Council of the European Union
General Secretariat

Interinstitutional files:
2018/0328(COD)

Brussels, 30 November 2018

WK 13078/2018 ADD 2

LIMITE

CYBER
TELECOM
CODEC
COPEN
COPS
COSI
CSC
CSCI
IND
JAI
RECH
ESPACE

WORKING PAPER

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

WORKING DOCUMENT

From: To:	Presidency Horizontal Working Party on Cyber Issues
N° Cion doc.:	12104/18
Subject:	Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres - Comments from the Italian delegation.

Delegations will find attached a new version of the compilation of Member States' text proposals and comments on the above-mentioned proposal for a Regulation. The changes compared to the previous version are the inclusion of additional comments and proposals from the Italian delegation on Articles 4(4)(b), 4(4)(c), 15(1) and 22.

PROPOSAL	DRAFTING SUGGESTIONS	COMMENTS
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** ***A contribution from the European Commission to the Leaders' meeting in Salzburg on 19-20 September 2018*** THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION, Having regard to the Treaty on the Functioning of the European Union, and in particular Article 173(3) and the first paragraph of Article 188 thereof, Having regard to the proposal from the European Commission,	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~~ Competence Centres** **(EE)**	**EE:** We suggest modifying the names of the Centre and the Network to have better clarity, follow the 2017 Council Conclusions, as well as solve the "semantical" issue. This means, leaving the word "competence" out of the Centre's name, as this will mainly be an administrative body. This would leave "European Cybersecurity Industrial, Technology and Research Centre". On the contrary, regarding the Network we propose replacing the word "coordination" with "competence", as the national bodies will have more than only administrative functions. Accordingly, the Network's name would be – "Network of National Competence Centres". This is a proposal that should be consistent throughout the text in our view, meaning every time the Network is mentioned, it should be "National Competence Centres' Network"; and every time we speak about the Centre, it would just be "Cybersecurity Industrial, Technology and Research Centre". **ES**: 1.- The Digital Europe and Horizon Europe Programmes are currently under discussion in different Council configurations (Telecom and Competitiveness). Even the Multiannual Financial Framework (MFP). This fact is identified as a potential risk to this proposal as the outcome of those two negotiations is still unknown. Furthermore, it is not clear that this proposal sticks to the procedure established within the Horizon Europe

		Programme negotiation, since this proposal aims to put in place a European Partnership that should be discussed in the context of the Strategic Planning Process that precisely deals, in particular, with European Partnerships. From our point of view, it would seem that COM is not taking into account its own procedures. For that reason, we consider that the negotiations and the final agreements on this regulation need more time than one semester in order to come out with a rational, efficient and well detailed structure that allows to tackle the important objectives under this initiative. Going further, the delegation may ask for "Reservation study" of the whole proposal given the contradictions incurred before. 2.- As the separation of research in cybersecurity from the rest of the clusters in Pillar-II of Horizon Europe can lead into a non-efficient cooperation and interrelation with the different application domains, the delegation may consider to, leave cybsersecurity research within the Pillar-II Security cluster in Horizon Europe. **DE:** <u>General Comments:</u> Germany supports the general aim of strengthening the union-wide coordination of Member State's efforts for better and trustworthy cybersecurity products and services; especially a deeper coordination of the Union's cybersecurity research programs. Nevertheless we express fundamental doubts that this draft offers an adequate, effective and efficient approach

		towards reaching these goals. We are concerned that the proposed structures will cause internal complexity and bureaucracy to an amount which in the end is counterproductive for achieving more cybersecurity. Our major concerns can be summed up as follows: • The objectives and tasks of the Competence Centre (cf. Article 4) are not formulated concretely enough to make sure that no detrimental conflicts with already existing national and/or union-wide institutions (like ENISA or Research Executive Agency (REA)) will arise. Especially the intended limitations of the Centre's objectives are not clearly stated. Moreover such a clarification is needed as cybersecurity issues have a deep impact on questions of national security. The Member States' ability to take appropriate measures must not be impaired by objectives and tasks of the Competence Centre. • The complicated structure of relations between different actors bear the risk of administrative burdens and delays which might peril the goals of the planned regulation. The present draft does not present sufficient arguments why "leaner" structures have been omitted early in the impact assessment. • Besides the few remarks in recital (21) the draft is not explicit enough with respect to the foreseen cooperation

		between the Competence Centre and existing Cybersecurity Organisations. • Given the fact that the pilot projects for Cybersecurity Competence Centres are just about to start their work we propose to start this regulation with leaner and more flexible structures in order to be able to react on relevant outcomes of these projects swiftly. • It is unclear what the fiscal effects of this draft will be - for the EU´s budget and even for the Member States. This has to be clarified before a regulation can be put in effect. • The voting rules of the Governing Board (cf. Article 15) do not represent a fair and reasonable balance between Member States and the European Commission. Especially with regard to the fact that cybersecurity issues often are connected to questions of national security this is not acceptable. As our remarks contain fundamental questions towards the intended structures and institutions we explicitly express a **scrutiny reserve** for any content in this or in further drafts of this regulation. **SK:** Slovak Republic in general supports the intention expressed in the present legislative proposal and therefore supports the proposal for a Regulation of the European Parliament and of the Council establishing the European

		Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres. The idea of creating a European Competence Centre in the area of cyber security as well as the establishment of a network of national coordination centres is regarded very positively. Slovak Republic believes that investing in science, research and innovation in this area will, among other things, have a beneficial effect on the development of the digital economy in EU, building expertise and capabilities, as well as enhancing the security of products and services and increasing trust in the digital single market. The SK agrees with the content of the proposal, including the tasks to be performed by the European Competence Centre and the National Coordination Centres, the choice of legal instrument and the dual legal basis chosen. Slovak Republic agrees with the strategic vision of the Union to ensure the development of its own technological capabilities in the context of building a more strategic autonomy, to ensure the protection and resilience of all its critical networks or information systems, while securing its own digital assets in cyber security, thereby supporting the already mentioned trust in the digital single market. Slovak republic also supports the idea and tendency for the Union to become "a global leader in cyber security by 2025 with the goal to keep a trust, reliability and protection for our

		citizens, consumers and businesses online and to provide free and legitimate internet." On the other hand during the negotiation it will be necessary to detail various issues and communicate several approaches to the proposal of the Commission, what was the position it assumed when determining the seat of the Competence Centre. Based on which conditions and in what way were the rules for financial coverage created regarding the administrative and operational costs of the Competence Centre, while it is necessary to open the question of other possibilities of financing from the EU budget. Explanatory Memorandum of the proposal for a regulation (context of the proposal - compliance with existing provisions in this kind of policy area) - Supporting research with objective to facilitate and speed up standardization and certification processes. Particularly for the area of cyber-security certification systems in the context of the proposed Cyber Security Act, Regulation (EU) No 526/2013 of the EP and of the Council concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004 (hereinafter "Cyber Security Act"). The current proposal - the Cyber Security Act in this context identifies ENISA as an authority on EU-level with a natural responsibility for cyber

		security issues. ENISA would take this role in order to bring together and coordinate the work of the relevant national certification entities. ***Opinion on the Explanatory Memorandum of the Proposal for a Regulation (context of the proposal - compliance with Existing Provisions in this Policy Area):*** SK considers and asks the Commission to verify whether if it is possible, under the Cyber Security Act, in relation to the certification within area of cyber-security process, the mandate planned for ENISA could be also assigned to the National Coordination Centre under the proposal of regulation on CCCN. ***Justification:*** The National Contact Point as an entity disposes or has direct access to cyber security technology expertise, particularly in areas such as cryptography, ICT security services, intrusion detection, system security, network security, software and application security, and security or aspects of security and protection privacy in relation to people and the whole society. It is also able to effectively engage and coordinate its activities with the relevant sector, the public sector including bodies, which are designated for this activity under European Parliament and Council Regulation (EU) 2016/1148 23, and the research community.

Having regard to the opinion of the European Economic and Social Committee[1], Having regard to the opinion of the Committee of the Regions[2], Acting in accordance with the ordinary legislative procedure, Whereas:		
(1) Our daily lives and economies become increasingly dependent on digital technologies, citizens become more and more exposed to serious cyber incidents. Future security depends, among others, on enhancing technological and industrial ability to protect the Union against cyber threats, as both civilian infrastructure and military capacities rely on secure digital systems.	**SE:** Our daily lives and economies become increasingly dependent on digital technologies, citizens become more and more exposed to serious cyber incidents. Future security depends, among others, on enhancing technological and industrial ability to protect the Union against cyber threats, as ~~both~~ civilian infrastructure ~~and military capacities~~ rely on secure digital systems.	**SE:** This is of course true, however SE does consider that this proposal should not at this stage include direct references to military activities, as the CCCN is not yet established, lacks structure and security measures etc. needed to manage military requirements. If the proposal at this stage should include enhancing military capacities or other military related aspects, SE believes the proposal would require considerable re-drafting in order to ensure and manage security issues, as well as clarifying and ensuring that the CCCN does not affect or impose on the competences of MS, in regards to national security, export control etc.

[1] OJ C , p. .
[2] OJ C , , p. .

(2)	The Union has steadily increased its activities to address growing cybersecurity challenges following the 2013 Cybersecurity Strategy[3] aimed to foster a reliable, safe, and open cyber ecosystem. In 2016 the Union adopted the first measures in the area of cybersecurity through Directive (EU) 2016/1148 of the European Parliament and of the Council[4] on security of network and information systems.		
(3)	In September 2017, the Commission and the High Representative of the Union for Foreign Affairs and Security Policy presented a Joint Communication[5] on "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU" to further reinforce the Union's resilience, deterrence and response to cyber-attacks.		

[3] Joint Communication to the European Parliament and the Council:: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace JOIN(2013) 1 final.

[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).

[5] Joint Communication to the European Parliament and the Council "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU", JOIN(2017) 450 final.

(4)	The Heads of State and Government at the Tallinn Digital Summit, in September 2017, called for the Union to become "a global leader in cyber-security by 2025, in order to ensure trust, confidence and protection of our citizens, consumers and enterprises online and to enable a free and law-governed internet."		
(5)	Substantial disruption of network and information systems can affect individual Member States and the Union as a whole. The security of network and information systems is therefore essential for the smooth functioning of the internal market. At the moment, the Union depends on non-European cybersecurity providers. However, it is in the Union's strategic interest to ensure that it retains and develops essential cybersecurity technological capacities to secure its Digital Single Market, and in particular to protect critical networks and information systems and to provide key cybersecurity services.		

(6)	A wealth of expertise and experience in cybersecurity research, technology and industrial development exists in the Union but the efforts of industrial and research communities are fragmented, lacking alignment and a common mission, which hinders competitiveness in this domain. These efforts and expertise need to be pooled, networked and used in an efficient manner to reinforce and complement existing research, technology and industrial capacities at Union and national levels.	**DE:** A wealth of expertise and experience in cybersecurity research, technology and industrial development exists in the Union. These efforts and expertise need to be pooled, networked and used in an efficient manner to reinforce and complement existing research, technology and industrial capacities at Union and national levels.	**DE:** The statement: "[…] but the efforts of industrial and research communities are fragmented, lacking alignment and a common mission, which hinders competitiveness in this domain." is not backed up by COM. It does not take sufficient account of the existing European research and funding landscape.
(7)	The Council Conclusions adopted in November 2017 called on the Commission to provide rapidly an impact assessment on the possible options to create a network of cybersecurity competence centres with the European Research and Competence Centre and propose by mid-2018 the relevant legal instrument.		

