Council of the European Union
General Secretariat

Interinstitutional files:
2018/0328(COD)

Brussels, 14 February 2020

WK 1788/2020 ADD 1

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, 5889/20
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 EL, FR, AT and PL

Delegations will find in Annex comments from EL, FR, AT and PL delegations on the above-mentioned draft Regulation. These comments relate to the text set out in documents 5341/1/20 REV 1 and 5889/20 (Articles 4a, 6, 7, 8 and 13 as well as Recitals 7b and 21).

TABLE OF CONTENT

GREECE

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 the Network of National Coordination Centres ~~a Cybersecurity competence network~~ together with the ~~a~~ European Cybersecurity Industrial, Technology and Research ~~Competence~~ Centre empowered ~~with a dual mandate~~ to pursue measures in support of industrial technologies as well as in the domain of research and innovation represents the ~~is~~ best instrument capable ~~suited~~ to implement ~~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.

(27) ~~The Competence Centre should have an Industrial and Scientific Advisory Board~~ **The Community** ~~should~~ **will act also** as an advisory body ~~source of advice~~ ensur**ing** regular dialogue **of the Centre** with the private sector, consumers' organisations, **academia** and other relevant stakeholders. ~~The Industrial and Scientific Advisory Board should focus on issues relevant to stakeholders and bring them to the attention of the Competence Centre's Governing Board~~. The composition of the **Community** ~~Industrial and Scientific Advisory Board~~ and the tasks assigned to it, such as being consulted regarding the work **programme**, should ensure sufficient representation of stakeholders in the work of the ~~Competence~~ Centre.

Commented [AM1]: C3 Directorate/MFA: We do not have any objection to the suggested wording because it fully complies with the wording under section 2.2. (What are the problems to tackle?) of the Commission Impact Assessment [SWD(2018) 403 final].

Commented [AM2]: C3 Directorate/MFA: We suggest these alterations for reasons of accuracy and consistency with the wording under section 8 (Preferred option) of the Commission Impact Assessment [SWD(2018) 403 final].

Commented [AM3]: We do not have any objection to this deletion.

Commented [AM4]: We prefer the wording included in the previous version of the mandate (ST 5341/20) for reasons of consistency with Articles 3 and 8 of the present mandate, which lay down the mission and role of the Community.

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 and avoiding any duplication of efforts with ENISA;

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

(bc) Coordinating National Coordination Centres through the Network and ensure 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. ~~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.~~

2. Implementation tasks

Commented [AM5]: **C3 Directorate/MFA:** Any duplication of efforts of the Centre with ENISA should be avoided. ENISA is the competent EU Agency for Cybersecurity and therefore its leading role in the field of cybersecurity should be preserved.

Commented [AM6]: **C3 Directorate/MFA:** We do not have any objection to this addition.

Commented [AM7]: **C3 Directorate/MFA:** We do not have any objection to this deletion.

Commented [AM8]: **C3 Directorate/MFA**: We disagree on the suggested deletion because we are of the opinion that all research and innovation based products and solutions in the field of cybersecurity should conform with the European cybersecurity framework under the Cybersecurity Act. We remind that ENISA's major task is the establishment and maintenance of a European cybersecurity framework for ICT products, service and processes.

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

(b) Establish and implement the Centre's annual work programme, in line with the Agenda, for the cybersecurity parts of :

i) 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 Horizon Europe, and

iii) other Union programmes when provided for in legal acts of the Union.

(c) Provide expert advice on cyber security to the Commission when it prepares its draft annual work programmes pursuant to Article 11 of Decision (XXXX) of the Council on establishing the specific programme implementing Horizon Europe for other than joint actions in the area of cybersecurity research and innovation;

(d) In accordance with Article 6 of the Horizon Europe Framework programme and subject to the conclusion of a contribution agreement, 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. 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];

(e) Facilitate the acquisition of cybersecurity infrastructures – at the service of industries, the public sector and research communities, through voluntary contributions from Member States and EU funding for joint actions, in line with the Agenda, multiannual work programme and the annual work programmes. EU funding shall not be conditioned to voluntary funding from Member States;

(f) Without prejudice to the civilian nature of projects to be financed from Horizon Europe and Digital Europe Programme and in line with the respective program

regulations. enhance synergies and exchange of knowledge and coordination between the cybersecurity civilian and defence spheres.

