a “virtual common-pot” these contributions are considered financial and not in-kind. Since the Centre is a Union body, and a partnership for the purpose of budget implementation (recital 9c), according to the HEU regulation a financial commitment (and not an in-kind commitment) is required from the Member State. Furthermore, additional clarity is needed in the regulation as to how in-kind contributions apply.

Articles

Article 1

Subject matter

2. The Competence Centre shall ~~contribute~~ **have an important role in** to the implementation of the cybersecurity part of the Digital Europe programme ~~established by Regulation No XXX~~ **and** in particular actions related to Article 6 of Regulation (EU) No XXX [Digital Europe Programme] ~~thereof~~ and of the Horizon Europe programme ~~established by Regulation No XXX~~ and in particular ~~Section 2.2.6 of Pillar II of Annex I~~ **3.1.3** of Decision No XXX on establishing the specific programme implementing Horizon Europe – the Framework Programme for Research and Innovation [ref. number of the Specific Programme].

Rationale: The correct reference should be 3.1.3 in accordance with the Partial General Approach (PGA). Council Legal Service can help clarify this question.

Article 2

Definitions

For the purpose of this Regulation, the following definitions ~~shall~~ apply:

- (1) 'cybersecurity' means ~~the protection of the activities necessary to protect network and information systems, the users of such systems, and other persons affected by~~ ~~against cyber threats;~~ cybersecurity as defined in point (1) of Article 2 of REGULATION (EU) 2019/881;

Rationale: Reference to the definition of cybersecurity in the Cybersecurity Act for the sake of coherence with article 2 (1a) concerning the definition of “network and information system” from the NIS Directive.

- (3) "joint actions" means an actions included in the **Centre's annual work programme** receiving Union financial support from the Horizon Europe programme and/or Digital Europe programme, and/or financial or in-kind support by ~~one~~ **three** or more Member States, ~~to be~~ which are implemented via projects involving beneficiaries established in the Member States which provide financial and/or in-kind support to those beneficiaries ~~entities~~ stemming from those Member States.

Rationale: Horizon Europe (article 18) stipulates that “joint-actions” must involve at least three independent legal entities each established in a different Member State or associated country and with at least one of them established in a Member State, unless the work programme provides otherwise, if duly justified; A “joint action” with just one Member States does not contribute to the overarching principle behind this regulation which is to avoid fragmentation in the field of cybersecurity in the EU.

- (4) "in-kind contribution **by Member States**" means those eligible costs, incurred by National Coordination Centres and other public entities **in implementing indirect actions corresponding to the research and innovation agenda, less the contributions by the Centre and any other Union contribution to those costs** ~~when participating in projects funded through this Regulation, which are not financed by a Union contribution. In the case of projects funded through Horizon Europe, eligible costs shall be calculated in line with Article 32 of the Regulation establishing Horizon Europe. In the case of~~

projects funded through Digital Europe, eligible costs shall be calculated in line with the Financial Regulation.²⁷

Rationale: This article must be aligned with recital (28a). Further clarification is therefore needed in the regulation as to how in-kind contributions are defined and apply. This suggested amendment aligns the definition of in-kind with the definition included in other partnerships, as for example EuroHPC.

Article 4a

Tasks of the Centre

1(b) (2) (ii) joint actions receiving support from the cybersecurity parts of the Horizon Europe programme established by Regulation (EU) No XXX established by Regulation No XXX and in particular Section 2.2.6 of Pillar II of Annex I. Section 2.2.6 of Pillar II of Annex I. 3.1.3 of Decision No XXX on establishing the specific programme implementing Horizon Europe – the Framework Programme for Research and Innovation [ref. number of the Specific Programme], and in accordance with the multiannual strategic work programme of the centre, and the strategic planning process of the Horizon Europe programme, and

Rationale: Additional clarification, as has been regularly requested in the HWP cyber, is needed on how the Centre is entitled to manage the entire budget (including “joint actions”) of the cybersecurity parts of Horizon Europe. What is the process through which the Centre manages the cybersecurity parts of Horizon Europe and how is this articulated with the programme approved by Horizon Europe programme committee, as the latter only takes into account the “input” from the Centre (see recital 9.b).

The correct reference should be 3.1.3 of the PGA (see previous reasoning on this point).

1 (b) (4) enabling the deployment and facilitating the acquisition of cybersecurity infrastructures, at the service of industries, the public sector, and research communities and operators of essential services, through *inter alia* voluntary contributions from Member States and Union funding for joint actions, in line with the Agenda, the multiannual work programme and the annual work programmes. Such Union funding shall not be conditioned to voluntary funding from Member States;

²⁷— Reference to the Financial Regulation and other legislative acts.

Rationale: This article refers to infrastructures and at the same time to joint-actions. If there is an European procurement in the name of MS there is a need to have MS contribution, so there is no need to reference that it is voluntary. One part is indeed voluntary (to participate in the calls), but there is a part that needs to be an upfront financial instalment. Clarification on this question is required throughout the text.

2. In accordance with Article 6 of the Horizon Europe Framework programme and subject to the conclusion of a contribution agreement as referred to in point (18) of Article 2 of Regulation (EU, Euratom) 2018/1046, the Centre may be entrusted with the implementation of the cybersecurity parts that are not co-funded by the Member States in the Horizon Europe Programme [established by Regulation No XXX and in particular ~~Section 2.2.6 of Pillar II of Annex I~~ Section 3.1.3 of Decision No XXX on establishing the specific programme implementing Horizon Europe – the Framework Programme for Research and Innovation [ref. number of the Specific Programme]

Rationale: ‘contribution agreement’ means an agreement concluded with persons or entities implementing Union funds pursuant to points (c)(ii) to (viii) of the first subparagraph of Article 62(1) of the Financial Regulation. Clarity is therefore needed on what form this contribution agreement takes. Article 62 of the Financial Regulation refers to the methods of budget implementation – and articles 70 and Article 71 are applicable here concerning public-private partnership bodies. Therefore the Centre is an other Union body in the form of a partnership. Therefore it should comply with the articles of Horizon Europe regarding partnerships. What occurs when the Centre is not entrusted with the implementation of the cybersecurity parts that are not co-funded by the Member States in the Horizon Europe Programme? The correct reference should be 3.1.3 of the PGA (see previous rationale on this point).