(8)	The Competence Centre should be the Union's main instrument to pool investment in cybersecurity research, technology and industrial development and to implement relevant projects and initiatives together with the Cybersecurity Competence Network. It should deliver cybersecurity-related financial support from the Horizon Europe and Digital Europe programmes, and should be open to the European Regional Development Fund and other programmes where appropriate. This approach should contribute to creating synergies and coordinating financial support related to cybersecurity research, innovation, technology and industrial development and avoiding duplication.	**SE:** The Competence Centre should be the Union's main instrument to pool investment in cybersecurity research, technology and industrial development and to implement relevant projects and initiatives together with the Cybersecurity Competence Network**,** without distoring competition / market and without prejudice to the sole responsibility of the Member States for the maintenance of national security. It should deliver cybersecurity-related financial support from the Horizon Europe and Digital Europe programmes, and should be open to the European Regional Development Fund and other programmes where appropriate. This approach should contribute to creating synergies and coordinating financial support related to cybersecurity research, innovation, technology and industrial development and avoiding duplication. **FR:** The Competence Centre should be ~~one of~~ the Union's main instrument to ensure **a coordinated and strategic approach to Union's** ~~pool~~ investment in cybersecurity research, technology and industrial development, and to implement relevant projects and initiatives together with the Cybersecurity Competence Network. It should deliver cybersecurity-related financial support from the Horizon Europe and Digital Europe programmes **for some specific actions**, and should be open to the	

	European Regional Development Fund, ***the Connecting Europe facility, the SME instrument*** and other programmes where appropriate. This approach should contribute to creating and coordinating synergies financial support related to cybersecurity research, innovation, technology and industrial development and avoiding duplication ***across programmes***.	**DK:** With the current provisions of the European Regional Development Fund, it is not necessarily relevant that ERDF funds should be directed towards the Cybersecurity Competence Network (though legally it may be possible). Also, the new rules concerning the European Structural and Investment funds post 2020 have not been approved as of yet, making it difficult to say which rules apply when this proposal comes into force. Hence, we would welcome that the Commission clarify why it is intended to use ERDF-funds. **PL:** It is very hard to decide about the scope and procedures in reference to the financial support from DEP and Horizon Europe, as both of these programmes together with MFF are now being discussed by different Council's working groups. Hence, we would welcome the EC's clarification with respect to the money distribution mechanism within these programs in the field of cybersecurity.

(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.		**SE:** SE questions the way the MS money respected. MS has already contributed to the EU-budget, but this solution require MS to put in more funding. See comment on art 15.2 which preamble 9 relates to. SE would at this stage like to see a calculation on different scenarios how this voting procedure could pan out, in order for the MS to assess the impact this would have. **DK:** Can non-participating member states, as well as businesses, organizations and public authorities located in these member states, participate in projects and activities financed and organized through the Competence Centre? **ES:** This might imply an unfair treatment to Member States that will provide funding through the Union´s budget to Horizon Europe and Digital Europe Programmes . Not to mention the Associated States that will most likely join those two Programmes. **PL:** Still the relation between the financial contribution from the MSs and the voting rights of the MSs is not clear. It may imply, as ES mentioned, unfair treatment of MSs that will provide funding through the Union´s budget to Horizon Europe and DEP. As described in the Impact Assessment, the idea is to make Europe globally competitive in the area of research and innovation. That is way none of MSs should be discriminated. Only

		together we can make Europe strong and decrease the difference between Europe, USA and other parts of the world. **CZ:** CZ agree with ES and SE. MS are already providing funding through the Union´s budget to Horizon Europe and Digital Europe Programmes. This solution require MS to put in more funding. **FR:** The linkage between the majority rule and the financial contribution is not acceptable as it stands given the lack of clarity regarding the contribution that would be expected from each member state.
(10) The participating Member States' financial participation should be commensurate to the Union's financial contribution to this initiative.	**FR:** ~~The participating Member States' financial participation should be~~ commensurate ~~to the Union's financial contribution to this initiative.~~	**FR:** There seems to be a lack of clarity over whether the financial participation expected from Member states needs to be commensurate to the Union's financial contribution to the administrative and operational costs or to the Union's financial contribution under Horizon Europe and the Digital Europe Programme. **PL:** At this moment we do not know how the future budget will look like, therefore it is impossible to predict the MS's contribution to this initiative. In any case the amount of financial contribution should be known in advance.

(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 activities related to this Regulation.	**SE**: 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 activities related to this Regulation.	**SE**: A general principle for union programs are that you receive funds under competition. What is the reason that this centre should be made to compete under the same conditions , in the strive for excellence **ES:** More details should be provided

(12) National Coordination Centres should be selected by Member States. In addition to the necessary administrative capacity, Centres should either possess or have direct access to cybersecurity technological expertise in cybersecurity, notably in domains such as cryptography, ICT security services, intrusion detection, system security, network security, software and application security, or human and societal aspects of security and privacy. They should also have the capacity to effectively engage and coordinate with the industry, the public sector, including authorities designated pursuant to the Directive (EU) 2016/1148 of the European Parliament and of the Council[6], and the research community.		**SE**: How does this pertain to civil vs military cyber security? The centre has been mention in the EDF; but, this list is not suitable in a EDF context- What kind of entity should the National Coordination Centres be? A national agency, a company, a university? All in the civilian sector? **DK:** Will non-participating member states also have to select a national coordination Centre? **ES:** More details shoul be provided concerning the role of military stakeholders. **PL:** With reference to recital 15 the question is about how the investment by MSs as well as cyber security technological agenda both civilian and military - should be combined in the same national coordination centre? What will be the relation between EDA and Competence Centre and National Coordination Centres? The Regulation lacks procedure and clarity how the sensitivity and restriction connected with the defence area are to be managed and secure.

[6] 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).

(13)	Where financial support is provided to National Coordination Centres in order to support third parties at the national level, this shall be passed on to relevant stakeholders through cascading grant agreements.		**ES:** Cascading grants, also known as FSTP (Financial Support to Third Parties) might be a suitable way to reach out and foster innovation ecosystems. However, public sector organizations face large administrative difficulties as they have to comply with specific national regulations in order to provide funding. A detailed and clear procedure should be provided in order to make this process easier.
(14)	Emerging technologies such as artificial intelligence, Internet of Things, high-performance computing (HPC) and quantum computing, blockchain and concepts such as secure digital identities create at the same time new challenges for cybersecurity as well as offer solutions. Assessing and validating the robustness of existing or future ICT systems will require testing security solutions against attacks run on HPC and quantum machines. The Competence Centre, the Network and the Cybersecurity Competence Community should help advance and disseminate the latest cybersecurity solutions. At the same time the Competence Centre and the Network should be at the service of developers and operators in critical sectors such as transport, energy, health, financial, government, telecom, manufacturing, defence, and space to help them solve their cybersecurity challenges.	**SE**: 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~~ most effective ~~—~~ cybersecurity solutions. At the same time the Competence Centre and the Network should be at the service of developers and operators in critical sectors such as transport, energy, health, financial, government, telecom, manufacturing, defence, and space to help them solve their cybersecurity challenges	**SE**: This needs further staffing …and elaboration what is intended here. In the proposal for a regulation establishing the European Defence Fund (EDF), recital p. 26, there is a reference to the initiative in this regulation. It is proposed that the CCCN could actively support Member States and other relevant actors by providing advice, sharing expertise and facilitating collaboration with regard to projects and actions as well as when requested by Member States acting as a project manager in relation to the European Defence Fund. However, this is only a proposal at this point. The negotiations of the EDF is ongoing and the mentioned statement is neither accepted or approved. Therefore any link, direct or indirect to the , is pending the negotiations of the EDF. . SE therefore suggest removing all direct references to defence or military aspects. Also, this regulation does not address security, protection of European Union Classified Information (EUCI), export control, etc..; aspects that needs to be clarified and address before any military issues can be relevant to approach. The

	ES: 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 most advanced states of the art and technologies. The Competence Centre, the Network and the Cybersecurity Competence Community should help advance and disseminate the latest cybersecurity solutions. At the same time the Competence Centre and the Network should be at the service of developers and operators in critical sectors such as transport, energy, health, financial,	centre should focus on civilian use, and once operational and evaluate, military related activities can be considered. What is meant by "be at the service of"? More concretely – what are they proposed to do? To correspond with similar changes made in the articles of this regulation and changes proposed by the Presidency in Digital Europe Programme, "at the service of developers and operators in critical sectors" – could be changed to point out the organisations these developers and operators are part of, for example public sector organisations and industry.

	government, telecom, manufacturing, defence, and space to help them solve their cybersecurity challenges.	**DE:** In the area of critical infrastructure there already exist various national structures and legislative regulations. It has to be clarified in how far facilities that provide critical infrastructures are being supported by the Competence Centre. **PL:** PL supports SE requesting further details in reference to the last sentence starting with: "At the same time the…". Especially we would like to know the definition of the phrase "at the service of".

(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 the cybersecurity technological agenda and facilitate access to the expertise gathered in the Network and the Cybersecurity Competence Community. 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 joint investment by the Union, Member States and/or industry.	**SE**: 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 the cybersecurity technological agenda and facilitate access to the expertise gathered in the Network and the Cybersecurity Competence Community. 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 joint investment by the Union, Member States and/or industry. **FR:** 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 the cybersecurity technological agenda and facilitate access to the expertise gathered in the Network and the Cybersecurity Competence Community. Secondly, it should implement **specific** parts of Digital Europe and **—of** Horizon Europe programmes by allocating grants, typically following a competitive call for proposals. Thirdly, the Competence Centre should facilitate joint investment by the Union,	**SE**: Will all the money from Horizon Europe be allocated through call for proposals? Or will money from Horizon Europe be used for the first function, or even allocating money without calls? It has to be clearer that researchers from any Member State can answer call for proposals from Horizon Europe and that any actor/company in Member States can answer call for tender (not only those from participating member states). **FR:** The Centre should not exclusively implement the cybersecurity part of Horizon Europe but carry out some specific actions that are at the crossroads between research and the development of technologies such as feasibility studies, support to certification, support to the coordination and networking of national centres of expertise and so on. In addition, the centre should have the ability to follow the state of the art of projects financed by Horizon Europe to strengthen the link between the research and deployment phase, . The French authorities would therefore like to ask the Presidency to clarify what is meant with the “term” implementation to better understand whether it means that the Centre would perform

	Member States and/or industry	the tasks related to the evaluation, follow-up and management of projects. **ES:** The Digital Europe and Horizon Europe Programmes are currently under discussion in different Council configurations (Telecom and Competitiveness). Even the Multiannual Financial Framework (MFP). This is identified as a potential risk to this proposal as the outcome of those two negotiations is still unknown. Furthermore, it is not clear that this proposal sticks to the procedure established within the Horizon Europe Programme negotiation, since this proposal aims to put in place a European Partnership that should be discussed in the context of the Strategic Planning Process that precisely deals, in particular, with European Partnerships. It seems like the COM is not taking into account its own procedures! **DE:** Is the Competence Centre's steering structure compatible with the different control structures for the programmes Digital Europe and Horizon Europe? Coordination/ cooperation ? See comment on Article 22 further down **PL:** An explanation is needed in reference to the third key function of the Competence Centre: joint investment by the Union, Member States and/or industry. It is needed to precisely describe the procedure of such a function, in particular, in the light of MSs voting rights limited only to those who contribute financially. **CZ:** We agree with SE and ES.

(16) The Competence Centre should stimulate and support the cooperation and coordination of the activities of the Cybersecurity Competence Community, which would involve a large, open, and diverse group of actors involved in cybersecurity technology. That Community should include in particular research entities, supply-side industries, demand side industries, and the public sector. The Cybersecurity Competence Community should provide input to the activities and work plan of the Competence Centre and it should also benefit from the community-building activities of the Competence Centre and the Network, but otherwise should not be privileged with regard to calls for proposals or calls for tender.		**ES:** ECSO (The European Cybersecurity Organization) has been deeply engaged with this community for the last two years. It should be mentioned and what will be its role. It is more pragmatic to build this initiative upon already existing structures. We must not show that the private cybersecurity sector will not play a very important role in this new initiative. **DE:** The diverse group of actors involved in the Cybersecurity Competence Community should also explicitly include actors from civil society groups dealing with issues related to cybersecurity, including privacy rights and access to information.