3. **Monitor the fulfilment of the strategic goals set up in the Agenda and, whenever necessary, provide proposals for the enhancement of their realisation.**

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.**

…

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 [AM9]: C3 Directorate/MFA: We do not have any objection to these additions.

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** 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 Article 4a taking into account relevant challenges for cybersecurity from different sectors;

Commented [AM10]: C3 Directorate/MFA: We do not have any objection to this addition.

…

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.

Commented [AM11]: C3 Directorate/MFA: We do not have any objection to this addition.

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;

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

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.

2. The Governing Board shall adopt its rules of procedure. These 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 comprehensive Agenda encompassing goals for a sustainable development of the European cybersecurity research, technological and industrial sector and monitor its implementation;

aa) based on the Agenda adopt a multi-annual **work programme**~~,~~ containing **the development of a common strategic, industrial, technology and research roadmap, on the basis of the needs identified by Member States in cooperation with the Community that require the focus of Union's financial support, including key technologies and domains for the Union's 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 and Digital Europe programmes, in accordance with its multi annual work programme, and the strategic planning process of Horizon Europe ~~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, 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 the ~~FR~~**Financial Regulation**];

ca) in the line with the annual work programme adopt decisions ~~to~~ ~~dedicate~~ allocate funds from the EU budget to joint actions between the Union and Member States;

cb) without prejudice to the regulations establishing Horizon Europe and the Digital Europe Programme, lay down and adopt the conditions for joint actions;

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, 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 advice to the Cybersecurity Competence Community with regard to the** establish**ment of** working 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 1271/2013[1];

l) set up a monitoring mechanism to ensure that the implementation of the respective funds is done in accordance with the Agenda, missions and the multiannual work programme of the Centre;

la) to ensure a regular dialogue and establish an effective cooperation mechanism with the Community;

[1] ~~Commission Delegated Regulation (EU) No 1271/2013 of 30 September 2013 on the framework financial regulation for the bodies referred to in Article 208 of Regulation (EU, Euratom) No 966/2012 of the European Parliament and of the Council (OJ L 328, 7.12.2013, p. 42).~~

~~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;

sa) register entities nominated by Member States as their National Coordination Centres;

sb) in deciding on the annual work programme and the multi-annual work programme, ensure coherence and synergies with those parts of the Digital Europe and the Horizon Europe programmes 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, ENISA shall provide the Executive Director and the Governing Board strategic advice and input for drafting Agenda, annual and multiannual work programme within the deadlines set by the Governing Board.

Formatted: None, Indent: Left: 0 cm, Hanging: 1.5 cm, Tab stops: Not at 2.5 cm

Commented [AM12]: C3 Directorate/MFA: We are of the opinion that ENISA should be actively involved in the preparation of the Centre's Agenda, annual and multi-annual work programme due to its indisputably leading role in European cybersecurity landscape. Therefore, we suggest the conduct of a consultation between the Centre and ENISA as a prerequisite condition to the adoption of Agenda, annual and multi-annual work programme by the Centre's Governing Board. We remind that in accordance with Regulation (EU) 2019/881 ENISA has assumed increased responsibilities, notably the establishment of EU cybersecurity certification framework for ICT products, services and processes. Furthermore, in accordance with recital 52 of Regulation (EU) 2019/881 ENISA should take full account of the ongoing research in the field of cybersecurity and is encouraged to establish cooperation with relevant EU agencies and bodies such as the European Research Council and the European Institute for Innovation and Technology.

Formatted: Font: (Default) Times New Roman, 12 pt, Not Bold

Article 44

Support from the host Member State

1. An administrative agreement may be concluded between the ~~Competence~~ Centre and the Member State ~~[Belgium]~~ in which its seat is located concerning privileges and immunities and other support to be provided by that Member State to the ~~Competence~~ Centre. The seat of the Centre shall be determined in a democratically accountable procedure, using transparent criteria and in accordance with Union law.

2. The host Member State shall provide the best possible conditions to ensure the proper functioning of the Centre, including a single location which would facilitate the cooperation between the Centre and ENISA due to the experience of ENISA in the field in all matters regarding cybersecurity.

Formatted: Indent: Left: 1 cm, First line: 0.27 cm, Line spacing: 1.5 lines, Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 1.27 cm + Indent at: 1.9 cm

Commented [AM13]: Given that there is no provision for the selection procedure of the Centre's seat, we support the European Parliament's proposed wording, which is included in its first reading position [P8_TA(2019)0419].

