Council of the European Union
General Secretariat

Interinstitutional files:
2018/0328(COD)

Brussels, 17 February 2020

WK 1788/2020 ADD 2

LIMITE

CYBER	**CSC**
TELECOM	**CSCI**
CODEC	**IND**
COPEN	**JAI**
COPS	**RECH**
COSI	**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: To:	General Secretariat of the Council Delegations
N° prev. doc.:	5341/1/20 REV 1
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 by HU, FI and SE

Delegations will find in Annex comments from HU, FI and SE delegations on the above-mentioned subject (doc. 5341/1/20 REV 1).

TABLE OF CONTENT

HUNGARY

(8a) **The ~~Competence~~ Centre should benefit from the ~~particular~~ ~~expertise~~ experience and the broad and relevant stakeholders' representation built through the contractual public-private partnership on cybersecurity during the duration of Horizon 2020, and the lessons learned from four pilot projects[1] 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 Community, and the representation of the 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 (the "Agenda"). The Agenda should be taken duly into account in particular within the (bi-) annual planning and implementation of the Horizon Europe and Digital Europe Programme in the area of cybersecurity. The Agenda ~~should~~ may also provide cybersecurity specific advice, where relevant, to the implementation of other Union programmes.**

(9a) **When the Centre is preparing its 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 EU matching contribution in the preparation of the draft general budget for the following year.**

(9b) **Where the Commission prepares the Horizon Europe Work Programme for matters related to cyber security, including in the context of its stakeholder consultation process and particularly before the adoption of the Work Programme, the Commission should take into ~~due~~ account the input of the Centre ~~Governing Board and Executive Director~~ and share its input with the Horizon Europe Programme Committee.**

Commented [A1]: We find the wording too strong; "…benefit from the experience…would be enough. Additionally, we support FI suggestion to name the cPPP also as the 4 pilot projects are listed.

Formatted: Strikethrough, Kern at 12 pt, Highlight

Formatted: Highlight

Formatted: Highlight

Commented [A2]: With regard to the limited scope of the Centre, we would like to see "may" instead of "should".

Formatted: Strikethrough, Kern at 12 pt, Highlight

Formatted: Highlight

Formatted: Highlight

Formatted: Highlight

[1] **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".**

(9c) In order to support its role in the area of cybersecurity and to provide a strong governance role for the Member States and the involvement of a Network 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 as laid down in Art 4 and 4a and by managing cybersecurity related funding from several programmes at the same time – notably Horizon Europe and Digital Europe, and possibly even further EU programmes, in line with their regulations. ~~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] and [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.

~~(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"), made up of National Coordination Centres in 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.

Commented [A3]: What does it mean in practice? Might be possible that the Centre will manage further Union fundings beside HE and DEP in the future?

Formatted: Highlight

Formatted: Highlight

Formatted: Highlight

Formatted: Strikethrough, Kern at 12 pt, Highlight

Commented [A4]: This sentence sounds weird and adds nothing to the explanation about the Centre's legal nature.

Formatted: Strikethrough, Kern at 12 pt, Highlight

(14) ~~Emerging technologies such as artificial intelligence, Internet of Things, high-performance computing (HPC) and quantum computing, blockchain and concepts such as secure digital identities create at the same time new challenges for cybersecurity as well as offer solutions. Assessing and validating the robustness of existing or future ICT systems will require testing security solutions against attacks run on HPC and quantum machines.~~ The ~~Competence~~ Centre, the Network and the Cybersecurity Competence Community should help advance and disseminate the latest cybersecurity solutions. At the same time the ~~Competence~~ Centre and the Network should ~~be at the service of~~ **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.**

(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 the Cybersecurity Competence Community. The Centre should ~~drive~~ **implement relevant parts of the Digital Europe and Horizon Europe programmes in accordance with its multiannual and annual ~~strategic~~ work programme and the strategic planning process of Horizon Europe 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.

Commented [A5]: We find still unclear how the Network will act in practice. What is meant by Network? Using the word "" in the text supposes an institutionalized framework. if that's the case the substance behind the Network should be filled. Otherwise we prefer creating a lighter structure and not having something which than will require more institutionalized framework.