(17) In order to respond to the needs of both demand and supply side industries, the Competence Centre's task to provide cybersecurity knowledge and technical assistance to industries should refer to both ICT products and services and all other industrial and technological products and solutions in which cybersecurity is to be embedded.		**SE**: Would this not distort competition within the Union? How can this role be delineated as to not compete with services available on the private market? Providing knowledge and technical assistance with this scope would be incredibly resource-demanding. It should be clarified that the Competence Centre will help provide this support through the Competence Network, and not directly to end-users. ? How would this be coherent with Art. 173 TFEU? **FI: Standardisation and certification:** As regards standardization and Competence Centre support to facilitate and accelerate in particular, the processes related to cybersecurity certification schemes, it is important to clearly define the responsibilities of the Centre in standardisation and certification. These should be agreed on and shared among the industry, the ECCC and NNCC. Currently, the industry role in the EC proposal is fairly limited which could also mean low impact on the matters related to standardization and certification. **DE:** Why can the need of the demand and supply side only be met by technical assistance of the Competence Centre? Why can this not be accomplished if the Competence Centre focuses on coordinating the National Competence Centres? **PL:** We would like to request an explanation in reference to the wording "technical assistance to the industry". How such an assistance should

		look like? What are the competences of the Competence Centre in this area?
(18) Whereas the Competence Centre and the Network should strive to achieve synergies between the cybersecurity civilian and defence spheres, projects financed by the Horizon Europe Programme will be implemented in line with Regulation XXX [Horizon Europe Regulation], which provides that research and innovation activities carried out under Horizon Europe shall have a focus on civil applications.	**SE:** ~~Whereas the Competence Centre and the Network should strive to achieve synergies between the cybersecurity civilian and defence spheres, projects financed by the Horizon Europe Programme will be implemented in line with Regulation XXX [Horizon Europe Regulation], which provides that research and innovation activities carried out under Horizon Europe shall have a focus on civil applications~~. **FR:** Whereas the Competence Centre and the Network should strive to achieve synergies between the cybersecurity civilian and defence spheres, projects financed by the Horizon Europe Programme will be implemented in line with Regulation XXX [Horizon Europe Regulation], which provides that research and innovation activities carried out under Horizon Europe shall have a**n exclusive** focus on civil applications	**SE**: See comments to p. 1 and 14. If the intention is to also strive for synergies between the civilian and defence cybersecurity – is this the best way? Is it appropriate to then use e.g. private entities as National Coordination Centres? **ES:** More detail should be provided on how these synergies are expected to be achieved. **DE:** In what areas do such synergies exist and how can the synergies be used? **A clear separation/division between support of programs in civilian and defence spheres is required.** **PL:** Both civilian and military spheres have different procedures in applying. In particular with respect to procurement and application of the resources. More details should be provided on how these synergies are expected to be achieved. **CZ:** We support ES position.

(19) In order to ensure structured and sustainable collaboration, the relation between the Competence Centre and the National Coordination Centres should be based on a contractual agreement.		**PL:** Bearing in mind the discussion during the HWP meeting on 28th September we would like to once again stress the need for one standard of contractual agreement, same for everyone. **SE:** Are the contracts between the Competence Centre and each MS centre envisaged to be standardised for all MS centres, or will they differ? If they may differ, would there be any particular aspects where no flexibility is foreseen?
(20) Appropriate provisions should be made to guarantee the liability and transparency of the Competence Centre.		
(21) In view of their respective expertise in cybersecurity, the Joint Research Centre of the Commission as well as the European Network and Information Security Agency (ENISA) should play an active part in the Cybersecurity Competence Community and the Industrial and Scientific Advisory Board.	**FR:** In view of their respective expertise in cybersecurity, ~~**the Joint Research Centre of the Commission as well as**~~ the European Network and Information Security Agency (ENISA) should play an active part in the Cybersecurity Competence Community and the Industrial and Scientific Advisory Board.	**FR:** The EU cybersecurity landscape is too fragmented, there is no need to have three bodies in charge of cybersecurity. **SE:** What is the intended relationship between the Competence Centre and the European Union Agency for Network and Information Security (ENISA)? How is ENISA supposed to "take an active part in the Cybersercurity Compentence Community and the Industrial and Scientific Advisory Board"? Do the tasks of ENISA in some aspect overlap with the tasks of the Competence Centre (and the Cybersecurity Competence Network)? Are both structures necessary?

		LV: The title of ENISA should be amended here, and throughout the regulation, according to the changes made in the Cybersecurity Act. **FI:** When planning new structures, it should be kept in mind that the development of cyber security products and solutions is based on market demand and conditions and by the companies operating under global competition. As a positive signal, the actions within the scope of the Proposal would be based on public-private partnership and collaboration. However, the role of companies is fairly limited, in particular, when comparing to the ambitious objectives of the proposal. It is important to assess synergies and possible overlaps with ENISA, and whether the proposal would weaken the role of ECSO, that is currently a significant channel for companies and industries to participate in the EU level actions and to develop European cyber security. **ES:** More details shouild be provided on how this initiative will be complementary to ENISA's efforts in order to follow the principle of building on already existing structures **DE:** This short recital is not sufficient to clarify the relation between the Competence Centre and existing national and union-wide organisations and structures acting in the field of cybersecurity. **PL:** In light of this recital we express an urgent need for clarification of competences between the future Competence Centre and such agencies as: ENISA, EDA, and JRC. We definitely should avoid overlap of tasks and

		competences. **CZ:** What should be exactly the role of ENISA?
(22) Where they receive a financial contribution from the general budget of the Union, the National Coordination Centres and the entities which are part of the Cybersecurity Competence Community should publicise the fact that the respective activities are undertaken in the context of the present initiative.		
(23) The Union contribution to the Competence Centre should finance half of the costs arising from the establishment, administrative and coordination activities of the Competence Centre, In order to avoid double funding, those activities should not benefit simultaneously from a contribution from other Union programmes.		

(24) The Governing Board of the Competence Centre, composed of the Member States and the Commission, should define the general direction of the Competence Centre's operations, and ensure that it carries out its tasks in accordance with this Regulation. The Governing Board should be entrusted with the powers necessary to establish the budget, verify its execution, adopt the appropriate financial rules, establish transparent working procedures for decision making by the Competence Centre, adopt the Competence Centre's work plan and multiannual strategic plan reflecting the priorities in achieving the objectives and tasks of the Competence Centre, adopt its rules of procedure, appoint the Executive Director and decide on the extension of the Executive Director's term of office and on the termination thereof.	**SE**: The Governing Board of the Competence Centre, composed of the Member States and the Commission, should define the general direction of the Competence Centre's operations, and ensure that it carries out its tasks in accordance with this Regulation. The Governing Board should be entrusted with the powers necessary to establish the budget, verify its execution, adopt the appropriate financial rules, establish transparent working procedures for decision making by the Competence Centre, adopt the Competence Centre's work plan and multiannual strategic plan reflecting the priorities in achieving the objectives and tasks of the Competence Centre, adopt its rules of procedure, appoint the Executive Director and decide on the extension of the Executive Director's term of office and on the termination thereof. <u>The Governing Board should be gender balanced.</u>	**SE:** If defence aspects are to be addressed, this would for example need further discussion concerning the requirements. **ES:** This might imply an unfair treatment to Associated States to Digital Europe and Horizon Europe programmes

(25)	In order for the Competence Centre to function properly and effectively, the Commission and the Member States should ensure that persons to be appointed to the Governing Board have appropriate professional expertise and experience in functional areas. The Commission and the Member States should also make efforts to limit the turnover of their respective Representatives on the Governing Board in order to ensure continuity in its work.		
(26)	The smooth functioning of the Competence Centre requires that its Executive Director be appointed on grounds of merit and documented administrative and managerial skills, as well as competence and experience relevant for cybersecurity, and that the duties of the Executive Director be carried out with complete independence.		**SE:** Any staff would require having suitable security clearance, regardless if focusing only civilian cyber security only. The issue needs to be further address in the regulation.

(27) The Competence Centre should have an Industrial and Scientific Advisory Board as an advisory body to ensure regular dialogue with the private sector, consumers' organisations 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 Industrial and Scientific Advisory Board and the tasks assigned to it, such as being consulted regarding the work plan, should ensure sufficient representation of stakeholders in the work of the Competence Centre.	**SE**: The Competence Centre should have an Industrial and Scientific Advisory Board as an advisory body to ensure regular dialogue with the private sector, consumers' organisations 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 Industrial and Scientific Advisory Board and the tasks assigned to it, such as being consulted regarding the work plan, should ensure sufficient representation of stakeholders in the work of the Competence Centre. The Industrial and Scientific Advisory Board should be gender balanced.	**SE:** Confidentiality requirements? **DE:** The need for an Industrial and Scientific Advisory Board in addition to the Competence Centre and the Coordination Centres is not sufficiently justified (s. comments on Art. 18-20).

(28) The Competence Centre should benefit from the particular expertise and the broad and relevant stakeholders' representation built through the contractual public-private partnership on cybersecurity during the duration of Horizon2020, through its Industrial and Scientific Advisory Board.		**ES:** Comment on 27 and 28: Again,-cf (16)- this has been one of the main tasks carried out by ECSO in the past two years. ECSO (The European Cybersecurity Organization) has been deeply engaged with this community for the last two years. ECSO should be mentioned and explained what will be its role. It is more pragmatic to build this initiative upon already exixting structures. We must not show that the private cybersecurity sector will not play a very important role in this new initiative **CZ:** We recommend to mention ECSO on this place as well as define properly its role.

(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[7]. 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.	**SE**: 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[8]. 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. In addition, a gender perspective shall be applied in the preparation, implementation, monitoring and evaluation of the ordinary functioning of the Competence Centre, including the budget process.	**SE**: How will this be foreseen to be managed? Important that the competence of MS is honoured, ie export control etc It could be considered to have more explicit rules regarding the handling of EUCI, especially if defence aspects should be included in the scope of this Regulation **ES:** More details should be provided. This is a critical issue for a proper operation of the Competence Centre and the whole network of National Coordination Centers. It is also an issue for the military stakeholders.

[7] 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).

[8] 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).

(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[9] [the Financial Regulation].		
(31)	The Competence Centre should operate in an open and transparent way providing all relevant information in a timely manner as well as promoting its activities, including information and dissemination activities to the wider public. The rules of procedure of the bodies of the Competence Centre should be made publicly available.	**DE:** The Competence Centre should operate in an open and transparent way providing all relevant information in a timely **and easily accessible** manner as well as promoting its activities, including information and dissemination activities to the wider public. The rules of procedure of the bodies of the Competence Centre should be made publicly available.	**DK:** Some potential national candidates to be selected as national coordination centres are connected to/integrated in intelligence services. Does that constitute a problem in relation to the Competence Centre operating in an open and transparent way? **PL:** Once again we would like to underline a necessity to further explain civilian and military synergies.

[9] [add title and OJ reference]

(32) The Commission's internal auditor should exercise the same powers over the Competence Centre as those exercised in respect of the Commission.		
(33) The Commission, the Competence Centre, the Court of Auditors and the European Anti-Fraud Office should get access to all necessary information and the premises to conduct audits and investigations on the grants, contracts and agreement signed by the Competence Centre.		

(34) Since the objectives of this Regulation, namely retaining and developing Union's cybersecurity technological and industrial capacities, increasing the competitiveness of the Union's cybersecurity industry and turning cybersecurity into a competitive advantage of other Union industries, cannot be sufficiently achieved by the Member States due the fact that existing, limited resources are dispersed as well as due to the scale of the investment necessary, but can rather by reason of avoiding unnecessary duplication of these efforts, helping to achieve critical mass of investment and ensuring that public financing is used in an optimal way be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve that objective.		**ES:** ok. Cf previous comment on (21) about ENISA **PL:** In reference to the SE's suggestion for new recital 35 we would like to support further discussion on that issue based on reference in the proposal to the civilian and the military spheres.

	SE: **(New 35)** This Regulation is without prejudice to the sole responsibility of the Member States for the maintenance of national security, as provided for in Article 4 (2) of the Treaty of the European Union (FEU), and to the right of the Member States to protect their essential security interests in accordance with Article 346 of the Treaty on the Functioning of the European Union (TFEU).	
HAVE ADOPTED THIS REGULATION:		

CHAPTER I **GENERAL PROVISIONS AND PRINCIPLES OF THE COMPETENCE CENTRE AND THE NETWORK** *Article 1* **Subject matter**		
1. This Regulation establishes the European Cybersecurity Industrial, Technology and Research Competence Centre (the 'Competence Centre'), as well as the Network of National Coordination Centres, and lays down rules for the nomination of National Coordination Centres as well as for the establishment of the Cybersecurity Competence Community.	**SE**: This Regulation establishes the European Cybersecurity Industrial, Technology and Research Competence Centre (the 'Competence Centre'), as well as the Network of National Coordination Centres (the 'Network'), and lays down rules for the nomination of National Coordination Centres as well as for the establishment of the Cybersecurity Competence Community (the 'Community'). **LV**: This Regulation establishes the European Cybersecurity Industrial, Technology and Research Competence Centre (the 'Competence Centre'), as well as the Network of National Coordination Centres ('the Network'), and lays down rules for the nomination of National Coordination Centres as well as for the establishment of the Cybersecurity Competence Community.	