Formatted: Font: (Default) Times New Roman, 12 pt, English (United Kingdom)

Commented [AM14]: Facilitating the close and effective cooperation between ENISA and the Centre should be a major criterion for the selection of the Centre's seat. ENISA's experience and expertise in all matters regarding cybersecurity is of pivotal importance for the establishment of the Centre.

FRANCE

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 ensure 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.~~

…..

Commented [15]: FR/ it seems that what we are aiming at is the growth of the sector and not the ecosystem. We would suggest in addition, to add after European cybersecurity sector : from research and innovation, the strengthening of cybersecurity skills and training and the deployment of cyber products and solutions,

Commented [16]: FR/We can support the deletion only if our amendement to aa) is included as otherwise it does not reflect the weakenesses identified in recital 7b

Commented [17]: FR/ First a general comment; to maintain a good spirit of negotiations, it is important not to reopen text that was subject to negotiations and agreements between Member states. We therefore oppose this deletion which is not justified. there is no indication on how projects related to the deployment of solutions in Europe would be selected in the regulation; as there is the cyberact that will aim at promoting the development of solutions that meet a certain security standard, this sentences aims at using, where appropriate and possible, that framework as a reference point.

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.**

…

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.**

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** ~~s~~ 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 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.

Commented [18]: FR/ although we would support more restrictive criteria for the Community as their role on the definition of the priorities has been strengthened, we would not support to bring national security within the competence of an Union body as the Centre might then have the right to ask how this entity comply with national security legislations or ask what are the relevant national security legislation. We would prefer to add the notion of checks by the NCC that the entities do not present cybersecurity risks , see below;

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, **including an assessment of cyber-security risks/on security grounds**, 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 at Union level. 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 [19]: FR/this clarification is needed to better understand at which level the community operates

7. **The Community shall through its representatives provide to the Executive Director and the Governing Board strategic advice and input ~~for drafting~~on 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~~ Union's cybersecurity research, technological and industrial sector and monitor its implementation;

Commented [20]: FR/ the addition of the term drafting goes a bit too far; we would prefer a more neutral term such as "on"

Commented [21]: FR/we usually talk about the "Union" and not "Europe"

AUSTRIA

Written Comments – Austria
Regulation of CCCN – Doc. 5341/1/20 and 5889/20

General Comments

Austria appreciates the Chair's work on the proposal and the support of the Commission.

Austria is one of the countries that is critical to the formation of a new body given there is a complex landscape in the European cybersecurity landscape already with existing structures that could have taken up the tasks.

Nevertheless, based on the assumption that the present proposal will be the basis for continued work, Austria is giving the views below, thereby referring to the following general comments:

- Financial contribution from MS should be the exception, not the rule.
- Mandatory contributions are not acceptable for AT.
- Duplications with existing structure – especially ENISA – must be avoided. We must aim for lean/streamlined structure.

These comments shall be considered as initial remarks and are not exhaustive.

General Request

AT would like to see a visualization and overview of how the different documents and programmes build on each other (Agenda, bi- and multiannual work programmes, annual work programmes), what governance and decision mechanisms apply to the different documents and programmes (Centre's Governing Board, HE programme committees, DEP governance structure) and how they interlink with each other on a timeline.

Comments to the text

Article 2(4)

The definition of "in-kind contribution" should be more precise and amended accordingly: "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. …

Article 4a

1.aa) Austria welcomes the specification that the scope of the Agenda is limited to cybersecurity industry, technology and research and welcomes the usage of the term "Cybersecurity Industrial, Technology and Research Agenda".

1.d) Notwithstanding Austria's support for the European cybersecurity certification framework and the work done under the framework, Austria welcomes the deletion of "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" as the provision was too vague.

Article 6 and 7 – the Network of National Competence Centres

The role of the Network is highly unclear. Art. 7 para 4 makes references to Art. 7 para 1. The reference to para 1 lit. c is superfluous because lit. c is deleted. The reference to lit. e and g is unclear because it refers to activities at national or regional level which should only be done by the National Coordination Centres. If "regional" refers to bi- or multilateral activities in this context, this should be made clear.

