Council of the European Union
General Secretariat

Interinstitutional files:
2018/0328(COD)

Brussels, 18 February 2020

WK 1788/2020 ADD 3

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 EE, FR (additional comments) and PT

Delegations will find in Annex comments from EE, FR (additional comments) and PT delegations on the above-mentioned subject (doc. 5341/1/20 REV 1 and 5889/20).

TABLE OF CONTENT

ESTONIA

Regarding article 4a, para aa) and d):
We should bear in mind ENISA-s tasks for drafting those two paragraphs, as set out in the EU Cybersecurity Act article 11, paras a and c and not duplicate those.: 11 para a - *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*; 11 para c: *contribute to the strategic research and innovation agenda at Union level in the field of cybersecurity*. The Centre should work in sync with ENISA. Therefore we propose to add a 4a para e) "*In performing those tasks [the Cybersecurity Competence Centre] and ENISA shall engage in structured cooperation to benefit from synergies and to avoid the duplication of activities*." This could be for instance inspired by the EU Cybersecurity Act article 7, which reads: "*In performing those tasks, ENISA and CERT-EU shall engage in structured cooperation to benefit from synergies and to avoid the duplication of activities*."

FRANCE

doc. 5341/1/20 REV 1

(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~~[1], 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 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.

Commented [1]: FR/ the creation of functions under Union law are either related to A JU or a Union body. In addition, national competent authorities are not established in accordance with Union but with national law; To be legally sound, it might be better to delete "created under Union law"

Commented [2]: FR/this addition seems very vague and therefore does not add anything as the point of this recital is to be illustrative on which entities could perform the role of NCC

1 ~~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 [3]: FR/promote the cybersecurity capability of the demand industry is a confusing sentence. It would make more sense to read " promote the take up by the demand side industry of cybersecurity capabilities" as the issue is often that the demand side industry is lacking cybersecurity capabilities

(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.

(29) The ~~Competence~~ Centre should have in place rules regarding the prevention and the management of conflict of interest. The ~~Competence~~ Centre should also apply the relevant Union provisions concerning public access to documents as set out in Regulation (EC) No 1049/2001 of the European Parliament and of the Council[2]. Processing of personal data by the ~~Competence~~ Centre will be subject to Regulation (EU) No XXX/2018 of the European Parliament and of the Council. The ~~Competence~~ Centre should comply with the provisions applicable to the Union institutions, and with national legislation regarding the handling of information, in particular sensitive non classified information and EU classified information.

(30) The financial interests of the Union and of the Member States should be protected by proportionate measures throughout the expenditure cycle, including the prevention, detection and investigation of irregularities, the recovery of lost, wrongly paid or incorrectly used funds and, where appropriate, the application of administrative and financial penalties in accordance with Regulation XXX (EU, Euratom) of the European Parliament and of the Council[3] [the Financial Regulation].

30a) For the purpose of simplification, the administrative burden should be reduced for all parties. Double audits and disproportionate amount of documentation and reporting should be avoided. Audits of recipients of Union funds under this Regulation should be carried out in compliance with Regulation (EU, Euratom) 2018/1046.

Commented [4]: Fr/ necessary addition to reduce administrative burden

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

3 [add title and OJ reference]

~~(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.[4]

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;

Commented [5]: FR/ we are a bit confused by whether this definition is strictly about in kind contribution; why couldn't some eligible costs be included as financial contributions ? We could suggest to add a definition as follows on Member's state contribution that covers both in kind and financial contributions
Member State contribution" means resources of whatever nature made directly or indirectly available by a Member State , including but not limited to contributions made available by legal entities duly established under the Law of said Member State and using resources made available by this Member State.

4 Reference to the Financial Regulation and other legislative acts.

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, its European Research Area and ~~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 adopted for the concerned programme

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;~~

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

Commented [ILK6]: Chaque programme de subvention de l'UE a sa stratégie (programmatique globale et processus de mise à jour régulière) pré-établie. Pour HE, c'est le programme spécifique réf. P8_TA(2019)0396, le SIA de l'IET, etc.

(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 concerned Member States and ~~EU funding for joint actions~~the Union, in ~~line~~ accordance with the Agenda, multiannual work programme and the annual work programmes. EU funding shall not be conditioned to voluntary funding from any Member ~~States~~State ;

(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.

The Competence Centre shall accredit **register** relevant **Union** bodies, agencies and offices **of the Union** as members of the Cybersecurity Competence Community after carrying out an assessment whether that entity meets the criteria provided for in paragraph 3. A n accreditation **registration** shall not be limited in time but may be revoked by the Competence Centre at any time if it 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**.

5. The representatives of **the ~~Commission~~ Union institutions, agencies and bodies** may participate in the work of the Community.

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 [7]: FR/this clarification is needed to better understand at which level the community operates

p) where appropriate, lay down rules on the secondment of national experts to the ~~Competence~~ Centre and on the use of ~~trainees~~ other staff 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.

Commented [8]: FR/ a suggestion could be to simply refer to Member's state contribution to cover both in kind and financial contribution

Commented [9]: FR/ repetition of point s)

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~~ renewed 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 chair, 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 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.