2.	The Competence Centre shall contribute to the implementation of the cybersecurity part of the Digital Europe Programme established by Regulation No XXX and in particular actions related to Article 6 of Regulation (EU) No XXX [Digital Europe Programme] thereof and of the Horizon Europe Programme established by Regulation No XXX and in particular Section 2.2.6 of Pillar II of Annex I. of Decision No XXX on establishing the specific programme implementing Horizon Europe – the Framework Programme for Research and Innovation[ref. number of the Specific Programme].	**ES:** The Competence Centre shall contribute to the implementation (this Competence Centre will be much more than an "implementing" body as it will deal with strategy and its definition) of the cybersecurity part of the Digital Europe Programme established by Regulation No XXX and in particular actions related to Article 6 of Regulation (EU) No XXX [Digital Europe Programme] thereof and of the Horizon Europe Programme established by Regulation No XXX and in particular Section 2.2.6 of Pillar II of Annex I. of Decision No XXX on establishing the specific programme implementing Horizon Europe – the Framework Programme for Research and Innovation[ref. number of the Specific Programme]. **FR:** The Competence Centre shall contribute to the implementation of **specific parts of** the cybersecurity and **trust objective** of the Digital Europe Programme established by Regulation No XXX ~~and in particular actions related to~~ Article 6 of Regulation (EU) No XXX [Digital Europe Programme] thereof and ***specific parts*** of the Horizon Europe Programme established by Regulation No XXX **relevant to cybersecurity** in particular Section 2.2.6 ***and*** **Section 3.2.2** of Pillar II of Annex I of Decision No XXX on establishing the specific programme implementing Horizon Europe – the Framework Programme for	**ES:** Digital Europe and Horizon Europe Programmes are currently under discussion in different Council configurations (Telecom and Competitiveness). This is identified as a potential risk to this proposal as the outcome of those two negotiations is still unknown . Furthermore, it is not clear that this proposal sticks to the procedure established within the Horizon Europe Programme negotiation, since it aims to put in place a European Partnership that should be discussed in the context of the Strategic Planning Process that precisely deals, in particular, with European Partnerships. It seems as if the COM would not be taking into account its own procedures. **FR:** Contribution of the Centre calls for clarification as regards The pillar on cybersecurity of the Digital Europe programme is called "cybersecurity and trust". Considering the current organization of the Centre, only the objective in article 6 (a) and (b) of DEP could be eligible. As regards Horizon Europe, the Centre should implement some specific actions from the programme to contribute to a more integrated approach for eligible projects between the research phase and the deployment of technologies. In general, we understand that the intention of

	Research and Innovation[ref. number of the Specific Programme].~~[…]~~.	the Commission is for the center to develop its own strategic programme to implement actions for cybersecurity, linking research and industry. Although this approach could work for some specific actions, we see an issue of synergies and articulation between the implementation of the multiannual strategic, industrial, technology, and research plan developed by the Center and the programme of both Horizon Europe and Digital Europe given the transversal aspect of cybersecurity. In this respect all the other specific objectives of the DEP have clear interactions and interest with cybersecurity issues, explicitly written : advanced digital skills, deployment and interoperability ; more implicitly written : I.A., and HPC. The same goes for Horizon Europe, explicitly not only the security Cluster but also digital and industry, but also actions related to energy, mobility and so on. In this respect, we would like to know from the European Commission whether the principle of a focus area such as the focus Area "security Union" that allows priority setting across the different budgets and synergies was envisaged , and how this could be implemented as far as this legislative proposal is concerned? Finally, the French authorities would like to ask the Presidency to clarify what is meant with the "term" implementation to better understand whether it means that the Center would perform the tasks related to the evaluation, follow-up and management of projects **PL:** It is very hard to decide about the scope and

		procedures in reference to the financial support from DEP and Horizon Europe, as both of these programmes together with MFF are now being discussed by different Council's working groups. Hence, we would welcome the EC's clarification with respect to the money distribution mechanism within these programs in the field of cybersecurity.
3. The seat of the Competence Centre shall be located in [Brussels, Belgium.]		**PL:** Is it already decided that the Centre's location would be in Brussels? Were other locations taken into account? **SK:** The Slovak Republic in long term asserted the opinion of the need for a geographical balance of the distribution of EU institutions and agencies between Member States and prioritises the placement of new EU agencies/institutions where none have been established. At the same time, SK suggests that the Commission justifies its choice and inform the Member States of the selection criteria for the EU Competence Centre based in Brussels. GEOGRAPHICAL SPREAD PRINCIPLE We wish to point out the principle of geographical spread for HQs of EU offices and agencies, as agreed by the Member States at the European Council of December 2003 and reiterated by the European Council of June 2008. In line with this principle, appropriate priority should be given to member states that acceded the Union in/after 2004 or that do not already host an EU office or agency. According to the Procedure, this principle should also be

		considered for relocations. This criterion becomes even more relevant given the currently disproportionate distribution of EU agencies' HQs among Member States.
4. The Competence Centre shall have legal personality. In each Member State, it shall enjoy the most extensive legal capacity accorded to legal persons under the laws of that Member State. It may, in particular, acquire or dispose of movable and immovable property and may be a party to legal proceedings.	**FR:** The Competence Centre shall have legal personality. ~~In each Member State, it shall enjoy the most extensive legal capacity accorded to legal persons under the laws of that Member State. It may, in particular, acquire or dispose of movable and immovable property and may be a party to legal proceedings.~~	**FR:** The second sentence seems redundant if the Centre already has legal personality. **PL:** In reference to the SE's suggestion for new Article 1.5 we would like to support further discussion on that issue based on a reference in the proposal to the civilian and the military spheres.
	SE: **New 5**. This Regulation is without prejudice to the sole responsibility of the Member States for the maintenance of national security, as provided for in Article 4 (2) of the Treaty of the European Union (FEU), and to the right of the Member States to protect their essential security interests in accordance with Article 346 of the Treaty on the Functioning of the European Union (TFEU).	

Article 2 **Definitions**		**FR:** 'industry' and its eventual different meanings by field (cybersecurity sector vs others) shall be defined too. Services in cybersecurity should be included. Those definitions should be in accordance with definitions given in other texts of the Union. Precise use of those further in the text should be done. In particular, the juridical status considered for the application of this regulation should be described. In order for a better articulation between the two programmes and this proposed regulation, it is suggested to introduce the adequate definitions that would help to identify the requirements of this text which would depend on Horizon Europe as regards R&D in cybersecurity and the requirements of this text which would depend on Digital Europe as regards deployment of cybersecurity, with a particular attention on transition between development and deployment **DE:** Definitions in Art. 2 have to comply with the definitions of other EU regulations in the area of cybersecurity. **CZ:** We would welcome to add a definition of cyber threat. **NL:** A definition of what "infrastructure" means would be welcome. This should be similar to what is in the Digital Europe text.

For the purpose of this Regulation, the following definitions shall apply: (1) 'cybersecurity' means the protection of network and information systems, their users, and other persons against cyber threats;	**UK:** **(1)** 'cybersecurity' comprises all activities necessary to protect ~~means the protection of~~ network and information systems, their users, and other persons against cyber threats; **(new 1a)** 'network and information system' means a system within the meaning of point (1) of Article 4 of Directive (EU) 2016/1148 **NL:** This definition should: 'cybersecurity' ~~means the protection of network and information systems, their users, and other persons against cyber threats;~~ comprises all activities necessary to protect network and information systems, their users, and affected persons from cyber threats;	**UK:** These changes are to bring in line with the Cyber Security Act. **SE**: As this is a new centre we are hesitant to, at this point, include defence/military aspects. Please see comment above. (eg. p. 1 and 14, recital). **LV**: The definition is worded too narrowly and does not cover all objectives set out in Article 6 of the proposal for Regulation of the European Parliament and of the Council establishing the Digital Europe programme for the period 2021-2027. Latvia proposes using the definition from ITU Rec. ITU-T X.1205 (04/2008): "Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and

		technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment." **FI:** The definition of 'cybersecurity' in this proposal should be the same as in Cybersecurity Act. **PL:** The definition should be harmonised with the definition proposed in the Cybersecurity Act. **CZ:** We stress that the definition of "cybersecurity" in this proposal should be the same as in Cybersecurity Act. **SK:** The term "cybersecurity" in the Regulation does not build on the definition of "network and information systems security" in the context of Article 4 Para 2 of the NIS Directive, where the security is regarded as the capability to withstand at certain level any action threatening access, authenticity, integrity and confidentiality of stored, transmitted or processed data or related services provided or accessible via these networks and systems. Definition in the submitted proposal focuses however on the protection of networks and information systems, their users and other individuals. We insist on making sure what the relationship is between cybersecurity in the context of the Regulation and networks and information systems security in the context of the NIS directive. It is also unclear whether it was the intention of the submitter to

		exclude from the definition data processed in the information systems or was it just an unfortunate slip.
(2) 'cybersecurity products and solutions' means ICT products, services or process with the specific purpose of protecting network and information systems, their users and affected persons from cyber threats;		
(3) 'public authority' means any government or other public administration, including public advisory bodies, at national, regional or local level or any natural or legal person performing public administrative functions under national law, including specific duties;		
(4) 'participating Member State' means a Member State which voluntarily contributes financially to the administrative and operational costs of the Competence Centre.		**ES:** A mention to the Associated States to Horizon or Digital Europe Programmes is needed which voluntarily further explanation requested on the precise meaning of this word in this context **PL:** Still the relation between the financial contribution from the MSs and the voting rights of the MSs is not clear. It may imply, as ES mentioned, unfair treatment of MSs that will provide funding through the Union´s budget to Horizon Europe and DEP. As described in the Impact Assessment, the idea is to make Europe globally competitive in the area of research and innovation. That is why none of MSs should be discriminated. Only

		together we can make Europe strong and decrease the difference between Europe, USA and other parts of the world. **SK:** The definition "participating Member State" in the proposal specifies such a State as defined in Article 2 Para 4 as a voluntary financial contributor to cover the administrative and operational costs of the Competence Centre. However, it is not clear the exact terms of voluntary conditions in the view of the willingness to provide the contribution and its amount. At the same time, we would also like to point to the vaguely defined position and relationship between the Member State and the participating Member State in relation to the Competence Centre.
	EE: (New 5) 'competence centre' means …	**EE:** If we clarify once and for all the definition of a competence centre, then it helps everyone involved, including Member States, to understand the difference between a competence centre and an administrative/coordination centre.

Article 3 **Mission of the Centre and the Network**	*Article 3* **Mission of the <u>Competence</u> Centre and the Network** **(LV)**	**LV**: Because Article 1, paragraph 1 notes that the European Cybersecurity Industrial, Technology and Research Competence Centre is shortened to "the 'Competence Centre'", Latvia suggests adding the word "Competence" to the title so to avoid any possible confusion between the Competence Centre and National Coordination **DE:** The provisions on mission, objectives and tasks contained here or in Article 4 (or in the corresponding recitals) do not make it sufficiently clear how exactly the EU envisages the fulfilment of the mission (also with regard to cooperation with other parties involved, e.g. ENISA or Member States). It should also be made clearer why existing bodies/corporations (e.g. ENISA or MS institutions) cannot or should not perform (at least some of) their tasks. This could enable a more effective and efficient coordination/control of the overall topic by dispensing with the need for further committees. In addition, (unnecessarily) cost-intensive double/parallel structures could be avoided in this way. **FR:** This article is about the Mission of the Centre and the network while paragraph 2 only refers to the Centre relying where appropriate on the network. In addition, although there is a specific article 4 related to the tasks and objectives of the Centre, and an article 7 related to the tasks of national coordination centres, there is no article that specifies how the network will function, although

		it is established in Article 1. It adds to our confusion over what will be the role of the network and how it will function
1. The Competence Centre and the Network shall help the Union to:	**SK:** The Competence Centre and the Network <u>of National</u> Coordination <u>Centres</u> shall help the Union to:	**SK:** In the introductory sentence, we propose to include the words "of National Coordination Centres" after the word "network". In this context, we propose to consider the introduction of the term "networks" as a basic concept, possibly introducing a legislative acronym.
(a) retain and develop the cybersecurity technological and industrial capacities necessary to secure its Digital Single Market;	**SE**: (a) retain and develop the <u>civil applications of</u> cybersecurity technological and industrial capacities necessary to secure its Digital Single Market; **UK:** (a) retain and develop the cybersecurity technological and industrial capacities necessary ~~to~~ <u>for the</u> security <u>and prosperity of</u> its Digital Single Market; **ES:** The Competence Centre shall undertake its tasks, where appropriate <u>Further explanation required</u>, in collaboration with the Network of National Coordination Centres and a Cybersecurity Competence Community. **FR:** retain and develop the cybersecurity technological and industrial **competencies and** capacities necessary to secure **autonomously** its Digital Single Market;	**SE**: It is necessary to dispute uncertainties of how the money will be spent, for example that it will not be spent on military applications. **UK:** Involvement of the national centres and/or community seem to be appropriate for all of the tasks the centre will be carrying out. **FR:** Securing the DSM is intimately linked to sovereignty of supported solutions at stake, and is a strategical matter for Member States

	(b) increase the competitiveness of the Union's cybersecurity industry and turn cybersecurity into competitive advantage of other Union industries.		**SE**: At other industries expense?
2.	The Competence Centre shall undertake its tasks, where appropriate, in collaboration with the Network of National Coordination Centres and a Cybersecurity Competence Community.	**SE:** (2) The Competence Centre shall undertake its tasks, ~~where appropriate~~ as far as possible, in collaboration with the Network of National Coordination Centres and a Cybersecurity Competence Community. **UK:** (2) The Competence Centre shall undertake its tasks, ~~where appropriate~~, in collaboration with the Network of National Coordination Centres and a Cybersecurity Competence Community	**UK:** Involvement of the national centres and/or community seem to be appropriate for all of the tasks the centre will be carrying out.