So one of the remaining task is lit. a (acting as contact point at the national level for the Community) which is also the task of each National Competence Centre. This seems to be a duplication and not useful.

The only task which seems to make sense is lit. b. There the questions remains whether it should be possible that a limited number of MS can also work together as the Network in that case or does it always have to be 27 MS. Art. 6 para 6 seems to indicate that the Network has to be composed of all 27 MS.

The recitals do not specify these provisions.

The new addition in Art. 4a para 1 lit. bc does not bring more clarity in this context. The Network needs clear and meaningful tasks. However, if we look at the text as whole – especially Art. 1 and 3 and the recitals – it indicates a much stronger role for the Network which is not reflected in the tasks.

As we always preferred a slight structure we would not want to add another layer of bureaucracy with the Network. We can agree that the representatives of the National Competence Centre shall meet regularly and exchange information, therefore the new addition in Art. 4a para 1 lit. bc is acceptable. The rest of the text however has to be amended accordingly.

Article 8

We seek clarification on the amendment "Furthermore they should comply with the relevant national security regulations." Is it possible to require members of the Community in a Union

legal act to comply with security provisions in national law? There is no specification in the legal act regarding national security provisions. Shouldn't the amendment be more of an entitlement (opening clause) to regulate this aspect of Community membership at a national level? On the other hand, is there a reason to use this soft form of obligation ("should" instead of "shall")?

Article 21

Austria strongly supports the addition of "voluntary" in para. 5.

Comments to the recitals

New Recital 7b

In our experience, the Impact Assessment is normally not quoted/repeated in a recital. Thus, we prefer to convey the message of the proposed recital without explicit reference to the Impact Assessment.

Recital 8a – Pilot projects

We heard so much about the four pilot projects so that the question remains whether we can add more coherence to the work done by these projects and integrate it better into the Community. Furthermore, it has to be noted that these projects are not contractual public-private partnerships which is why the recital should be amended accordingly: "…thereby building on the existing experience that has been set up by the contractual public-private partnership and the four pilot projects on cybersecurity,…"

POLAND

Polish comments on
Proposal for a REGULATION of CCCN and the NCCs. -document 5889/20 and 5341/1/20
REV 1

1) Recital 9c we suggest to delete sentence „The Centre will therefore have a special nature.", and add one stating that the Centre would be implementing body.
2) In art. 2 par 3 the words „entities stemming from those Member States" should remain;
3) art. 4a (1) (aa) is not in line with the wording of art. 13 (3) (a). According to art. 4a (1) (aa): Agenda will set out strategic recommendations and goals for development and growth of European cybersecurity ecosystem. This is to wide. These goals are implemented by the Cybersecurity Strategy. Agenda will not be a strategy. Wording „cybersecurity ecosystem" should be replaced by „cybersecurity research, technological and industrial sector", which is used in art. 13 (3) (a). Using „cybersecurity system" may suggest that Agenda would be an overall cybersecurity strategy, not as it should be, only in the area of „research, technology and industry". It should be clear what are the interdependencies between Agenda and other documents concerning cybersecurity policy.
4) Recital 9 and 24 are inconsistent. Recital 9 states that 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, while recital 24 states only about fullfilling by the Centre the strategic goals of Agenda.
5) The task to: „Coordinate the work of the Network and the Community in order to achieve the mission set out in Article 3, in particular supporting cybersecurity start-ups and SMEs in the European Union, facilitating their access to expertise, funding, investment and to markets" is not an implementing task. It should be put into strategic and probably merged with task in (1) (bc)
6) We propose again the following wording for the implementation tasks of the Centre:

   a) implement the cybersecurity parts of Digital Europe Programme established by Regulation No XXX and in particular actions related to Article 6 of Regulation (EU) No XXX [Digital Europe Programme] in accordance with the multiannual strategic plan of the Centre, by managing all the phases in the lifetime of the project in particular carry out calls for proposals, monitor the implementation and evaluation, and gather, analyse and transmit to the Commission all the information needed to guide the implementation of that parts.
   b) implement 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 plan of the Centre, and the Strategic Plan of Horizon Europe, and
   c) implement other relevant EU funds when provided for in the legal acts of the Union or delegated by the Commission.
   e) facilitate the acquisition of cybersecurity infrastructures – at the service of industries, the public sector and research communities, through voluntary contributions

from Member States and EU funding for joint actions, in line with the Strategy, multiannual strategic plan and the annual work plans. EU funding shall not be conditioned to voluntary funding from Member States

7) Task in art. 4a (2) (f) is not an implementation task.
8) We propose the following wording for art. 8 (2):

„3. Only entities which are established within the Union and **guarantee public trust** may be ~~accredited~~ **registered** as members of the Cybersecurity Competence Community. **The entities shall not be under corporate control, including the actual influence, of a state other than an EU Member State, its entity or a citizen of that state. In the case of an entity being under such control, it should be determined whether it may threaten national security, including economic security, of the Member State.** 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).