Formatted: Highlight

Formatted: Highlight

~~(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" mean actions included in the Centre's Work Programme receiving Union financial support from the Horizon Europe and/or Digital Europe Programmes as well as financial or in-kind support by one or more Member States, to be 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.[2]

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 **Union's** ~~the~~ cybersecurity **research,** technological and industrial capacities ~~**in an autonomous manner** necessary~~ to **strengthen trust and security in** ~~secure~~ **the** Digital Single Market;

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

[2] Reference to the Financial Regulation and other legislative acts.

Commented [A6]: How could only one MS launch a joint action? Joint action should suppose at least two MS, but rather more, otherwise it could be barely considered as a European initiative.

Commented [A7]: To make the text more ease of reading we suggest to modify the text in this way.

Formatted: Highlight

Formatted: Highlight

Formatted: Highlight

Formatted: Font: (Default) Times New Roman, Romanian, Highlight

Formatted: Highlight

Formatted: Justified, Indent: Left: 0.5 cm, First line: 0 cm

Formatted: Highlight

Commented [A8]: We would like to see the green part deleted from the text.

Formatted: Strikethrough, Kern at 12 pt, Highlight

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.

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

3. ~~**and by**~~ **stimulating cooperation and coordination within National Coordination Centres and 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;~~

Commented [A9]: See our comment at recital 14.

Formatted: Strikethrough, Highlight

Commented [A10]: This part is already included in Article 3. Mission of the Centre.

Formatted: Strikethrough, Highlight

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 Art. 21(5) and not exceed [the amount determined in the strategic planning process]** ~~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 strategic and annual work programmes of the Centre**.

Commented [A11]: This paragraph should be harmonized and motified in accordance with the definition of joint actions laid down in Article 2. Since joint actions could be financed from HE and DEP too, it should be noted here equally.

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 Centre~~s~~ 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**;

Commented [A12]: What does "operational" mean?

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.

FINLAND

(8a) **The ~~Competence~~ Centre should benefit from the particular ~~expertise~~ experience and the broad and relevant stakeholders' representation built through the contractual public-private partnership on cybersecurity during the duration of Horizon 2020, and the lessons learned from four pilot projects[3] 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 Community, and the representation of the Community in the Centre.**

Commented [A13]: Add name of the partnership.

(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 (the "Agenda"). The Agenda should be taken duly into account in particular within the (bi-) annual planning and implementation of the Horizon Europe and Digital Europe Programme in the area of cybersecurity. The Agenda should also provide cybersecurity specific advice, where relevant, to the implementation of other Union programmes.**

(9a) **When the Centre is preparing its 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 EU matching contribution in the preparation of the draft general budget for the following year.**

(9b) **Where the Commission prepares the Horizon Europe Work Programme for matters related to cyber security, including in the context of its stakeholder consultation process and particularly before the adoption of the Work Programme, the Commission should take into ~~due~~ account the input of the Centre ~~Governing Board and Executive Director~~ and share its input with the Horizon Europe Programme Committee.**

---

[3] **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".**

(9c) In order to support its role in the area of cybersecurity and to provide a strong governance role for the Member States and the involvement of a Network 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 as laid down in Art 4 and 4a and by managing cybersecurity related funding from several programmes at the same time – notably Horizon Europe and Digital Europe, and possibly even further EU programmes, in line with their regulations. ~~The Centre will therefore have a special nature. Nevertheless, e~~Considering that the funding for the functioning of the Centre would originate primarily from the [DEP] and [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 [A14]: This description should apply also to the rest of the recital, and be placed at the end of the recital. However, we think that the special nature of the Centre is evident from the text and this mention could be left out.

Furthermore, the passage after the word 'Nevertheless' appears as an argument minimizing the special nature of the Centre, and could be replaced with 'furthermore' or the sentence deleted as track-change-marked here.

~~(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"), made up of National Coordination Centres in 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 delegation, subject to public law obligations** selected by Member States. In addition to the necessary administrative capacity, Centres should ~~either~~ possess or have ~~direct~~ access to cybersecurity **Industrial, Technology 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 Council~~[4], and the research community.

(12a) The functions of National Coordination Centre in a given Member State can be carried out by the same entity also fulfilling other functions created under Union law, such as that of a national competent authority and/or single point of contact in the meaning of the NIS Directive~~, any~~ or other Union Regulation, or digital innovation hub in the meaning of the Digital Europe Programme.

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

~~[4] 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 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.**

Commented [A15]: The Centre and the Network could play a more active role in supporting the development of cybersecurity capability of demand side industry than be at their service supporting developers and operators in the said sectors to respond to cybersecurity challenges.