	EE: *(New Article 3a)* **Objectives of the Centre and the Network**	**EE:** In our view, only the first two points are the tasks of the Centre, the rest seems to be objectives. However, merging the two together only creates unnecessary confusion as the points 3-8 cannot be achieved by the Centre alone. Therefore, we are proposing to split this article into two articles. The first two points as the Centre's tasks will remain as Article 4 (below) and the points 3-8 will be the objectives of the Centre and Network together as Article 3a. The reasoning for this is that the Centre alone will not be able to fulfil these objectives, and as are the missions, these objectives should also be achieved together with the Network.
	The Centre and the Network shall aim to:	
	1. enhance cybersecurity capabilities, knowledge and infrastructures at the service of industries, the public sector and research communities, by carrying out the following tasks:	

	(a) having regard to the state-of-the-art cybersecurity industrial and research infrastructures and related services , acquiring, upgrading, operating and making available such infrastructures and related services to a wide range of users across the Union from industry including SMEs, the public sector and the research and scientific community;	
	(b) having regard to the state-of-the-art cybersecurity industrial and research infrastructures and related services, providing support to other entities, including financially, to acquiring, upgrading, operating and making available such infrastructures and related services to a wide range of users across the Union from industry including SMEs, the public sector and the research and scientific community;	
	(c) providing cybersecurity knowledge and technical assistance to industry and public authorities, in particular by supporting actions aimed at facilitating access to the expertise available in the Network and the Cybersecurity Competence Community;	
	2. contribute to the wide deployment of state-of-the-art cyber security products and solutions across the economy, by carrying out the following tasks:	

	(a) stimulating cybersecurity research, development and the uptake of Union cybersecurity products and solutions by public authorities and user industries;	
	(b) assisting public authorities, demand side industries and other users in adopting and integrating the latest cyber security solutions;	
	(c) supporting in particular public authorities in organising their public procurement, or carrying out procurement of state-of-the-art cybersecurity products and solutions on behalf of public authorities;	
	(d) providing financial support and technical assistance to cybersecurity start-ups and SMEs to connect to potential markets and to attract investment;	
	3. improve the understanding of cybersecurity and contribute to reducing skills gaps in the Union related to cybersecurity by carrying out the following tasks:	
	(a) supporting further development of cybersecurity skills, where appropriate together with relevant EU agencies and bodies including ENISA.	

	4. contribute to the reinforcement of cybersecurity research and development in the Union by:	
	(a) providing financial support to cybersecurity research efforts based on a common, continuously evaluated and improved multiannual strategic, industrial, technology and research agenda;	
	(b) support large-scale research and demonstration projects in next generation cybersecurity technological capabilities, in collaboration with the industry and the Network;	
	(c) support research and innovation for standardisation in cybersecurity technology	
	5. enhance cooperation between the civil and defence spheres with regard to dual use technologies and applications in cybersecurity, by carrying out the following tasks:	
	(a) supporting Member States and industrial and research stakeholders with regard to research, development and deployment;	

	(b) contributing to cooperation between Member States by supporting education, training and exercises ;	
	(c) bringing together stakeholders, to foster synergies between civil and defence cyber security research and markets;	
	6. enhance synergies between the civil and defence dimensions of cybersecurity in relation to the European Defence Fund by carrying out the following tasks:	
	(a) providing advice, sharing expertise and facilitating collaboration among relevant stakeholders;	
	(b) managing multinational cyber defence projects, when requested by Member States, and thus acting as a project manager within the meaning of Regulation XXX [Regulation establishing the European Defence Fund].	

Article 4 **Objectives and Tasks of the Centre**	*Article 4* **Objectives and Tasks of the <u>Competence</u> Centre (LV)** *Article 4* **~~Objectives and~~ Tasks of the Centre (EE)**	**EE:** As explained above, this article would only contain the real tasks of the Centre. **DE:** The tasks of the Competence Center have to be defined more concretely and have to be clearly separated from tasks that should remain in national sovereignty. The limits of the tasks and objectives must be clarified. The distribution of competences has to be defined according to the European Treaties: **<u>This clarification and definition is crucial for Germany.</u>** **PL:** PL supports EE's idea of dividing this part into two separate articles. Tasks and objectives should be described separately. As the tasks have to be executed in an effective way, it is possible only when cooperating with the Network and the Community. **EL:** Greece is concerned about the overlap between ENISA and the European Competence Center which is a matter of investigation and clarification. **FR:** The tasks of the Centre should be more clearly defined and the perimeter in which the centre operates should be more detailed. Unlike the tasks of certain joint undertakings created or programmes set up, the eligible actions for financing are very unclear.

The Competence Centre shall have the following objectives and related tasks:	**EE:** The Centre shall 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;	**LV**: facilitate and help coordinate the work of the ~~National Coordination Centres Network ('the~~ Network~~')~~ referred to in Article 6 and the Cybersecurity Competence Community referred to in Article 8;	
2. contribute to the implementation of the cybersecurity part of the Digital Europe Programme established by Regulation No XXX[10] and in particular actions related to Article 6 of Regulation (EU) No XXX [Digital Europe Programme] and of the Horizon Europe Programme established by Regulation No XXX[11] and in particular Section 2.2.6 of Pillar II of Annex I. of Decision No XXX on establishing the specific programme implementing Horizon Europe – the Framework Programme for Research and Innovation[ref. number of the Specific Programme]. and of other Union programmes when provided for in legal acts of the Union];	**FR:** contribute to the implementation of **specific parts of** the cybersecurity **and trust** ~~part~~**objective** of the Digital Europe Programme established by Regulation No XXX[12] ~~and in particular actions related to~~ Article 6 of Regulation (EU) No XXX [Digital Europe Programme] and **some specific actions** of the Horizon Europe Programme established by Regulation No XXX[13] ~~and~~ **relevant to cybersecurity** in particular Section 2.2.6 **and 3.2.2** of Pillar II of Annex I. ~~–~~of Decision No XXX on establishing the specific programme implementing Horizon Europe – the Framework Programme for Research and Innovation[ref. number of the Specific Programme]. and of other Union programmes when provided for in legal acts of the Union]~~;~~	**FR:** Paragraph 2 seems to repeat Article 1 paragraph 2. In addition, we would like to have further clarification on the practical consequences of extending the perimeter competence of the Competence Centre to other Union programmes dealing with cybersecurity. Similar to our comment to recital 15 and Article 1 paragraph 2 the French authorities would like to ask the Presidency to clarify what is meant with the "term" implementation to better understand whether it means that the Center would perform the tasks related to the evaluation, follow-up and management of projects

10 [add full title and OJ reference]
11 [add full title and OJ reference]
12 [add full title and OJ reference]
13 [add full title and OJ reference]

		DK: It is important that unnecessary administrative burdens are avoided – for the businesses as well as public authorities making use of the services and grants under these programmes. **ES:** Digital Europe and Horizon Europe Programmes are currently under discussion in different Council configurations (Telecom and Competitiveness). This is identified as a potential risk to this proposal as the outcome of those two negotiations is still unknown. Furthermore, it is not clear that this proposal sticks to the procedure established within the Horizon Europe Programme negotiation, since it aims to put in place a European Partnership that should be discussed in the context of the Strategic Planning Process that precisely deals, in particular, with European Partnerships. It seems as if the COM would not be taking into account its own procedures. **DE:** The proposal for the specific programme of Horizont Europa provides for the establishment of a European Network of Competence and Centre of Competence for Cyber Security as one of three broad lines in 2.2.6 Cybersecurity. What is the legal basis on which such a funding line can be made an implementation structure for the entire programme area? **SE:** What is meant by "contribute to the implementation"? What kind of tasks could it include, could some examples be presented?

3. enhance cybersecurity capabilities, knowledge and infrastructures at the service of industries, the public sector and research communities, by carrying out the following tasks:	**UK:** enhance cybersecurity capabilities, knowledge and infrastructures at the service of industries, the public sector and research communities, identified by the National Coordination Centres, by carrying out the following tasks:	**UK:** We would welcome more clarity on how these industries will be identified and for each of the tasks to be carried out in a fair, open and transparent way in order to ensure trust of the wider community. It might also be worth defining what is meant by cybersecurity infrastructure. **DE:** The definition of operative competences for the Competence Centre is unclear and allows different interpretations. Why should the Competence Centre acquire operative tasks that go beyond coordinative tasks? **CZ:** CZ requires to clarify and more precisely define the task of the Centre, in order to ensure transparency. **FR:** This paragraph 3 seems to be a general paragraph on which paragraph 4 on deployment, paragraph 5 on skills and paragraph 6 on research rely upon. These four paragraphs should be fine-tuned to understand more clearly what would be the missions of the Center and in particular eligible actions for funding; In addition there should be more details in this proposal about the objectives, eligible actions and award criteria, as it remains very unclear on the basis of which criteria services, products or infrastructures would be selected.

	(a) having regard to the state-of-the-art cybersecurity industrial and research infrastructures and related services, acquiring, upgrading, operating and making available such infrastructures and related services to a wide range of users across the Union from industry including SMEs, the public sector and the research and scientific community;	**SE**: having regard to the state-of-the-art cybersecurity industrial and research infrastructures and related services, ~~acquiring~~, ~~upgrading, operating~~ promoting knowledge and use of ~~and making available~~ such infrastructures and related services to a wide range of users across the Union from industry including SMEs, the public sector and the research and scientific community; **UK:** having regard to the state-of-the-art cybersecurity industrial and research infrastructures and related services, providing support in a fair, open and transparent way to other entities, including financially, to acquiring, upgrading, operating and making available such infrastructures and related services to a wide range of users across the Union from industry including SMEs, the public sector and the research and scientific community;	**SE:** Is state-of-the-art always the best solution in MS? And what infrastructures do you have in mind? How can industry, national authorities, etc. be able to use it based on very different needs and conditions? Who will evaluate what to invest in and who will get that asset? Is the intention that the competence center in fact shall develop technology (it says upgrading and operating)? It seems unreasonable both from an operational and economic perspective, but also since the center shall be temporary until 2029. It should not be a primary task of the centre to acquire, upgrade or operate infrastructure. A better option would be for the centre to provide guidance and disseminate best-practice on methodologies on acquisition and maintaining such infrastructures and services. If the centre itself should at all engage in acquisition of infrastructure and services, it should be in limited and specific cases, possibly piloting new technology. **UK:** In addition to the suggested change, it is a little unclear what is meant by this as it currently reads as if the centre itself would acquire, upgrade and operate cybersecurity services rather than facilitating this for industry? **DK:** We support the explicit reference to SMEs. **DE:** By using the terms "acquiring, upgrading, operating" the task description of the Competence Centre is not sufficiently precise. The tasks have to be clearly defined and have to

		be limited to specific areas and sectors. There is no clear separation of competences between the Competence Center and already existing institutions at EU and national level. **NL:** Would support switching A and B around. The Centre's focus should be primarily to support **others** in improving their cybersecurity, rather than taking on tasks of its own.
(b) having regard to the state-of-the-art cybersecurity industrial and research infrastructures and related services, providing support to other entities, including financially, to acquiring, upgrading, operating and making available such infrastructures and related services to a wide range of users across the Union from industry including SMEs, the public sector and the research and scientific community;	**UK:** having regard to the state-of-the-art cybersecurity industrial and research infrastructures and related services, providing support in a fair, open and transparent way to other entities, including financially, to acquiring, upgrading, operating and making available such infrastructures and related services to a wide range of users across the Union from industry including SMEs, the public sector and the research and scientific community; **SE:** having regard to the state-of-the-art cybersecurity industrial and research infrastructures and related services, providing support ~~to other entities,~~ including financially, to the Member States to acquiring, upgrading, operating and making available ~~–~~such infrastructures and related services ~~to a wide range of users across the Union from industry including SMEs, the public sector and the research and scientific community~~;	**SE**: It seems unrealistic that a centre in Brussels would be able to provide direct support to public sector bodies, SMEs etc throughout the EU in these matters. This encompasses tens of thousands of stakeholders. However, indirect support though the MS network could be relevant, but if so this must be further specified. Is the intention that the Centre shall support national authorities and companies to buy and upgrade infrastructure? Can the commission provide a flowchart and example of how a potential and realistic process can look like?