The assessment of request of the entity should also include its risk profile, including security reasons."

Compliance with national security regulations might be insufficient, the criterium of corporate control suits better for the purpose of building trustworthy community.

9) We propose to add in art. 13 new para stating that:

„(…) **ENISA shall provide the Executive Director and the Governing Board strategic advice and input while drafing the Agenda, multiannual and annual work programmes within the deadlines set out by the Governing Board".**

It should be noted that the proposed wording is in line with the PREZ proposal for art. 8 par. 7 in doc. 5889/20. ENISA is a very important member of the Cybersecurity Community. Therefore ENISA is the entity that should first of all have the possibility to advice and give input to the Centre when it's preparing the strategic documents. This proposal remains in line with the provisions of Cybersecurity Act which foresees for ENISA the task to advise Union structures on reasearch (art. 11, recital 52).
Recital 52 of the Regulation (EU) 2019/881 of the European Parliament and of 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) provides that
ENISA should take full account of the ongoing research, development and technological assessment activities, in particular those activities carried out by the various Union research initiatives **to advise Union institutions, bodies, offices and agencies and where relevant, the Member States at their request**, on research needs and priorities in the field of cybersecurity. In order to identify the research needs and priorities, ENISA should also consult the relevant user groups. In line with above art.

11 of Cybersecurity Acts states that in relation to research and innovation, ENISA shall: **advise the Union institutions, bodies, offices and agencies and the Member States on research needs and priorities in the field of cybersecurity.** with a view to enabling effective responses to current and emerging risks and cyber threats, including with respect to new and emerging information and communications technologies, and with a view to using risk-prevention technologies effectively; **Moreover art. 11 (c) of Cybersecurity Act states that ENISA shall** contribute to the strategic research and innovation agenda at Union level in the field of cybersecurity.
What is more, recital 4 of Cybersecurity Act foresees that by making the relevant information available to the public, ENISA **contributes to the development of the cybersecurity industry** in the Union, in particular SMEs and start-ups. ENISA should strive for closer cooperation with universities and research entities in order to contribute to reducing dependence on cybersecurity products and services from outside the Union and to reinforce supply chains inside the Union. Recital 41 states that ENISA should make use of available best practices and experience, especially the best practices and experience of academic institutions and IT security researchers.

The wording of above cited recitals and provisions of Cybersecurity Act is clear. The Cybersecurity Act foresees for ENISA a strong role in the area of cybersecurity industry, research and innovation, precisely stating the task of ENISA **to advise** Union structures on research needs and priorities in the field of cybersecurity. Therefore, there are no legal doubts with regard to the possibility of giving ENISA the task of advising the Centre, which is, notwithstanding its special nature, a Union structure (body) under art. 188 of the Treaty.

It should be noted that the aim of the Agenda, foreseen in the proposal for a Regulation establishing the ECCN, is to set out strategic recommendations and goals for development and growth of the European cybersecurity ecosystem. These recommendations and goals shall be futher specified in the multiannual and annual work programmes of the Centre. A key and special role of ENISA in the cybersecurity ecosystem is obvious. It is crucial to ensure that the Centre while defining its priorities and planning actions receives the suport of ENISA, which has the knowlegde and skills stemming from years of experience in the field of european cybersecurity. The role of obserwer at the management board is welcomed but remains inssuficient. It is important to ensure the input from ENISA at the stage of drafting the Agenda and working programmes.

10) In art. 15 it should be clear that the decision to put the joint action into the Centre working programme is made in accordance with rule: one MS and EC - one vote. But the decisions concerning the governance of joint actions, after there are approved by standard procedure (one MS and EC - one vote), should be made based on rule that votes are proportional to relevant contribution on specific joint action. Therefore the text should be amended to clearly reflect these rules.

_____