Article 13

Tasks of the Governing Board

3. (ca) ~~in the line with the Centre's~~ as part of the Centre's annual work programme adopt decisions ~~to dedicate~~ allocate funds from the Union budget to joint actions between the Union and Member States;

3. (cb) as part of the annual work programme and in accordance with the decisions referred to in point (ca) ~~of this paragraph~~, and ~~without prejudice according to the regulations~~ establishing Horizon Europe and the Digital Europe Programme, **adopt decisions relating to the description the joint actions referred to in point (ca) and lay down conditions for their implementation.**

Rationale: Red line for PT. The regulation has to comply with the HE and DEP. See recitals 9a (on joint actions) and 9c (on compliance with HE and DEP).

3. (s) adopt the methodology to calculate the ~~voluntary~~ financial **and in-kind** contribution from contributing Member States **in accordance with Horizon Europe and Digital Europe Regulations;**

Rationale: This article should be in line with art.21.b).

Article 15

Voting rules of the Governing Board

-2. The Governing Board shall take its decisions by a majority of at least 75% of all its members, ~~with voting rights~~, **the representatives of the Commission constituting a single member for this purpose.** An absent member of the Governing Board may delegate his or her vote to his or her alternate or, in the absence of his or her alternate, to another member. Any member of the Governing Board may represent not more than one other member. ~~For decisions related to the usage of Union funds in Article 13(3) except point (cb), the Union should hold 50% of the voting rights.~~

Rationale: This is a red line for PT. The Commission needs to respond for the implementation of the programmes budget. According to the Financial Regulation, and in alignment with what occurs in other partnership regulations, the European Commission must have 50% of voting rights.

-2a. **[For decisions related to the task laid down in point (cb) of Article 13(3), contributing Member States and the Commission shall hold votes in a manner that is proportional to their relevant contribution on a specific joint action in line with the methodology adopted pursuant to point (s) of Article 13(3).]**

Rationale: Red Line for PT. This article is only acceptable as long as the changes we propose to 13(3) (cb) are incorporated.

Article 21

Union and Member States' financial contribution

2. The ~~maximum~~ Union contribution shall be paid from the appropriations in the general budget of the Union allocated to [Digital Europe Programme] and to the specific programme implementing Horizon Europe, established by Decision XXX.

Rationale: redundant.

3. The ~~Competence~~ Centre shall implement cybersecurity actions of [Digital Europe Programme] and [Horizon Europe Programme]⁶² in accordance with point (c)(iv) **of the first subparagraph** of Article 62 **(1), 70 and 71** of Regulation (EU, Euratom) ~~XXX²³ the Financial Regulation~~ **2018/1046**.

Rationale: Include reference to Union Bodies referred to in articles 70 and 71 of the Financial Regulation (see compromise agreement on this point).

54. ~~The Union financial contribution shall not cover the tasks referred to in Article 4(8)(b).~~ **Contributions from Union programmes other than those referred to in paragraphs 1 and 2 above that are part of a Union co-financing to a programme implemented by one of the Member States shall not be accounted for in the calculation of the Union ~~maximum~~ financial contribution referred to in paragraphs 1 and 2) above.**

Rationale: Redundant, see rationale above for article 21.2. Perhaps, additional clarification on this paragraph is required.

65. ~~Member States can make voluntary financial contributions for joint action with the Union, paid in instalments and in-kind contributions consisting of costs incurred by National Coordination Centres and beneficiaries in implementing actions that are not reimbursed by the Centre.~~

Voluntary contributions made by ~~one~~ **three** or more Member States for joint actions with the Union may take the form of financial or in-kind contributions.

Administrative costs must be cover by ex-ante financial contributions.

Financial contributions by Member States may take the form of support by Member States provided to participants in joint actions.

In-kind contributions by Member States shall consist of eligible costs incurred by National Coordination Centres and other public entities when participating in projects funded through this Regulation less any Union contribution to those costs. In the case of projects funded through Horizon Europe, eligible costs shall be calculated in line with Article 32 of the Regulation establishing Horizon Europe. In the case of projects funded through Digital Europe, eligible costs shall be calculated in line with the Financial Regulation (EU, Euratom) 2018/1046.

The envisaged amount of total Member State ~~voluntary~~ contributions, including for administrative costs, to joint actions under the Horizon Europe Framework programme shall be determined in order to be taken into account in ~~as part of the~~ strategic planning process of the Horizon Europe programme to be carried out pursuant to Article 6(6) of Regulation XXX [Horizon Europe Regulation], with input from the Governing Board of the Centre.

For actions under the Digital Europe programme, notwithstanding Article 15 of the [Regulation establishing the Digital Europe Programme], the Member States may make a contribution to the costs of the ~~Competence~~ Centre that are co-financed from the Digital Europe programme that is lower than the amounts specified in [Article 21(1)(ab) – reference to be checked] of this Regulation.

Rationale: There is a need for an ex-ante contribution to be financial and not in-kind to go beyond the funding of calls and to, at least, cover administrative costs.

Article 23

Costs and resources of the ~~Competence~~ Centre

1. ~~The Competence Centre shall be jointly funded by the Union and Member States through financial contributions paid in instalments and contributions consisting of costs incurred by National Coordination Centres and beneficiaries in implementing actions that are not reimbursed by the Competence Centre.~~
2. The administrative costs of the ~~Competence~~ Centre shall not exceed EUR [number] and shall be covered by means of financial contributions divided equally on an annual basis between from the Union. and the participating Member State. **Additional contributions shall be made by contributing Member States in proportion to their ~~voluntary~~ contributions to joint actions between the Union and Member States.** If part of the contribution for administrative costs is not used, it may be made available to cover the operational costs of the ~~Competence~~ Centre.

Rationale: Ensure coherence with rest of text. There is no need to refer here if the contributions are voluntary or not. Moreover there is a need for an ex-ante commitment not in proportion to the voluntary contributions because the Centre needs to operate on a regular basis independent of the fluctuation of the voluntary contributions.

3. (b) **voluntary financial and/or in-kind** contributions from the ~~participating contributing~~ Member States **in case of joint actions between the Union and Member States** in the ~~form of:~~

Rationale: Same rationale as previously mentioned to ensure consistency throughout the whole text. The expression “financial and/or in kind” used in recital (28a) should be the expression to be used throughout the whole text of the regulation.

4. (b) ~~participating contributing~~ Member States' **voluntary** financial contributions to the administrative **costs in case of joint actions between the Union and Member States;**

Rationale: Contributions to administrative costs must be financial. See rationale presented for article 4a 1(b) (4) and for article 21.5.

SLOVAK REPUBLIC

- 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 - Mandate for negotiations with European Parliament

- article 1 (4a) – We propose to delete the whole provision, because it is in contradiction with the recital (7a). We are convinced that the Council should take the decision about the seat.