		"providing support" must be defined. In order to make smart use of the common resources, it should be clarified that the centre should only provide indirect support. **DK:** We support the explicit reference to SMEs. **CZ:** We support SE position to this provision. **NL:** What would be operated here? Not sure that is feasible or desirable. **FR:** "other entities" requires to be defined
(c) providing cybersecurity knowledge and technical assistance to industry and public authorities, in particular by supporting actions aimed at facilitating access to the expertise available in the Network and the Cybersecurity Competence Community;	**UK:** providing cybersecurity knowledge and technical assistance to industry and public authorities <u>in a fair open and transparent way,</u> in particular by supporting actions aimed at facilitating access to the expertise available in the Network and the Cybersecurity Competence Community; **SE:** providing cybersecurity knowledge ~~and technical assistance~~ to industry and public authorities, ~~in~~ particular by supporting actions aimed at <u>developing and</u> facilitating access to the expertise available in the Network and the Cybersecurity Competence Community;	**UK:** In addition to the suggested change, could facilitating access to expertise be expanded upon – eg: through networks, developing access tools (portals etc)? **SE**: What infrastructure and related services will be provided on EU level? What technical assistance is meant here? How would these services be delivered? SE would suggest this should be further specified, underlining that the centre itself should not engage in direct support but rather provide knowledge and assistance via the Network. How is this in line with the principle of subsidiarity? Generally, SE ask the commission to further elaborate the analysis of subsidiarity regarding the whole Article 4. In this para, we argue that "in particular" be

	FR: Supporting actions aimed at facilitating access to the expertise in the Network and the Cybersecurity Competence Community ~~providing cybersecurity knowledge and technical assistance to industry and public authorities, in particular by supporting actions aimed at facilitating access to the expertise available in the Network and the Cybersecurity Competence Community:~~	deleted as to show that the centre will provide indirect support through the Network. **FR:** seems redundant with Article 4 paragraph 1 as facilitating the coordination between the "network "should aim at facilitating access to the expertise ; c) could be possibly be merged with 4..1. In addition, technical assistance should be deleted as this has a very operational meaning and therefore seems out of scope of the objectives of this proposal
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:	**SE**: contribute to the wide deployment of ~~state-of-the-art~~ effective cyber security products and solutions across the economy, by carrying out the following tasks **UK:** contribute to the wide deployment of state-of-the-art internationally recognised cyber security products and solutions across the economy, by carrying out the following tasks:	**SE**: It might not always be the best solution to only deployment the latest or the most modern product or solution. "effective" or "best fit for purpose" corresponds to similar comments in this regulation and in DEP. **UK:** This will be helpful to avoid market fragmentation which is in the interests of better cyber security as well as a more competitive market. **DE:** The definition of operative competences for the Competence Centre is unclear and allows different interpretations. Why should the Competence Centre acquire operative tasks that go beyond coordinative tasks? **CZ:** We would welcome the clarifying of this para too.

(a) stimulating cybersecurity research, development and the uptake of Union cybersecurity products and solutions by public authorities and user industries;	**SE**: stimulating cybersecurity research and~~,~~ development ~~and the uptake of Union cybersecurity products and solutions by public authorities and user industries~~ in all member states regardless of financial participation in the centre; **UK:** a. stimulating cybersecurity research, including that carried out by ENISA, and the development and the uptake of Union cybersecurity products and solutions by public authorities and user industries; **FR:** stimulating ~~cybersecurity research, development and~~ the uptake of Union cybersecurity products and solutions by public authorities and user industries;	**SE**: It must be clearer who is the recipient of the services and that these ~~recipients~~ are not solely the participating member states who provide financial contributions. This should not be limited to "Union cybersecurity products" – for instance in cases where relevant products are needed but not available from European suppliers. **UK:** ENISA also has a role in research and market based activities so it would be good to ensure that the link between the two is clarified **FR:** Cybersecurity research, development" seems to be more relevant to § 6. below. Transition from development to deployment shall be refined to guaranty an efficient articulation between § 6 and 4 that respectively deals with those subjects.
(b) assisting public authorities, demand side industries and other users in adopting and integrating the latest cyber security solutions;	**SE**: advice public authorities, demand side industries and other users concering ~~in~~ adopting and integrating the ~~latest~~ most effective cyber security solutions, in particular by supporting actions aimed at facilitating access to the expertise available in the Network and the Cybersecurity Competence Community; **NL:** assisting ~~public authorities~~, demand side industries and other users in adopting and integrating the latest cyber security	**SE**: This whole paragraph should be deleted. It does not add anything that is not already in other paragraphs. As a second, but worse option, it should be amended as proposed. SE is questioning how this act of "assisting public authorities" will be carried out in practice. Could the COM develop this further by illustrating examples? However, we prefer the center to advice instead of assisting. SE suggests this should primarily be done

	solutions; **IT:** assisting public authorities (~~at their request)~~ <u>on a voluntary basis</u>, demand side industries and other users in adopting and integrating the latest cyber security solutions;	through the Network, and only in very specific and limited cases should. "The latest" solution might not be the best solution – effective or best fit for purpose corresponds to similar comments in this regulation and in DEP. What exactly does "solutions" mean in this context? **NL:** In both cases this would/could overlap with ENISA, whose task it is to support Member States **New IT:** Assistance to national public authorities should be deployed only when requested.
(c) supporting in particular public authorities in organising their public procurement, or carrying out procurement of state-of-the-art cybersecurity products and solutions on behalf of public authorities;	**SE**: ~~supporting in particular public authorities in organising their public procurement, or carrying out procurement of state-of-the-art cybersecurity products and solutions on behalf of public authorities~~ **NL:** ~~supporting in particular public~~	**SE**: What is meant by supporting here and how does it relate to the objectives of the national coordination centre? How will this be carried out in practice? How is this in line with the principle of subsidiarity? And concerning "carrying out procurement of state-of-the-art cybersecurity products and solutions on behalf of publiv authorities, how is this in line with the principle of subsidiarity? This must be for the MS to handle. – the Centre should not in itself engage in procurement of products. Why is this necessary? **NL:** In both cases this would/could overlap with

	~~authorities in organising their public procurement, or carrying out procurement of state-of-the-art cybersecurity products and solutions on behalf of public authorities;~~ **IT:** supporting in particular public authorities, <u>at their request</u>, in organising their public procurement, or carrying out procurement of state-of-the-art cybersecurity products and solutions on behalf of public authorities	ENISA, whose task it is to support Member States **PL:** An explanation with reference to the wording: "supporting public authorities in organising their public procurement or carrying out procurement in behalf of public authorities" is needed. How it would look like? **IT:** In alternative to the above suggested text, the proposal should better specify to whom the procurement is referred. **New IT:** The text of para c) is not clear. Is public procurement referred to national public procurement? In this case, any form of support for national public procurement must be approved by national authorities who are the only responsible for requesting it. **CZ:** We agree with SE comment and ask for clarification of what "supporting" means. **FR:** It would be helpful to have information from the Commission about cases in other sectors where the Union has carried out procurement on behalf of public authorities to illustrate this proposal.
(d) providing financial support and technical assistance to cybersecurity start-ups and SMEs to connect to potential markets and to attract investment;	**UK:** providing financial support and technical assistance to cybersecurity start-ups and SMEs to connect to potential markets and to attract investment <u>in a fair open and transparent manner;</u> **SE:** ~~providing financial support and technical assistance to cybersecurity start-ups and SMEs to connect to potential~~	**UK:** This change is to ensure trust of the wider community. **SE:** How will this be carried out in practice? This function is not at all suitable for the Centre, and is the role for the National Coordination

	~~markets and to attract investment~~;	Centres. Possibly the Competence Centre could coordinate the MS network in this task. Developing capacity to be able to provide direct support to a large number of businesses throughout Europe requires large manpower and niche expertise that cannot be established at Brussels-level, it must be in the MS. **DE:** What areas/tasks are being covered by the term "technical assistance"?

5. improve the understanding of cybersecurity and contribute to reducing skills gaps in the Union related to cybersecurity by carrying out the following tasks:	**UK:** improve the understanding of cybersecurity and contribute to reducing skills gaps in the Union related to cybersecurity by carrying out the following tasks <u>together with National Coordination Centres:</u>	**UK:** National Coordination Centres will be important to help deliver this work as they will be able to identify sector needs within their Member State and have closer access to the relevant infrastructures in order to help deliver the programmes. **DE:** In the area of Capacity Building the tasks of the Competence Centre overlap/clash with already existing competences/tasks of ENISA. **PL:** It is important not to overlap competences with such agencies like ENISA.
(a) supporting further development of cybersecurity skills , where appropriate together with relevant EU agencies and bodies including ENISA.	**UK:** supporting further development of cybersecurity skills , where appropriate together with <u>National coordination centres,</u> relevant EU agencies and bodies including ENISA.	
6. contribute to the reinforcement of cybersecurity research and development in the Union by:		**SE**: This has to be specified. On the 8th of October Commission said that **participating** MS will be part of defining programmes with calls that researchers from **all** MS can answer. Where is this information put in plain text? **DE:** It has to be clarified how the tasks of the Competence Centre are clearly separated from the tasks/competences of national institutions

(a) providing financial support to cybersecurity research efforts based on a common, continuously evaluated and improved multiannual strategic, industrial, technology and research agenda;	**SE**: through open calls that any member state can answer the centre will provide~~ing~~ financial support to cybersecurity research efforts based on a common, continuously evaluated and improved multiannual strategic, industrial, technology and research agenda;	**SE**: How? By calls? Who can answer calls? All bullets in this paragraph should be subject of open calls. **UK:** We would welcome clarification on how this will relate to ENISAs research efforts as well as ongoing work within the cPPP. **CZ:** We ask for further clarification of the system of providing support in this mean.
(b) support large-scale research and demonstration projects in next generation cybersecurity technological capabilities, in collaboration with the industry and the Network;		
(c) support research and innovation for standardisation in cybersecurity technology	**FR:** support research and innovation for standardisation **and** certification in cybersecurity technology	**FR:** Support should be provided to certification as well **PL:** Taking into consideration the Cybersecurity Act a special attention should be draw to the challenge of overlapping competences – Cybersecurity Act and ENISA.

7.	enhance cooperation between the civil and defence spheres with regard to dual use technologies and applications in cybersecurity, by carrying out the following tasks:	**SE:** ~~enhance cooperation between the civil and defence spheres with regard to dual use technologies and applications in cybersecurity, by carrying out the following tasks:~~ **FR:** ~~enhance cooperation between the civil and defence spheres with regard to dual use technologies and applications in cybersecurity, by carrying out the following tasks:~~	**SE**: SE understands the potential dual use, but stresses the importance of not spending money from Horizon Europe on military applications. SE is also hesitant to give the CCCN such a task at this point. SE consider that this proposal should not at this stage include direct references to military activities, as the CCCN is no yet establish, lacks structure and security measure etc. needed to manage military requirements. **FR:** Actions in the defence area are subject to specific rules defined in particular in the European Defence Industrial Development Programme. We therefore question the inclusion of the defence sphere within this proposal in particular in light of the absence of clearly defined eligible actions, the voting rules, and the existing funding programmes for defence. **UK:** It would be helpful to define what is meant by 'defence' in this context. **PL:** A special attention should be draw to the challenge of overlapping competences – EDA. **CZ:** We agree with SE and UK.