However, we recognize the preference of many MS to focus the work of the Centre on cybersecurity 'supply side' sector rather than the ecosystem.

(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 the Cybersecurity Competence Community. The Centre should ~~drive~~ **implement relevant parts of the Digital Europe and Horizon Europe programmes in accordance with its multiannual and annual ~~strategic~~ work programme and the strategic planning process of Horizon Europe 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.

Additional Presidency Compromise Proposals

RECITALS

(7b) **The Commission Impact Assessment stated that the EU still lacks sufficient technological and industrial capacities to autonomously secure its economy and critical infrastructures and to become a global leader in cybersecurity field. The assessment identified the following problems: there is an insufficient level of strategic and sustainable coordination and cooperation between industries, cybersecurity research communities and governments; the EU suffers from subscale investment and limited access to cybersecurity know- how, skills and facilities across Europe; and few European cybersecurity research and innovation outcomes are translated into marketable solutions and widely deployed across the economy. The analysis concluded that the option of creating a Cybersecurity competence network together with a European Cybersecurity Industrial, Technology and Research Competence Centre with a dual mandate to pursue measures in support of industrial technologies as well as in the domain of research and innovation is best suited to achieve the goals of the initiative while offering the highest economic, societal, and environmental impact and safeguarding the Union's interests.**

(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 relevant Union stakeholders, as well as its collection of inputs through its tasks, ~~for instance on cybersecurity certification and standardisation~~ the European Union for Cybersecurity (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.

ARTICLES

Article 4a

Tasks of the Centre

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:

1. Strategic tasks

(aa) Developing and monitoring the implementation of a comprehensive and sustainable Cybersecurity Industrial, Technology and Research Agenda which will set out strategic recommendations and goals for development and growth of the European cybersecurity ecosystem (the "Agenda");

(a) Through the Agenda and the multiannual work programme defining priorities **for its work on** enhancing cybersecurity research and its deployment, developing cybersecurity capacities and capabilities, skills and infrastructure and supporting cybersecurity industry, with a view to strengthening European excellence, capacities and competitiveness on cybersecurity;

(b) Ensuring synergies and cooperation with relevant Union institutions, agencies and bodies such as ENISA;

(bc) Coordinating National Coordination Centres through the Network and ensuringe regular exchange of expertise;

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

(d) Facilitating the use of results from research and innovation projects in actions related to the development of cyber products and solutions, seeking to avoid fragmentation and duplication of efforts and to replicate good cybersecurity practices, products and solutions, including those developed by 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.~~

…..

Article 6

Nomination of National Coordination Centres

…

2. On the basis of **the nomination by a Member State of an entity which fulfils** the criteria laid down in paragraph 4, the **Governing Board** shall **enrol** that entity as a National Coordination Centre **no later than 3 months after the nomination**. The list of National Coordination Centres shall be published by the **Centre.**

Commented [A16]: We wonder if the word 'list' could be used here, if what the Centre publishes is a 'list' rather than a register.

…

6. The National Coordination Centres Network shall be composed of all the National Coordination Centres nominated by the Member States. **Coordination of the Network shall be done by the Centre.**

Commented [A17]: This is already in article 4a (bc), which is a better place for this clause if needed. The coordination of the NCCs should be light.

Article 7

Tasks of the National Coordination Centres

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

a) **acting as contact point at the national level for the Cybersecurity Competence Community to** support the Centre in achieving its objective **and missions**~~**.**~~

a1) ~~in particular in~~ coordinating the Cybersecurity Competence Community **through the coordination of its national members**;

Commented [A18]: Listing this as a separate task would make the article easier to read.

aa) providing expertise and actively contributing to the strategic planning of the activities according to Article 4a taking into account relevant challenges for cybersecurity from different sectors;

….

Article 8

The Cybersecurity Competence Community

…

3. Only entities which are established within the Union may be **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;

   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 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, on whether that entity meets the criteria provided for in paragraph 3. A **registration** shall not be limited in time but may be revoked by the Centre at any time if it or the relevant National Coordination Centre considers that the entity does not fulfil the criteria set out in paragraph 3**,** ~~ or it~~ falls under the relevant provisions set out in Article 136 of Regulation XXX [new financial regulation**], or for justified security reasons**.