- article 6 (4) – To increase the clarity of the text we propose to return the reference to the NIS Directive:

“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).”

- article 8 – We propose to keep the Cybersecurity Competence Community as uncomplicated as possible, without any administrative burdens. With the aim to have a clearly defined role of the Community in respect to the Governing Board, we propose to insert **“and the structure of the Community”** into the last sentence of paragraph (6):

*“The requirements, the number of representatives **and the structure of the Community** shall be further specified by the Governing Board.”*

- article 13 (3) cb) - With the aim to clearly establish in legal way that this provision is relating only to “joint actions” we propose the following wording: **“lay down and adopt the conditions for joint actions within the framework of the regulations establishing Horizon Europe and the Digital Europe Programme in accordance with the decisions referred to in point (ca) of this paragraph;”**

- article 26 (1) – We propose to delete a newly added wording:

“also through redeployment of staff.”

We believe that there should not be any barriers for hiring new staff. We are convinced that principles of open, transparent and non-discrimination conditions will guarantee the most capable staff.

- article 31 (7) – We propose to delete a newly added sentence:

“The human resources required in the Centre shall be met inter alia by redeployment of posts from Union institutions, bodies, offices and agencies.”.

We believe that there should not be any barriers for hiring new staff. We are convinced that principles of open, transparent and non-discrimination conditions will guarantee the most capable staff.

FINLAND

Comments of Finland to the Document 5341/3/20 Rev3 - Key points

Seat of the Centre (Rec 7a, Art 1): We propose: Describe only the decision procedure in the Recital, state the location in Article 1, leave the Article in square brackets until the location is agreed.

Centre considered as partnership (Rec. 9c): Remove the sentence from the text of the recital due to apparent incompliance with Horizon Europe partnership approach. CLS view to our understanding is that this part of the recital is not necessary for the Commission to be able to finance the functioning of the Centre from DEP and HE programmes.

Implementing cyber parts of HE and DEP (Rec 15): Change the order: implementing them primarily according to work programmes of those programmes, following the Centre's own multiannual and annual work programmes.

Autonomous manner (Art 3-1): We find it important that the Article refers clearly to **the strategic autonomy of the Union** rather than to that of the Centre and the Network. FI proposes the following text formulation:

The Competence Centre and the Network shall help the Union to:

- a) *strengthen **its strategic autonomy in cybersecurity** by retaining and developing the Union's research, technological and industrial capacities and capabilities necessary to enhance trust and security in the Digital Single Market;*

Revocation of registration of national entities to CCC (Art 8-4): The Center should assess only compliance of national entity with financial regulation, the NCC should assess compliance with this Regulation.

Voluntary contributions (Art 21-23): We propose the removal of the word '**voluntary**' from 4 paras/subparas to be compliant and consistent with earlier removal of the word from Art 21-1b and with HE funding rules for joint actions.

Funding from other programmes than HE and DEP (Art 22): The paragraph should be in square brackets due to MFF negotiations still continuing.

Assets in case of dissolution of the Centre (Art 23-8):

The meaning of the paragraph seems to have become the opposite to intended with the word 'not': "when the ~~Competence~~ Centre is wound up, any excess revenue over expenditure shall ~~not~~ be paid to the ~~participating~~ **contributing** members of the ~~Competence~~ Centre."

Commented [A65]: F1 – wondering if the purpose of this paragraph became the opposite to intended with the word 'not' left in the text.

MORE DETAILED TRACK-CHANGES COMMENTS IN THE REGULATION TEXT BELOW.

- (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 **research and technological capacities to secure its Digital Single Market as outlined by the Commission in its Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions entitled "A Digital Single Market Strategy for Europe"**, and in particular to protect critical networks and information systems and to provide key cybersecurity services.

- (6) A wealth of expertise and experience in cybersecurity research, technology and industrial development exists in the Union, but the efforts of industrial and research communities are fragmented, lacking alignment and a common mission, which hinders competitiveness in this domain. These efforts and expertise need to be pooled, networked and used in an efficient manner to reinforce and complement existing research, technology and industrial capacities at Union and national levels.
- (7) The Council Conclusions adopted in November 2017 called on the Commission to provide rapidly an impact assessment on the possible options to create a Network of Cybersecurity Competence Centres, **together with the a European Cybersecurity Research and Competence Centre and propose by mid-2018 the relevant legal instrument.**
- (7a) **The decision regarding the seat of the European Cybersecurity Industrial, Technology and Research Centre (the "Centre") will be taken by common agreement between the Representatives of the Governments of the Member States. ~~It is imperative for the proper and efficient performance of its tasks, for staff recruitment and retention and for enhancing the efficiency of networking and coordination activities that the Centre be based in an appropriate location, among other things providing appropriate transport connections and facilities for spouses, partners and children accompanying members of staff of the Centre. The necessary arrangements should be laid down in an agreement between the Centre and the host Member State concluded after obtaining the approval of the Governing Board of the Centre.~~**

Commented [A66]: F1 – In our view, recital (7a) should only describe the **procedure for deciding the location of the Centre.**

The location of the seat could remain in Art 2, but in square brackets, if it has not been agreed by the time of agreement on other parts of this Regulation.

(8) The ~~Competence~~ Centre should be the Union's main instrument to pool investment in cybersecurity research, technology and industrial development and to implement relevant projects and initiatives together with ~~the a Cybersecurity Competence Network of National~~ **Coordination Centre ("the Network")**.

Commented [A67]: Editorial suggestions:

FI - Divide Recital (8) into three recitals for easier readability and to separate three different issues.

(8ab): proposed wording.

(8aa) **The Centre** ~~It~~ should deliver cybersecurity-related financial support from ~~the~~ Horizon Europe - **the Framework Programme for Research and Innovation established by Regulation 2020/... of the European Parliament and of the Council²⁸ ('the Horizon Europe programme')** and ~~the~~ Digital Europe programme established by Regulation 2020/... of the European Parliament and of the Council²⁹ ('the Digital Europe programmes'), and should be open to the European Regional Development Fund and other programmes where appropriate. This approach should contribute to creating synergies and coordinating financial support related to cybersecurity research, innovation, technology and industrial development and avoiding unnecessary duplication.

(8ab) **The Centre should not play an operational role or provide a operational technical assistance role. However, Upon request from a Member State, the Centre should be able to may provide expert advice to that Member State.**

²⁸ Regulation 2020/... of the European Parliament and of the Council, of ..., establishing Horizon Europe - the Framework Programme for Research and Innovation, laying down its rules for participation and dissemination (OJ ...) [2018/0224(COD)].