(a) supporting Member States and industrial and research stakeholders with regard to research, development and deployment;	**SE:** ~~supporting Member States and industrial and research stakeholders with regard to research, development and deployment;~~ **FR:** ~~supporting Member States and industrial and research stakeholders with regard to research, development and deployment;~~	**SE:** what does deployment mean in this context? For some areas this can potentially intrude on MS competence in terms of national security
(b) contributing to cooperation between Member States by supporting education, training and exercises ;	**SE:** ~~contributing to cooperation between Member States by supporting education, training and exercises ;~~ **FR:** ~~contributing to cooperation between Member States by supporting education, training and exercises ;~~	
(c) bringing together stakeholders, to foster synergies between civil and defence cyber security research and markets;	**SE:** ~~bringing together stakeholders, to foster synergies between civil and defence cyber security research and markets;~~ **FR:** ~~bringing together stakeholders, to foster synergies between civil and defence cyber security research and markets;~~	**SE:** Security arrangement etc is lacking to be able to deliver this in a secure way. Pls see related comments above

8.	enhance synergies between the civil and defence dimensions of cybersecurity in relation to the European Defence Fund by carrying out the following tasks:	**SE:** enhance synergies between the civil and defence dimensions of ~~cybersecurity~~ **when appropriated and agreed by MS** ~~in relation to the European Defence Fund by carrying out the following tasks:~~ **FR**: ~~enhance synergies between the civil and defence dimensions of cybersecurity in relation to the European Defence Fund by carrying out the following tasks:~~	**SE**: This is, as mentioned above, pending EDF negotiation. Given this and the concerns related to the capability to manage defence related issues, as commented above, SE does not, at this point, consider it appropriate to give the CCCN this task. This task also seems to go beyond the scope that is likely to be agreed in the EDF. The CCCN cannot go beyond the EDF regulation. **FR:** Actions in the defence area are subject to specific rules defined in particular in the European Defence Industrial Development Programme. We therefore question the inclusion of the defence sphere within this proposal in particular in light of the absence of clearly defined eligible actions, the voting rules, and the existing funding programmes for defence. **DE: We ask for a clear separation between the civil and defence** dimensions **of cybersecurity.** **PL:** A special attention should be drawn to the challenge of overlapping competences – EDA. Furthermore, further explanation is needed with regard to EDF.
	(a) providing advice, sharing expertise and facilitating collaboration among relevant stakeholders;	**FR:** ~~providing advice, sharing expertise and facilitating collaboration among relevant stakeholders;~~	

(b) managing multinational cyber defence projects, when requested by Member States, and thus acting as a project manager within the meaning of Regulation XXX [Regulation establishing the European Defence Fund].	**SE:** ~~managing multinational cyber defence projects, when requested by Member States, and thus acting as a project manager within the meaning of Regulation XXX [Regulation establishing the European Defence Fund].~~ **FR:** ~~managing multinational cyber defence projects, when requested by Member States, and thus acting as a project manager within the meaning of Regulation XXX [Regulation establishing the European Defence Fund].~~	**SE**: The CCCN is not specifically indicated in the EDF as such project manager, this goes beyond the EDF regulation as any such appointments lays in the hands of co-funding MS when relevant in the EDF. SE suggest that this is delete based on this and on previous indicated concerns regarding lacking capability to address/manage defence issues. **ES:** The outcome of the negotiation of the proposal for a Regulation of the EDF is still unknown. **DE:** The Competence Centre should not be granted such extensive competences in the area of defence projects.

Article 5 **Investment in and use of infrastructures, capabilities, products or solutions**		**SE:** In the COM proposal under the justification for it in terms of subsidiarity and proportionality principle a pan-European quantum communication network is mentioned, that could require EU investment of approximately EUR 900 million. What is this network, is it something that is decided to be developed? Shall those millions be taken from the posts from Horizon and Digital Europe that is being discussed? We thought that the budget posts in majority should be available for the MS. Our experience of the creation of new European systems is that it will always be significantly costlier than first estimated and that would affect the remaining amount of funds left for other measures by the MS.
1. Where the Competence Centre provides funding for infrastructures, capabilities, products or solutions pursuant to Article 4(3) and (4) in the form of a grant or a prize, the work plan of the Competence Centre may specify in particular:	**UK:** Where the Competence Centre provides funding for infrastructures, capabilities, products or solutions pursuant to Article 4(3) and (4) in the form of a grant or a prize, the work plan, <u>which should be made publicly available,</u> of the Competence Centre may specify in particular: **SE:** Where the Competence Centre provides funding for infrastructures, capabilities, products or solutions pursuant to Article 4(3) ~~and (4)~~ in the form of a grant or a prize, the work plan of the Competence Centre may specify in particular:	**UK:** To ensure the principles of openness and transparency are met. **SE:** Dependending on solution of above question. **NL:** See also Article 2. A clear(er) definition of what is meant by infrastructure is necessary in order to properly scope what can and cannot be done.

(a) rules governing the operation of an infrastructure or capability, including where relevant entrusting the operation to a hosting entity based on criteria that the Competence Centre shall define;		**SE**: Isn't this under the competence of the MS that gets that grant to decide and handle if it isn't a joint procurement as mentioned in 5.2?
(b) rules governing access to and use of an infrastructure or capability.		**SE**: Isn't this under the competence of the MS that gets that grant to decide and handle if it isn't a joint procurement as mentioned in 5.2?
	SE: (new c) rules governing that research products are compatible with the European Open Science Cloud (EOSC) and thereby openly available and re-usable for all Member States.	**SE**: In order to guarantee the greater impact in all member states of the commonly funded knowledge that will lay ground for an enhanced European cyber defence, the research output, both research data and publications, must follow principles of open access and re-usability without embargo periods (European Research Area priority 5).
2. The Competence Centre may be responsible for the overall execution of relevant joint procurement actions including pre-commercial procurements on behalf of members of the Network, members of the cybersecurity Competence Community, or other third parties representing the users of cybersecurity products and solutions. For this purpose, the Competence Centre may be assisted by one or more National Coordination Centres or members of the Cybersecurity Competence Community.		**SE**: "the Network" should be defined in article 1, so that it cannot be confused with other Network initiatives. **CZ:** We require to clarify the process of joint procurement actions. **NL:** How would procurement for commercial entities work? Is this not the responsibility of every actor themselves? **FR:** "other third parties" requires to be defined

Article 6 **Nomination of National Coordination Centres**	*Article 6* **Nomination of National ~~Coordination~~ <u>Competence</u> Centres** **(EE)**	
1. By [date], each Member State shall nominate the entity to act as the National Coordination Centre for the purposes of this Regulation and notify it to the Commission.		**SE**: Is there a preliminary time frame for the nomination date? What kind of entity can be most suitable for this task? Can you please provide with an example of a suitable organisation? A coordinating authority, university, research institute or something else? At the moment there is no given entity in Sweden suitable for these tasks. Therefore, we need quite a lot of time for this nomination process. **DK:** We support that Member States may choose which entity is appointed as the national coordination centre. **SK:** Article 6 Para 1 provides that each Member State shall nominate an entity, designated as National Coordination Centre for the purposes of this Regulation, until such time as not to be determined, and this nomination shall be notified to the Commission. Subsequently, Article 7 of the proposal deals with the tasks of the National Coordination Centres. SK would like to know the Commission's position, if it is possible that the national

		coordination centre under Article 6 of the proposal could be designated within the meaning of Article 8 Para 3 of the NIS Directive (as a national single point of contact) can set up national cyber security partnerships at both national and international level. This opinion is important for us despite the fact that it is a national competence. In that case the same national authority may be entrusted with the exercise of the future national coordination centre, by the Article 8 (3) of the NIS Directive, also implements the tasks of the single point of contact. ***Justification:*** The tasks of the National Coordination Centre within the meaning of the proposal may be in direct synergy with the tasks of the NCP within the meaning of the NIS Directive. The National Contact Point is capable of effectively engaging and coordinating its activities with the relevant sector, both public and private. It would be appropriate for both the national coordination centre and the tasks of the national single point of contact to be carried out by one institution/ enterprise.

2.	On the basis of an assessment concerning the compliance of that entity with the criteria laid down in paragraph 4, the Commission shall issue a decision within 6 months from the nomination transmitted by the Member State providing for the accreditation of the entity as a National Coordination Centre or rejecting the nomination. The list of National Coordination Centres shall be published by the Commission.	**FR:** ~~On the basis of an assessment concerning the compliance of that entity with the criteria laid down in paragraph 4, the Commission shall issue a decision within 6 months from the nomination transmitted by the Member State providing for the accreditation of the entity as a National Coordination Centre or rejecting the nomination. The list of National Coordination Centres shall be published by the Commission.~~	**FR:** We question the ground for the Commission to assess the nomination of the National Coordination centre and issue a decision. In particular the Commission at the same time gives flexibility to member states to decide which entity would be the most appropriate to play that role. We believe it would be more practical to clarify the criteria that this national coordination centre should meet rather than for the Commission to have this discretionary power. **DK:** As national coordination centres most likely will be selected among existing centres in member states, rather than established as new centres, the regulation should include a prioritized list of which skills/competencies the centres should possess. This would help make the process of accreditation – and possible rejection – more transparent. **ES:** The power to accept or reject the nomination of a National CC should be the competence of the Governing Board. Additionally, there are no objective and specific criteria to perform this assessment as Art. 3 just states the mission to be supported in general terms **DE:** The COM should not have the right to ultimately refuse a National Coordination Center that was nominated by a member state. Further, a list of clear criteria should be formulated in this regulation that defines requirements that have to be met in selecting a National Coordination Centre.

		PL: PL supports ES in their request for further explanation of the procedure of rejection of the nomination. There are no specific criteria to perform this task by the Commission. We agree with the ES that such a competence should be assigned to the Governing Board. **CZ:** We support DK remark on this provision.
3. Member States may at any time nominate a new entity as the National Coordination Centre for the purposes of this Regulation. Paragraphs 1 and 2 shall apply to nomination of any new entity.		**CZ:** We propose to set up the condition, that in one MS will be only one National Coordination Centre only.
4. The nominated National Coordination Centre shall have the capability to support the Competence Centre and the Network in fulfilling their mission laid out in Article 3 of this Regulation. They shall possess or have direct access to technological expertise in cybersecurity and be in a position to effectively engage and coordinate with industry, the public sector and the research community.	**DE:** The nominated National Coordination Centre shall have the capability to support the Competence Centre and the Network in fulfilling their mission laid out in Article 3 of this Regulation. They shall possess or have direct access to technological expertise in cybersecurity and be in a position to effectively engage and coordinate with industry, the public sector, the research community **and relevant civil society actors**.	**SE:** Can the national coordination centre be a national consortia?

5.	The relationship between the Competence Centre and the National Coordination Centres shall be based on a contractual agreement signed between the Competence Centre and each of the National Coordination Centres. The agreement shall provide for the rules governing the relationship and division of tasks between the Competence Centre and each National Coordination Centre.		**DE:** The contracts should be harmonized in their essential content. We ask that the COM present an example of such a contractual agreement - so that the content of such an agreement becomes apparent. **PL:** Bearing in mind the discussion during the HWP meeting on 28th September we would like to once again stress the need for one standard of contractual agreement, same for everyone. **NL:** Would this be after a negotiation process, or will it be the same for every centre? In case of the latter, what if no entity can be found willing to sign the contract. More general: what is the purpose of having a contract-based relationship? In the HWP meeting on October 9, it was hinted at by the Commission that there would be financing available for the operating of the coordination centre. Would that be part of the contract and can that be clarified?
6.	The National Coordination Centres Network shall be composed of all the National Coordination Centres nominated by the Member States.		

Article 7 **Tasks of the National Coordination Centres**	*Article 7* **Tasks of the National ~~Coordination~~ <u>Competence</u> Centres** **(EE)**	**SE**: It is unclear, as it is not mentioned in the article, if and how the National Coordination Centres (and the Cybersecurity Community) will have a part to play in the work of the Digital Innovation Hubs in DEP. Perhaps this could be amended by reference to the DIHs? **LV** : The outlined requirements for the National Centre requires a wide range of expertise - administrative capacity, specific ICT competence, they should be at the service of developers and operators in critical sectors as well as monitor the use of grants. Because of the fact that National Centres are involved in the distribution of finances, they themselves do not qualify for the grants. Therefore, Latvia sees that the tasks and capacity requirements for the National Coordination Centres would create a situation, where a highly qualified organisation would not be able to receive funding for projects they may wish to develop. Considering the general shortage of ICT security experts, this would impede Latvia's contribution to goals set out in Article 3, paragraph 1.

		ES: To be clarified how to solve the potential conflicts of interest within National Competence Centres (NCCs), which could act both as call managers and call beneficiaries. **PL:** This provision needs to be clarified with respect to how to solve the potential conflicts of interest within National Competence Centres (NCCs), which could act both as call managers and call beneficiaries. **EL:** Greece is concerned about the conflict of interest that exists for national centers regarding their ability to qualify for the grants. In that sense maybe it should be clarified whether the national centers can participate or not to the relevant calls and if these centers should be academic or governmental.
1. The National Coordination Centres shall have the following tasks:		**UK:** In addition to the tasks proposed, it might be helpful to have an evaluation or review for each centre assess progress against objectives.
(a) supporting the Competence Centre in achieving its objectives and in particular in coordinating the Cybersecurity Competence Community;	**UK:** supporting the Competence Centre in achieving its objectives and in particular in coordinating the Cybersecurity Competence Community; <u>in line with the Competence Centre's rolling work plan.</u>	**UK:** This change helps to provide alignment between the work of the National centres and the Centre. **CZ:** We would welcome a better clarification of what "supporting" means in this case.