Commented [10]: FR/ in article 12 related to the representatives nominated in the governing board, they are nominated for four years; the timing is therefore not coherent

Commented [11]: FR/ to be consistent with the nomination of the representatives

c) after consultation with the Governing Board and the Commission, **and taking into account the opinion of the Network and Community, and in accordance with the Agenda,** prepare and submit for adoption to the Governing Board the draft multiannual **work programme** and the annual work **programme** of the ~~Competence~~ Centre including the scope of the calls for proposals, calls for expressions of interest and calls for tenders needed to implement the work **programme** and the corresponding expenditure estimates as proposed by the Member States and the Commission;

d) prepare and submit for adoption to the Governing Board the draft annual budget, including the corresponding staff establishment plan indicating the number of temporary posts in each grade and function group and the number of contract staff and seconded national experts expressed in full-time equivalents;

e) implement the work **programme** and report to the Governing Board thereon;

f) prepare the draft annual activity report on the ~~Competence~~ Centre, including the information on corresponding expenditure **and realisation of the strategic goals and priorities set out in the Agenda and the multiannual work programme of the Centre, and if necessary accompanied by proposals for further improvement of the realisation and/or reformulation of the strategic goals and priorities;**

g) ensure the implementation of effective monitoring and evaluation procedures relating to the performance of the ~~Competence~~ Centre;

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

Commented [12]: FR/ only the work programme ? what about the Agenda, and the multiannual work programme ?

k) approve and manage the launch of calls for proposals, in accordance with the work **programme** and administer the grant agreements and decisions;

l) approve the list of actions selected for funding on the basis of the ranking list established by a panel of independent experts;

m) approve and manage the launch of calls for tenders, in accordance with the work **programme** and administer the contracts;

n) approve the tenders selected for funding;

o) submit the draft annual accounts and balance sheet to the Internal Auditing Function, and subsequently to the Governing Board;

p) ensure that risk assessment and risk management are performed;

q) sign individual grant agreements, decisions and contracts;

r) sign procurement contracts;

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

t) prepare draft financial rules applicable to the ~~Competence~~ Centre;

u) establish and ensure the functioning of an effective and efficient internal control system and report any significant change to it to the Governing Board;

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

w) take any other measures needed to assess the progress of the ~~Competence~~ Centre towards its mission and objectives as set out in Articles 3 and 4 of this Regulation;

Commented [13]: FR/ to make it more coherent, r) could be merged with n) as procurement contracts will have to be correlated with tenders

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 [14]: FR/ As we have not received any confirmation that there will be any budgetary element we would suggest to go back to the original text

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~~ takingen ~~into account in as part of~~ the strategic planning process 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 the Regulation.

Commented [15]: /FR/ As we have not received any confirmation that there will be any budgetary elemen as part of the strategic planning process we would suggest to refer to the fact that as the amount of horizon Europe will be determined by taking into account the strategic planning process, then the contributions of Member states that will be matched by HE budget should also take into account that same process.

Commented [16]: FR/ This should be put in brackets in coherence with article 21 paragraph 1 – b

~~*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 be considered as contributions as those actions are in the remit of the Centre's missions and tasks.

3. The European Anti-Fraud Office (OLAF) may carry out investigations, including on-the-spot checks and inspections, in accordance with the provisions and procedures laid down in Council Regulation (Euratom, EC) No 2185/96[5] and Regulation (EU, Euratom) No 883/2013 of the European Parliament and of the Council[6] with a view to establishing whether there has been fraud, corruption or any other illegal activity affecting the financial interests of the Union in connection with a grant agreement or a contract funded, directly or indirectly, in accordance with this Regulation.

4. Without prejudice to paragraphs 1, 2 and 3 of this Article, contracts and grant agreements resulting from the implementation of this Regulation shall contain provisions expressly empowering the Commission, the ~~Competence~~ Centre, the Court of Auditors and OLAF to conduct such audits and investigations in accordance with their respective competences. Where the implementation of an action is outsourced or sub-delegated, in whole or in part, or where it requires the award of a procurement contract or financial support to a third party, the contract, or grant agreement shall include the contractor's or beneficiary's obligation to impose on any third party involved explicit acceptance of those powers of the Commission, the ~~Competence~~ Centre, the Court of Auditors and OLAF.

5. The Centre shall ensure that the financial interests of its members are adequately protected by carrying out or commissioning appropriate internal and/or external controls.

---

5 Council Regulation (Euratom, EC) No 2185/96 of 11 November 1996 concerning on-the-spot checks and inspections carried out by the Commission in order to protect the European Communities' financial interests against fraud and other irregularities (OJ L 292, 15.11.1996, p. 2).

6 Regulation (EU, Euratom) No 883/2013 of the European Parliament and of the Council of 11 September 2013 concerning investigations conducted by the European Anti-Fraud Office (OLAF) and repealing Regulation (EC) No 1073/1999 of the European Parliament and of the Council and Council Regulation (Euratom) No 1074/1999 (OJ L 248, 18.9.2013, p. 1).

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 [17]: 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 [18]: 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 [19]: 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.**

Commented [20]: FR/We support Germany's comment that it might be clearer to say that the Secretariat of the Network shall be done by the Centre . The concept of administrative coordination is not less clear.

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.

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 [21]: 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;

Commented [22]: 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 [23]: FR/ the addition of the term drafting goes a bit too far; we would prefer a more neutral term such as "on"

Commented [24]: FR/we usually talk about the "Union" and not "Europe"

PORTUGAL

Comment 1:
Article 2
Article2(1) and 2(2):

"[…] network and information systems, the users of such systems and other persons affected by exposed to cyber threats.

Or alternatively

"[…] network and information systems, the users of such systems and other persons affected by cyber threats incidents").

Comment 2:

Article 8

Article 8.6

" [...]gender, as well as intra-sectorial balance."

Comment 3:

Article 13

Article 13(3cb) is linked with Article 15 (2a) (concerning voting rights) and Mentions exceptions to the general rule on voting rights when deciding "joint actions".

Portugal considers the following:

In Article 13 (3cb) which, when read with article 15 stipulates an exception to the general rule (of consensus and 75 % voting in the lack thereof) through proportional voting based on Member States contributions (to joint actions), Portugal considers that this exception should only apply to decisions related to the management of said joint actions and not be a blanket decision on all decisions related to joint actions as would currently be the case in 13 (3cb).

This last point is considered as a red line for us.