²⁹ Regulation 2020/... of the European Parliament and of the Council, of ..., establishing the Digital Europe programme for the period 2021-2027 (OJ ...) [2018/0227(COD)].

(8a) ~~The Competence Centre would benefit from the particular expertise~~ The experience and the broad and relevant stakeholders' representation built through the contractual public-private partnership on cybersecurity between the Commission and European Cyber Security Organisation ECSO Association during the duration of the Framework Programme for Research and Innovation (2014-2020) ("Horizon 2020"), established by Regulation (EU) No 1291/2013 of the European Parliament and of the Council³⁰, and the lessons learned from four pilot projects³¹ launched in early 2019 under Horizon 2020, ~~thereby building on the existing experience that has been set up by the contractual public-private partnership on cybersecurity,~~ ~~should be made use of for building up~~ the management of the Cybersecurity Competence Community, and the representation of the Cybersecurity Competence Community in the Centre.

Commented [A68]: FI – repetitive.

Formatted: Not Strikethrough

(9) The Centre should develop and monitor the implementation of a comprehensive and sustainable Cybersecurity Industrial, Technology and Research Agenda ~~Strategy~~ which will set out strategic recommendations and priorities for development and growth of the European cybersecurity ~~ecosystem~~ industrial, technological and research sector (the "Agenda"). The Agenda ~~should provide the basis for the annual and multi-annual work programme of the Centre. Furthermore, the Agenda~~ should be taken duly into account in particular within the ~~bi-annual and annual~~ planning and implementation of the Horizon Europe programme and the Digital Europe programme in the area of cybersecurity. The Agenda ~~could also serve be able to provide as~~ cybersecurity specific advice, where relevant, ~~for~~ the implementation of other Union programmes.

Commented [A69]: FI – We propose a more proactive wording in the recital than merely raising the possibility of the Centre benefiting from the experience and representation of ECSO and the four pilots.

³⁰ Regulation (EU) No 1291/2013 of the European Parliament and of the Council of 11 December 2013 establishing Horizon 2020 - the Framework Programme for Research and Innovation (2014-2020) and repealing Decision No 1982/2006/EC (OJ L 347, 20.12.2013, p. 104).

³¹ CONCORDIA, ECHO, SPARTA and CyberSec4Europe are the four winning pilot projects of the 2018 Horizon 2020 cybersecurity call "establishing and operating a pilot for a European Cybersecurity Competence Network and developing a common European Cybersecurity Research & Innovation Roadmap".

- PUBLIC
- (9a) When the Centre is preparing its annual work programme ("annual work programme"), it should inform the Commission on its co-funding needs based on the Member States' planned co-funding contributions to joint actions, in order for the Commission to take into account the Union matching contribution in the preparation of the draft general budget for the following year.
- (9b) Where the Commission prepares the ~~Horizon Europe W~~work programme of the ~~Horizon Europe~~ programme for matters related to cyber security, including in the context of its stakeholder consultation process and particularly before the adoption of that work programme, the Commission should take into ~~due~~ account the input of the ~~Centre Governing Board and Executive Director~~ and share ~~its~~ such input with the ~~Horizon Europe~~ Programme Committee of the Horizon Europe programme.
- (9c) In order to support its role in the area of cybersecurity and the involvement of the Network and to provide a strong governance role for the Member States ~~of National Coordination Centres~~, the Centre should be established as a Union body with legal personality. ~~To achieve its role, it should manage funding.~~ The Centre should perform a dual role by undertaking specific tasks in the area of cybersecurity industry, technology and research as laid down in Art 4 and 4a this Regulation and by managing cybersecurity related funding from several programmes at the same time – notably the Horizon Europe programme and the Digital Europe programme, and possibly even further Union programmes. Such management should be in line accordance with their ~~regulations~~ rules applicable to those programmes. ~~The Centre will therefore have a special nature~~ Nevertheless, considering that the funding for the functioning of the Centre would originate primarily from the [DEP] Digital Europe programme and the [Horizon Europe] funding programmes and in view of the absence of appropriate funding alternatives in those funding programmes, it is necessary that the Centre is considered as a partnership for the purpose of budget implementation, including the programming phase.

Commented [A70]: F1 – We suggest removing this sentence as it is not compliant with the Horizon Europe partnership approach, and funding for the functioning of the Centre should be possible even without this sentence in the recital.

(12a) ~~In addition to the necessary administrative capacity,~~ The National Coordination

Centres ~~should have the necessary administrative capacity and should either possess or have direct access to cybersecurity industrial, technological and research 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 and be in a position to effectively engage and coordinate with and coordinate Cybersecurity Competence Community members of the industry, the public sector, including authorities designated pursuant to the Directive (EU) 2016/1148 of the European Parliament and of the Council³², and the research community.~~

- (13) Where financial support is provided to National Coordination Centres in order to support third parties at the national level, ~~this that financial support should be passed on to relevant stakeholders beneficiaries~~ through cascading grant agreements.

Commented [A71]: F1 – For consistency with Art 7-1, the NCC should engage with and coordinate national members of the CCC (rather than coordinate [no object] with the listed sectors:

Art 6-4: ... It [NCC] ~~shall 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 Council⁴**, and the research community.

Art 7-1

The National Coordination Centres shall have the following tasks:

- (a) **acting as contact points at the national level for the Cybersecurity Competence Community to supporting the Competence Centre in achieving its objective and missions, and in particular in coordinating the Cybersecurity Competence Community through the coordination of its national members;**

³² 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).

- (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 **products and** solutions. At the same time the Competence Centre and the Network should ~~be at the service of~~ **promote the cybersecurity capability of the demand side industry, in particular by activities supporting** 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, for example, ~~in order to achieve~~ security-by-design. They should also support the deployment of cybersecurity products and solutions ~~and to the extent while promoting where possible, rely the implementation of~~ the European cybersecurity certification framework as defined by Regulation (EU) 2019/881 of the European Parliament and of the Council³³ ~~the Cybersecurity Act~~.

Commented [A72]: FI – we do not think that the Centre, Network and the Community should **disseminate cybersecurity products** that could even be (embedded in) physical products – and even disseminating cybersecurity **solutions** would be a more appropriate task for businesses. In our view, **to advance** – and possibly, **disseminate information on...** would suffice.

³³ 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 L151, 7.6.2019, p. 15).