6. The Community shall designate its own representatives to ensure an efficient and regular dialogue and cooperation with the Centre. Representatives of the Community shall have expertise with regard to cybersecurity research, industrial development, professional services or the deployment thereof. The representation of the Community should be balanced between scientific, industrial and civil society entities, demand and supply side industries, large and small and medium enterprises, as well as in terms of geographical provenance and gender. The requirements and number of representatives shall be further specified by the Governing Board;

Commented [A19]: If references are made to compliance of these entities with relevant national security regulations, it could be made here: …and compliant with relevant…

Commented [A20]: list?

Commented [A21]: Listing an entity as a member of the Cybersecurity Competence Community…

7. **The Community shall through its representatives provide to the Executive Director and the Governing Board strategic advice and input for drafting the Agenda, annual and multiannual work programme within the deadlines set by the Governing Board. They should also promote and collect feedback on the annual and multiannual work programme of the Centre.**

Article 13

Tasks of the Governing Board

...

3. The Governing Board shall take the necessary strategic decisions, in particular:

a) develop and adopt the comprehensive Agenda encompassing goals for a sustainable development of the European cybersecurity research, technological and industrial sector and monitor its implementation;

SWEDEN

SE is one of those countries that has been hesitant to create a new Union body when there are other agencies that can execute the tasks. On the assumption that we now are working on the present proposal with the creation of a new organization to handle these issues our views on the text are given below.

General Swedish views on how a centre (as a separate organisation) should work are the following:

- 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 Swedish views on the proposed regulation (5341/1/20 Rev 1 and 5889/20):

Recitals

Recital 9: SE:s view from HWG 4 February remains. The strategy should be for the centre's work, not for the "European ecosystem".

SE:s view remains that it is not HE/DEP or other programmes that should take the Agenda into consideration, but that centre should when working out the Agenda base it on the work in programme committees in HE/DEP in order not to undermine the work of the programme committees. An Agenda must also take the strategy of ENISA into consideration. Generally, the reference to the Agenda is made together with the multi-annual work programme which indicates that the differences are very small.

Recital 9 c: SE agrees that the reference to financing from DEP and HE can be described as a partnership. SE question what the" special nature" of the centre means (if this remains in the text) and wants this to be clarified in the text.

Recital 15: SE agrees but want it to be clarified in the text what it means for projects (Joint Actions) funded by DEP and HE respectively (article 15.2.a referring to article 13.3.cb).

Recital 18: SE wants a clearer statement on the non-military nature of the centre and its work. Synergies and transfer of knowledge is acceptable, but the centre should not have any specific work on cyber defence.

Recital 18 a: SE suggests that also DEP should be referred to in the same way.

Recital 28a: It is important for SE that national financing of NCC can be counted as in-kind contribution to the centre. We think that this should be stated in an article rather than in a recital (which is not legally binding?).

Articles

Article 1:3. SE accept that the chair wants to handle to localization of the centre separately. The question still remains, until then, how it will be assigned and how the staff can be reallocated from Commission and other Union bodies (article 31.7), especially if the centre is to be located outside of Brussels.

Article 3.2a It needs clarification how this will be financed. The cooperation of the centre with MS, NCC's and ENISA is crucial for the efficiency of the work. Financing of this cannot be based on the voluntary contributions of MS.

Art 4 a.2 If this article remains SE maintain its earlier views on articles 4 a 2e and 2f. These are:

Article 4a 2 (e): SE asks how the competence can be assured when it is a specific competence requiring expertise and resources that is beyond the specific competence of the centre.

Article 4a 2 (f): SE is of the view that the clarification (earlier asked for by SE) that the centre will focus on civilian issues regarding HE and DEP are sufficient but that it still needs to be clarified that it also holds for issues beyond those finances by HE and DEP, that it should be clear that the centre only should focus on civilian issues.

Article 13 3aa: SE want it to be clarified what Union strategic autonomy is in this context. As described in the article it can also infringe on MS competence regarding national security, which SE cannot accept.

Articles 14–20: OK conditioned that it is clear that when referring to voting rules it is meant one country – one vote (article 15.2) and that voting weight is independent of financial contribution. It should also be clear that when there is a reference to Joint Actions in HE (article 15.2a) the described voting rules are only for the specific action jointly financed.

SE has suggested a cost analysis on the proposed centre in comparison to a smaller centre with only strategic tasks, or if the functions are entrusted to an existing organization, such as ENISA. Although we are willing to continue working on the present proposal we are of the opinion that such an analysis can be a way to ensure that we create the most cost-effective way to execute the tasks of the centre.