- (15) The Competence Centre should have several key functions. First, the Competence Centre should facilitate and help coordinate the work of the European Cybersecurity Competence Network and nurture support the Cybersecurity Competence Community. The Centre should drive implement cybersecurity relevant parts of the Digital Europe programme and the Horizon Europe programme in accordance with its the Centre's multiannual work programme ("multiannual work programme") and the annual strategic work programme and the strategic planning process of the Horizon Europe programme by allocating grants, typically following a competitive call for proposals the cybersecurity technological agenda in accordance with its multiannual work programme and the annual work programme, and facilitate transfer of access to the expertise gathered in the Network and the Cybersecurity Competence Community and . Secondly, it should implement relevant parts of Digital Europe and Horizon Europe programmes by allocating grants, typically following a competitive call for proposals. Thirdly, the Competence Centre should facilitate support joint investment by the Union, Member States and/or industry.
- (16) The Competence Centre and the National Coordination Centres should stimulate and support the cooperation and coordination of the activities of the Cybersecurity Competence Community, which would involve a large, open, and diverse group of actors involved in cybersecurity technology. That Community should include in particular research entities, supply-side industries, demand-side industries, civil society groups in the area of cybersecurity and the public sector. The Cybersecurity Competence Community should provide input to the activities, and multiannual work programme and the annual work programme of the Competence Centre and it. It should also benefit from the community-building activities of the Competence Centre and the Network, but otherwise should not be privileged with regard to calls for proposals or calls for tender.

Commented [A73]: FI – The Centre should implement the cybersecurity relevant parts of DEP and HE primarily in accordance with the strategic planning process of those programmes while following the Centre's multiannual and annual work programmes.

Commented [A74]: FI – editorial, separate listed items with commas, and into two sentences. The word 'also' not needed.

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

Commented [A75]: F1 – editorial - we find the word 'all' excessive here.

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

~~(18a) This Regulation should not utilise resources from Horizon Europe to fund projects which have a focus on military applications.~~

(18b) The enhancement of dual use application of cybersecurity technologies for cybersecurity purposes is without prejudice to the civilian nature of this Regulation and should therefore reflect specificities of Member States in cases when cybersecurity policy is pursued by civil-military or military authorities, and ensure complementarity but not overlap to the cyber defence related funding instruments.

(19) ~~In order to ensure structured and sustainable collaboration, the relation between the Competence Centre and the National Coordination Centres should be based on a contractual agreement.~~

(20) Appropriate provisions should be made to guarantee the liability and transparency of the ~~Competence Centre~~.

Article 2

Definitions

For the purpose of this Regulation, the following definitions ~~shall~~ apply:

- (1) 'cybersecurity' means ~~the protection~~ **the activities necessary to protect** network and information systems, ~~the-users~~ **of such systems**, and other persons **affected by** ~~against~~ cyber threats;
- (1a) **'network and information system' means a network and information system as defined in point (1) of Article 4 of Directive (EU) 2016/1148;**
- (2) 'cybersecurity products and solutions' means ICT products, services or processes with the specific purpose of protecting network and information systems, ~~their~~ users **of such systems** and ~~other affected~~ persons **affected by** ~~from~~ cyber threats;
- (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;~~

- (4) ~~participating Member State contributing Member State~~ means a Member State which voluntarily contributes financially to the administrative and operational costs of the Competence Centre.
- (3) "joint actions" means an actions included in the **Centre's annual work programme** receiving Union financial support from the Horizon Europe programme and/or Digital Europe programme, as well as financial or in-kind support by one or more Member States, ~~to be~~ **which are-is** implemented via projects involving beneficiaries established in the Member States ~~which provide~~ **in-kind** financial or in-kind support to those beneficiaries ~~entities~~ stemming from those Member States.
- (4) "in-kind contribution **by Member States**" means those eligible costs, incurred by National Coordination Centres and other public entities when participating in projects funded through this Regulation, which are not financed by a Union contribution. ~~In the case of projects funded through Horizon Europe, eligible costs shall be calculated in line with Article 32 of the Regulation establishing Horizon Europe. In the case of projects funded through Digital Europe, eligible costs shall be calculated in line with the Financial Regulation.~~³⁴

Commented [A76]: F1 - editorial

Article 3

Mission of the ~~Competence~~ Centre and the Network

1. The ~~Competence~~ Centre and the Network shall help the Union to:
- (a) ~~retain and develop, in an autonomous manner, the Union's the~~ **strengthen its strategic autonomy in** cybersecurity ~~by retaining and developing its~~ **research,** technological and industrial capacities **and capabilities** necessary to ~~strengthen enhance~~ **trust and security in** ~~secure~~ the Digital Single Market;
- (b) increase the **global** competitiveness of the Union's cybersecurity industry and turn cybersecurity into a competitive advantage of other Union industries.

Formatted: Not Strikethrough

Commented [A77]: F1 – we find it important that the Article refers clearly to **the strategic autonomy of the Union** rather than to that of the Centre and the Network.

Formatted: Not Strikethrough

Formatted: Not Strikethrough

Commented [A78]: F1 – to avoid repeating the word 'strengthen'.

³⁴ **Reference to the Financial Regulation and other legislative acts.**

Article 4a

Tasks of the Centre

1. In order to fulfill the mission laid out in Article 3 and the objectives laid out in Article 4, the Centre shall, in close cooperation with the Network, have the following ~~strategic and implementation~~ tasks:

(a) strategic tasks, consisting of:

(1) developing and monitoring the implementation of a comprehensive and sustainable Cybersecurity Industrial, Technology and Research Agenda, which ~~will~~ shall set out strategic recommendations and goals for the development and growth of the European cybersecurity industrial, technological and research ~~sectorecosystem~~ (the “Agenda”);

(2) through the Agenda and the multiannual work programme, while avoiding any duplication of ~~efforts~~ activities with ENISA:

(i) defining priorities for its work on:

- ~~for its work on~~ the enhancement of cybersecurity research and innovation and its deployment,
- the development of cybersecurity industrial, technological and research capacities ~~and~~ capabilities, ~~skills~~ and infrastructure,
- the reinforcement of cybersecurity **industrial, technological and research** skills and training and
- the deployment of cybersecurity products and solutions, and

(ii) supporting cybersecurity industry, with a view to strengthening Union excellence, capacities and competitiveness on cybersecurity;

- (3)** ensuring synergies and cooperation ~~while avoiding duplication of activities~~ with relevant Union institutions, agencies and bodies such as ENISA ~~while avoiding any duplication of activities with such Union institutions, agencies and bodies;~~
- (4)** coordinating National Coordination Centres through the Network and ensuring regular exchange of expertise;
- (5)** ~~providing expert advice upon request from a Member State to that Member State;~~
- (6)** facilitating collaboration and sharing of expertise among relevant stakeholders, in particular members of the **Cybersecurity Competence Community**; ~~this may include financially supporting education, training, exercises and building up cybersecurity skills;~~
- (7)** facilitating the use of results from research and innovation projects in actions related to the development of cybersecurity products and solutions, seeking to avoid fragmentation and duplication of efforts and ~~to replicating~~ good cybersecurity practices and **cybersecurity** products and solutions, including those developed by **small and medium enterprises (SMEs)** and those based on open-source software; ~~Support to the deployment of cybersecurity products and solutions should to the extent possible rely on the European cybersecurity certification framework as defined by the Cybersecurity Act.~~
- (b)** implementation tasks, consisting of:
- (1)** coordinating ~~and administrating~~ the work of the Network and the **Cybersecurity Competence Community** in order to achieve the mission set out in Article 3, in particular supporting cybersecurity start-ups and SMEs in the ~~European~~ Union and facilitating their access to expertise, funding, investment and to markets;

- (2) establishing and implementing the Centre's annual work programme, by managing all the phases in the lifetime of the project, in accordance with the Agenda and the multiannual work programme, for the cybersecurity parts of:
- (i) cybersecurity parts of the Digital Europe programme established by Regulation No XXX and in particular actions related to Article 6 of Regulation (EU) No XXX [Digital Europe Programme],
 - (ii) joint actions receiving support from the cybersecurity parts of the Horizon Europe programme established by Regulation (EU) No XXX established by Regulation No XXX and in particular Section 2.2.6 of Pillar II of Annex I. of Decision No XXX on establishing the specific programme implementing Horizon Europe – the Framework Programme for Research and Innovation [ref. number of the Specific Programme], and in accordance with the multiannual strategic work programme of the Centre, and the strategic planning process of the Horizon Europe programme, and
 - (iii) other Union programmes when provided for in legal acts of the Union;
- (3) providing expert advice on cyber security to the Commission when it prepares its the draft annual work programmes pursuant to Article 11 of Council Decision (XXXX)³⁵ of the Council on establishing the specific programme implementing Horizon Europe for other than joint actions in the area of cybersecurity research and innovation;

Commented [A79]: F1 – misplaced – would be repetitive for (ii) here -> move to beginning of (2i)

³⁵ Council Decision ..., of ..., on establishing the specific programme implementing Horizon Europe – the Framework Programme for Research and Innovation (OJ ...) [2018/0225(COD)].

Article 6

Nomination of National Coordination Centres

1. By [date], each Member State shall nominate **an** entity to act as the National Coordination Centre for the purposes of this Regulation and notify it **without delay** to the **Governing Board of the Centre** ~~Commission~~. Such entity may be an entity already established in that Member State.
2. On the basis of **the nomination by a Member State of an entity which fulfils** the criteria laid down in paragraph 4, the ~~Commission~~ **Governing Board** shall ~~issue a decision within 6 months from the nomination transmitted by the Member State providing for the accreditation record/en list that~~ entity as a National Coordination Centre **no later than 3 months after the nomination or rejecting the nomination**. The list of National Coordination Centres shall be published by the **Centre Commission**.
3. Member States may at any time nominate a new entity as the National Coordination Centre for the purposes of this Regulation. Paragraphs 1 and 2 shall apply to **the** nomination of any new entity.
4. The ~~nominated~~ National Coordination Centre shall ~~have~~ **be a public sector entity or an entity with a majority of public participation performing public administrative functions under national law, including by means of delegation, subject to public law obligations and having** the capability to support the ~~Competence~~ Centre and the Network in fulfilling their mission laid out in Article 3 of this Regulation. ~~They~~ **It shall either possess or have direct access to research and technological expertise in cybersecurity, and be in a position. It shall should also have the capacity to effectively engage and coordinate** with **and coordinate Cybersecurity Competence Community members of/representing** the industry, the public sector, **including authorities designated pursuant to the Directive (EU) 2016/1148 of the European Parliament and of the Council³⁶**, and the research community. ~~They~~ **It shall also have the administrative capacity to manage funds.**

Commented [A80]: FI - editorial

Commented [A81]: FI – ref our comment on Recital 12a)

³⁶ 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).

Article 8

The Cybersecurity Competence Community

1. The Cybersecurity Competence Community shall contribute to the mission of the ~~Competence Centre and the Network~~ as laid down in Article 3 and enhance and disseminate cybersecurity expertise across the Union.
2. The Cybersecurity Competence Community shall, **on the one hand**, consist of industry, academic and non-profit research organisations, **other relevant civil society and** associations as well as public entities and other entities dealing with **cybersecurity** operational and technical matters **and, on the other hand, where relevant, actors of sectors having an interest in cybersecurity and facing cybersecurity challenges**. It shall bring together the main stakeholders with regard to cybersecurity **research**, technological and industrial capacities in the Union. It shall involve National Coordination Centres as well as Union institutions and bodies with relevant expertise, **such as ENISA**.
3. Only entities which are established within the Union may be ~~accredited~~ **registered** as members of the Cybersecurity Competence Community. They shall demonstrate that they **can contribute to the missions as set out in Article 3 and shall** have cybersecurity expertise with regard to at least one of the following domains:
 - (a) research **and innovation**;
 - (b) industrial **or product** development;
 - (c) training and education;
 - (d) **information security and/or incident response operations**;
 - (e) **scientific or technical partnerships or cooperation with academic and/or public authorities as defined under Article 2(3)**.

~~Furthermore they should comply with the relevant national security regulations.~~

4. The ~~Competence~~ Centre shall ~~accredit~~ **register** 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, ~~including an assessment on security grounds~~, of whether that entity meets the criteria provided for in paragraph 3 of this Article. **That assessment shall also take into account, where relevant, any national assessment on security grounds made by the national competent authorities.** A ~~registration -accreditation~~ shall not be limited in time but may be revoked by the ~~Competence~~ Centre at any time if ~~the Centre it~~ or the relevant National Coordination Centre considers that the entity does not fulfil the criteria set out in paragraph 3 of this Article ~~or~~ **for justified security reasons or if the Centre considers that the entity does not fulfil the** ~~it falls under the~~ relevant provisions set out in Article 136 of Regulation **(EU, Euratom) 2018/1046XXX [new financial regulation]**, or for justified security reasons.

Commented [A82]: FI – The NCC should assess compliance with this Regulation, the Centre only the compliance with the financial regulations.

CHAPTER III

FINANCIAL PROVISIONS

Article 21

Union and Member States' financial contribution

-1. The Centre shall be funded by the Union.

1. The Union's contribution to the ~~Competence~~ Centre to cover administrative costs and operational costs shall comprise the following:
 - a) [EUR 1 981 668 000] from the Digital Europe programme, including up to [EUR 23 746 000] for administrative costs;
 - b) an amount from the Horizon Europe programme, including for administrative costs, **for joint actions, which shall be equal to the amount contributed voluntary by Member States pursuant to paragraph 5 of this Article 21(5) and but not exceed the amount determined in the strategic planning process of the Horizon Europe programme** ~~to be determined by taking into account the strategic planning process~~ to be carried out pursuant to Article 6(6) of Regulation XXX [Horizon Europe Regulation] **and the multiannual work programme and the annual work programmes of the Centre.**
2. The maximum Union contribution shall be paid from the appropriations in the general budget of the Union allocated to [Digital Europe Programme] and to the specific programme implementing Horizon Europe, established by Decision XXX.
3. The ~~Competence~~ Centre shall implement cybersecurity actions of [Digital Europe Programme] and [Horizon Europe Programme] in accordance with point (c)(iv) **of the first subparagraph** of Article 62 **(1)** of Regulation (EU, Euratom) ~~XXX²³~~ **(the Financial Regulation) 2018/1046.**
54. ~~The Union financial contribution shall not cover the tasks referred to in Article 4(8)(b).~~ **Contributions from Union programmes other than those referred to in paragraphs 1 and 2 above that are part of a Union co-financing to a programme implemented by one of the Member States shall not be accounted for in the calculation of the Union maximum financial contribution referred to in paragraphs 1 and 2) above.**
65. ~~Member States can make voluntary financial contributions for joint action with the Union, paid in instalments and in kind contributions consisting of costs incurred by~~

Commented [A83]: FI – remove the square brackets. However, if there is a formulation for this kind of of cap for funding already appearing in some other piece of EU legislation, that could possibly be reused here.

~~National Coordination Centres and beneficiaries in implementing actions that are not reimbursed by the Centre.~~

Voluntary contributions made by one or more Member States for joint actions with the Union may take the form of financial or in-kind contributions.

Financial contributions by Member States may take the form of support by Member States provided to participants in joint actions.

In-kind contributions by Member States shall consist of eligible costs incurred by National Coordination Centres and other public entities when participating in projects funded through this Regulation less any Union contribution to those costs. In the case of projects funded through Horizon Europe, eligible costs shall be calculated in line with Article 32 of the Regulation establishing Horizon Europe. In the case of projects funded through Digital Europe, eligible costs shall be calculated in line with the Financial Regulation (EU, Euratom) 2018/1046.

The envisaged amount of total Member States' ~~voluntary~~ contributions, including for administrative costs, to joint actions under the Horizon Europe Framework programme shall be determined in order to be taken into account in ~~as part of the~~ strategic planning process of the Horizon Europe programme to be carried out pursuant to Article 6(6) of Regulation XXX [Horizon Europe Regulation], with input from the Governing Board of the Centre.

For actions under the Digital Europe programme, notwithstanding Article 15 of the [Regulation establishing the Digital Europe Programme], the Member States may make a contribution to the costs of the ~~Competence~~ Centre that are co-financed from the Digital Europe programme that is lower than the amounts specified in [Article 21(1)(a**b**) – reference to be checked] of this Regulation.

Commented [A84]: FI – The word 'voluntary' should be removed from here in consistence with the removal from Art 21-1b.

Article 22

Contributions of participating Member State contributing of Member States

1. The participating Member States shall make a total contribution to the operational and administrative costs of the Competence Centre of at least the same amounts as those in Article 21(1) of this Regulation.

7.1a. Member States' co-funding of actions supported by Union programmes other than Horizon Europe and Digital Europe ~~could~~ shall be considered as contributions when as those actions are in the remit of the Centre's missions and tasks.

8.2. For the purpose of assessing the contributions referred to in paragraph 1 of this Article and in point (b)ii of Article 23(3), the costs shall be determined in accordance with the usual cost accounting practices of the Member States concerned, the applicable accounting standards of ~~that~~ Member State, and the applicable international accounting standards and international financial reporting standards. The costs shall be certified by an independent external auditor appointed by the Member State concerned. The valuation method may be verified by the Competence Centre should there be any uncertainty arising from the certification.

9.3. Should any ~~participating~~ Member State be in default of its commitments concerning its financial ~~and/or in-kind~~ contribution **pursuant to joint actions**, the Executive Director shall put this in writing and shall set a reasonable period within which such default shall be remedied. If the situation is not remedied within that period, the Executive Director shall convene a meeting of the Governing Board to decide whether the defaulting participating Member State's right to vote is to be revoked or whether any other measures are to be taken until **that Member State meets** its obligations ~~have been met~~. The defaulting Member State's voting rights **concerning joint actions** shall be suspended until the default of its commitments is remedied.

Commented [A85]: FI – contributions to what?

Commented [A86]: FI –

Para 7.1a. should be put in square brackets, because this topic of synergies between MFF programmes is part of the MFF discussions where agreement has not been reached yet. The text should be re-visited when the MFF agreement has been found.

- 10.4. The Commission may terminate, proportionally reduce or suspend the Union's financial contribution to ~~the Competence Centre~~ **joint actions** if the ~~participating-contributing~~ Member States do not contribute, contribute only partially or contribute late with regard to the contributions referred to in **point (b) of paragraph 1.**
- 11.5. The ~~participating-contributing~~ Member States shall report by 31 January ~~of~~ each year to the Governing Board on the value of the contributions referred to in paragraphs ~~4~~ **5** for **joint action with the Union** made in each of the previous financial year.

Article 23

Costs and resources of the Competence Centre

1. ~~The Competence Centre shall be jointly funded by the Union and Member States through financial contributions paid in instalments and contributions consisting of costs incurred by National Coordination Centres and beneficiaries in implementing actions that are not reimbursed by the Competence Centre.~~
2. The administrative costs of the Competence Centre shall not exceed EUR [number] and shall be covered by means of financial contributions ~~divided equally~~ on an annual basis ~~between from the Union and the participating Member State.~~ **Additional contributions shall be made by contributing Member States in proportion to their voluntary contributions to joint actions between the Union and Member States.** If part of the contribution for administrative costs is not used, it may be made available to cover the operational costs of the Competence Centre.
3. The operational costs of the Competence Centre shall be covered by means of:
 - (a) the Union's financial contribution;
 - (b) voluntary **financial and in-kind** contributions from the ~~participating-contributing~~ Member States **in case of joint actions between the Union and Member States in the form of:**
 - i. ~~Financial contributions; and~~

Commented [A87]: FI- editorial - Check the number of the Article.

Commented [A88]: FI – the word 'voluntary' should be removed from here in consistence with removal from Art 21 (1b).

Commented [A89]: 'Voluntary' should be removed from here as well, in consistence with the removal from Art 21 (1b). Most of the contributions might be voluntary, but not all, like in Horizon Europe joint actions.

ii. ~~where relevant, in-kind contributions by the participating contributing Member States. A contributing Member State's in-kind contribution to a given action supported by the Centre shall consist of the relevant costs incurred by the National Coordination Centres and beneficiaries established in that Member State in implementing indirect actions less the contribution of the Competence Centre and any other Union contribution to those costs. The Governing Board shall specify an operational methodology for calculating the in-kind contributions of Member States;~~

4. The resources of the ~~Competence~~ Centre entered into its budget shall be composed of the following contributions:

- (a) **the Union's financial contributions to the operational and administrative costs;**
- (b) ~~participating contributing~~ Member States' **voluntary** financial contributions to the administrative costs in case of joint actions ~~between the Union and Member States;~~
- (c) ~~participating contributing~~ Member States' **voluntary** financial contributions to the operational costs **in case of joint actions between the Union and Member States;**
- (d) any revenue generated by the ~~Competence~~ Centre;
- (e) any other financial contributions, resources and revenues.

5. Any interest yielded by the contributions paid to the ~~Competence~~ Centre by the ~~participating contributing~~ Member States shall be considered to be its revenue.

6. All resources of the ~~Competence~~ Centre and its activities shall be aimed to achieve ~~to~~ the objectives set out in Article 4.

Commented [A90]: FI – see the previous comment.

Commented [A91]: Refers to joint actions where the Centre participates with voluntary financial contributions from Member States?

7. The ~~Competence~~ Centre shall own all assets generated by it or transferred to it for the fulfilment of its objectives **without prejudice to Article 13(3)(cb).**
8. Except when the ~~Competence~~ Centre is wound up, any excess revenue over expenditure shall ~~not~~ be paid to the ~~participating-contributing~~ members of the ~~Competence~~ Centre.

Commented [A92]: F1 – wondering if the purpose of this paragraph was the opposite.

Article 24

Financial commitments

The financial commitments of the ~~Competence~~ Centre shall not exceed the amount of financial resources available or committed to its budget by its members.

Article 25

Financial year

The financial year shall run from 1 January to 31 December.

Article 26

Establishment of the budget

1. Each year, the Executive Director shall draw up a draft statement of estimates of the ~~Competence~~ Centre's revenue and expenditure for the following financial year, and shall forward it to the Governing Board, together with a draft establishment plan **as referred to in point (g) of Article 13(3).** Revenue and expenditure shall be in balance. The expenditure of the ~~Competence~~ Centre shall include the staff, administrative, infrastructure and operational expenses. Administrative expenses shall be kept to a minimum, **also through redeployment of staff.**

SWEDEN

General comments on CCCN

Sweden can accept the proposal for a new agency CCCN with these general conditions.

- Mandatory contributions cannot be accepted by SE. Financial contribution from MS should be exception and not rule.
- All MS should have a vote in GB. All MS contribution should be voluntary and not affect MS possibilities to contribute and participate in decision taking in Governing Board (GB) and other fora.
- The centre should not work with defence issues.

Specific comments on the text

Recitals

Recital 7a: SE supports the text and suggest that the brackets are removed.

Recital 8: Comment given also on March 11: SE asks for clarification of last sentence and why it has been added. The same holds for Article 4a.1.a5. If it is advice connected to R&D, and R&I it is acceptable. It should clarify that the Centre should not have an operative role. SE suggest that it is added that the providing expert advice within the scope of the Center's mandate upon request from a Member State to that Member State.

Recital 9. Comment also given on March 11 and on February 26. It is SE*s view that the CCCN agenda should be for the activities of the centre, not for HE and DEP Even if there is a clarification in Recital 15 and Article 13 it should be stated also here. SE accept the reference to that HE and DEP should take the agenda into account in their planning.

Recital 18: Also, DEP should be mentioned regarding the comment on” exclusive focus on civil application”

Articles

Articles 1:1–5. Regarding location of the Centre. SE will assess all proposals and following that decide on the one SE assessed to be the best choice.

Article 4a 1 (a) 5: Comment also given on March 11: SE agrees that the centre should provide expert advice if it refers to R&D, and R&I. But the centre should not be an operative support function. The same comment is given on Recital 8. All other text in Article 4a is acceptable for SE, but it needs rewriting to be clear on what text belongs to what heading. We suggest that the text is written as: “providing expert advice within the scope of the Center's mandate upon request from a Member State to that Member State”;

Article 8.4: Sweden does not agree with the text as it is formulated now. It is our opinion it's only the National Coordination Center who made the accreditation, that has the right to revoke the it. The Center cannot by itself take the decision to revoke the "accreditation" since its not within the mandate of the center to do. The wording of art. 8.4 as it currently stands is in our opinion, in violation of TFEU art.4.2 when it talks about national security concerns, because if there are security concerns the EU or a Center does not have competence in this field to make any decision.

Sweden therefore suggest the following wording: The Centre shall register entities 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, of whether that entity meets the criteria provided for in paragraph 3 of this Article. That assessment shall also take into account, where relevant, any national assessment on security grounds made by the national competent authorities. A registration shall not be limited in time but may be revoked at any time if the parent National Coordination Centre considers that the entity does not fulfil the criteria set out in paragraph 3 of this Article or falls under the relevant provisions set out in Article 136 of Regulation (EU, Euratom) 2018/1046XXX or for justified security reasons.

Article 13.3.L: Comments also given on March 11: It should be clarified that it is not only in accordance with the Agenda, but also according to the work programmes of HE and DEP. Although it might be stated in other recitals and articles it must be included also in Article 13.3. L

Article 15: Comment given also on March 11: SE is opposed to giving the Union 50 percent of the votes in cases relating to using Union funds. Voting for these should be the same as for other decisions, one vote for each partner.