(b) facilitating the participation of industry and other actors at the Member State level in cross-border projects;	**FR:** facilitating the participation of industry, **from the supply and the** demand **side** and other actors at the Member State level in cross-border projects;	**FR:** It echoes our more general comment on the need to clarify what is meant by industry, to ensure that we refer to the supply side of cybersecurity products, solutions and services, but also the demand side of those.
(c) contributing, together with the Competence Centre, to identifying and addressing sector-specific cyber security industrial challenges;	**LV**: Contributing, together with the Competence Centre, to identifying and addressing ~~sector-specific~~ cyber security industrial challenges in transport, energy, health, financial, government, telecom, manufacturing, defence, and space sectors. **FR:** contributing, together with the Competence Centre, **in particular the Commission contributions,** to identifying and addressing sector-specific cyber security industrial challenges;	**LV** : Here a clarification should be given on what is understood by "sector-specific", e.g. what sectors will the centre cover? If they are the sectors outlined in introductory point (14) (transport, energy, health, financial, government, telecom, manufacturing, defence, and space), a reference to the appropriate section of the document should be added. **FR:** Considering the composition of the Competence Centre as provided in Article 11, it is considered important to stress on the need for necessary inputs of competent DG of the Commission for this purpose. **DE:** The National Coordination Centres should also contribute to assessing potential negative impacts industrial solutions may have on fundamental rights and freedoms, including privacy rights.
(d) acting as contact point at the national level for the Cybersecurity Competence Community and the Competence Centre;		
(e) seeking to establish synergies with relevant activities at the national and regional level;		

	(f) implementing specific actions for which grants have been awarded by the Competence Centre, including through provision of financial support to third parties in line with Article 204 of Regulation XXX [new Financial Regulation] under conditions specified in the concerned grant agreements.		
	(g) promoting and disseminating the relevant outcomes of the work by the Network, the Cybersecurity Competence Community and the Competence Centre at national or regional level;	**SE**: promoting and disseminating the outcomes of the work by the Network, the Cybersecurity Competence Community and the Competence Centre at national or regional level <u>in benefit for the competitiveness that follows with principles of open science and open innovation</u>;	**SE**: In accordance with above comment on open science and open innovation all outcomes that can be disseminated should be disseminated. Only for reasons of personal integrity, national security and other reasons, the outcomes of research and innovation funded by the EU-budget should not be openly available and re-usable for Member States.
	(h) assessing requests by entities established in the same Member State as the Coordination Centre for becoming part of the Cybersecurity Competence Community.		
2.	For the purposes of point (f), the financial support to third parties may be provided in any of the forms specified in Article 125 of Regulation XXX [new Financial Regulation] including in the form of lump sums.		

3.	National Coordination Centres may receive a grant from the Union in accordance with Article 195 (d) of Regulation XXX [new Financial Regulation] in relation to carrying out the tasks laid down in this Article.		**FR:** We would like to have clarification on whether the grant would come from the Horizon Europe or Digital Europe budgets or from other sources.
4.	National Coordination Centres shall, where relevant, cooperate through the Network for the purpose of implementing tasks referred to in points (a), (b), (c), (e) and (g) of paragraph 1.		**DE:** What is meant by the term „Network“ here? **FR:** It is still very unclear how the network would be set up and function, although one of the key objectives of this proposal should be to facilitate the coordination between the industry and other actors in cross-border projects;

Article 8 **The Cybersecurity Competence Community**		**DE:** It has to be examined whether already existing national communities can be used here and whether the European cooperation can be organized through the networking of those national coordination centers. **NL:** How would any of this be enforced?
1. The Cybersecurity Competence Community shall contribute to the mission of the Competence Centre as laid down in Article 3 and enhance and disseminate cybersecurity expertise across the Union.		**FI:** While there are a number of clauses on the expected activities and contributions of the Cybersecurity Competence Community, it is unclear what the benefits of being a member of the Community will be, and what would motivate organizations to become members. **CZ:** We agree with FI. **NL:** How would any of this be enforced? **FR:** The European Commission explained at the Horizontal working party meeting that the Community would be managed at national level, although it is described here as having the role to disseminate expertise across the Union. There is a need to clarify the level at which the Community would operate.

2.	The Cybersecurity Competence Community shall consist of industry, academic and non-profit research organisations, and associations as well as public entities and other entities dealing with operational and technical matters. It shall bring together the main stakeholders with regard to cybersecurity technological and industrial capacities in the Union. It shall involve National Coordination Centres as well as Union institutions and bodies with relevant expertise..	**NL:** The Cybersecurity Competence Community ~~shall~~ **may** consist of industry, academic and non-profit research organisations, and associations as well as public entities and other entities dealing with operational and technical matters. It shall bring together the main stakeholders with regard to cybersecurity technological and industrial capacities in the Union. It shall involve National Coordination Centres as well as Union institutions and bodies with relevant expertise.. **UK:** The Cybersecurity Competence Community shall consist of industry, academic and non-profit research organisations, and associations as well as public entities and other entities dealing with operational and technical matters. It shall bring together the main stakeholders with regard to cybersecurity technological and industrial capacities in the Union. It shall involve National Coordination Centres as well as Union institutions and bodies with relevant expertise. The number of entities within the Community is intended to be flexible according to need. **DE:** The Cybersecurity Competence Community shall consist of industry, academic and non-profit research organisations, associations **and other relevant civil society actors** as well as public entities and other entities dealing with operational and technical matters. It shall	**NL:** This would have legal effect through shall but would not oblige any entity to participate. May would be better here. **UK:** It would be helpful to understand whether responsibility for identifying community members would lie with ECSO or National Coordination Centres. ECSO has real experience of coordinating an efficient public-private partnership and can cover tasks linked to governance and efficient support, including identifying community members. It would also be helpful to have an indication of whether there is a size limitation to the Community.

	bring together the main stakeholders with regard to cybersecurity technological and industrial capacities in the Union. It shall involve National Coordination Centres as well as Union institutions and bodies with relevant expertise.. **FR:** The Cybersecurity Competence Community shall consist **on the one hand** of industry, academic and non-profit research organisations, and associations as well as public entities and other entities dealing with operational and technical matters**, and on the other hand, where relevant, actors of other vertical sectors facing cybersecurity challenges** . It shall bring together the main stakeholders with regard to cybersecurity technological and industrial capacities in the Union. It shall involve National Coordination Centres as well as Union institutions and bodies with relevant expertise.	**FR:** It is suggested to integrate in a secondary perimeter of the Community actors from application fields of cybersecurity solutions, knowing that they might influence, with their needs, developments of the cybersecurity core business

3.	Only entities which are established within the Union may be accredited as members of the Cybersecurity Competence Community. They shall demonstrate that they have cybersecurity expertise with regard to at least one of the following domains:	**LV** : Only entities which are established within the Union may be accredited as members of the Cybersecurity Competence Community. Based on the criteria adopted by the Governing Board, they shall demonstrate that they have cybersecurity expertise with regard to at least one of the following domains: **FR:** Only entities which are established within the Union **and are effectively controlled by Member states and/or nationals of Member States** may be accredited as members of the Cybersecurity Competence Community. They shall demonstrate that they have cybersecurity expertise with regard to at least one of the following domains:	**LV** : This point lacks detail in regards to what criteria will determine sufficient expertise in one of the mentioned domains. For entities to be able to demonstrate their expertise, they should have an understanding what is taken into consideration. A reference should be added to Article 13, paragraph 3 (e). **UK:** It would be useful here to set out ECSO's role in the new configuration and how to avoid duplication. ECSO currently hold working groups in key areas and coordinate across public administrations (through NAPAC). Further, the current ECSO membership base is likely to have a similar perimeter to the proposed Community. **EE:** We disagree to accrediting only entities within the Union. The Union has close ties to EFTA countries for example, and they should have the right to participate in the Community, as well as apply to the existing calls. **FR:** This addition is required for the proposed regulation to meet the objectives set out in article 3
(a) research;			

	(b) industrial development;		
	(c) training and education.		
4.	The Competence Centre shall accredit entities established under national law as members of the Cybersecurity Competence Community after an assessment made by the National Coordination Centre of the Member State where the entity is established, on whether that entity meets the criteria provided for in paragraph 3. An accreditation shall not be limited in time but may be revoked by the Competence Centre at any time if it or the relevant National Coordination Centre considers that the entity does not fulfil the criteria set out in paragraph 3 or it falls under the relevant provisions set out in Article 136 of Regulation XXX [new financial regulation].	**NL:** The ~~Competence~~ relevant National Coordination Centre shall accredit entities established under national law as members of the Cybersecurity Competence Community after an assessment made by the National Coordination Centre of the Member State where the entity is established, on whether that entity meets the criteria provided for in paragraph 3. An accreditation shall not be limited in time but may be revoked by the ~~Competence Centre~~ at any time if ~~it or~~ the relevant National Coordination Centre considers that the entity does not fulfil the criteria set out in paragraph 3 or it falls under the relevant provisions set out in Article 136 of Regulation XXX [new financial regulation].	**NL:** Why would this go to the Competence Centre if the purpose is to create national communities? **LV :** See comments on paragraph 3. **FI:** As regards the accreditation of National Coordination Centres and members of the Cybersecurity Competence Community, the full control of the EC in both defining the accreditation criteria and assessing whether organizations meet the criteria (including the right to revoke accreditations) would not be an ideal solution. A better choice would be assigning an independent entity to take accreditation decisions (based on the criteria defined by the EC). A public sector driven network including a formal accreditation

		procedure would not be a desirable solution in the global and rapidly developing cyber security market. It should be ensured that the conditions for accreditation will be equal to all the companies and will not put companies in a different position e.g. based on their size. It appears that the current formulation would not support these objectives, neither does the procedure follow the usual accreditation practices (such as e.g. the accreditation for a pre-determined time). The responsibilities for defining the accreditation criteria and implementing the accreditation process should lie on two different actors. It is important to ensure the trust towards the actions and procedures, and avoid distortion of competition. **DK:** The Cybersecurity Competence Community appears to be open for all entities within EU but what is the application process and point of contact/entry for entities in non-participating member states? **UK:** We are concerned about the burden for the Competence Centre carrying out all the accreditation. We recommend either accreditation through: Peer accreditation process (as used by ECSO). National Coordination Centres with Competence Centre oversight (using guidelines which expand on para (3)). **ES:** This might imply a risk of fragmentation of the current European Community built by ECSO.

		DE: Why is a formal accreditation required at EU level? A formal accreditation leads to high administrative costs and no reason can be seen why this should be necessary. In our point of view it is sufficient to leave the responsibility to determine whether certain entities qualify as members of the Cybersecurity Competence Community to the national coordinating bodies. **PL:** The procedure to become a member of the Cybersecurity Competence Community is not transparent enough and does not respond to market needs. In this respect we support the advisory competence of the Industrial and Scientific Advisory Board in cooperation with national coordination centre. Following FI comment, the responsibilities for defining the accreditation criteria and implementing the accreditation process should be entrusted with two different actors. It is important to ensure the trust towards the actions and procedures, and avoid distortion of competition.

5. The Competence Centre shall accredit relevant 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. An accreditation 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].		**LV** : See comments on paragraph 3. **DE**: Same commentary as to no. 4
6. The representatives of the Commission may participate in the work of the Community.		
Article 9 **Tasks of the members of the Cybersecurity Competence Community**		**ES:** A link with ECSO is needed. **CZ:** We support ES position regarding ECSO.
The members of the Cybersecurity Competence Community shall:		**NL:** How is any of this enforceable? The members do not appear to have to sign any contract upon joining. Furthermore: given a member apparently takes on many obligations with no specific advantages listed here, why would anyone want to join

(1) support the Competence Centre in achieving the mission and the objectives laid down in Articles 3 and 4 and, for this purpose, work closely with the Competence Centre and the relevant National Coordinating Centres;		
(2) participate in activities promoted by the Competence Centre and National Coordination Centres;		**FI:** What does the participation mean in practice, and how to prove the participation? **CZ:** We would appreciate the clarification what the participation means in this provision.
(3) where relevant, participate in working groups established by the Governing Board of the Competence Centre to carry out specific activities as provided by the Competence Centre's work plan;		**NL:** How and by whom would this be determined? And what if any activity is relevant, but a member is for any reason unable to participate? **FR:** There should be clarification on the role of the „Network" and the future of ECSO, in particular ECSO's working groups to avoid the duplication of working groups and activities that would make it impossible for small entities to attend
(4) where relevant, support the Competence Centre and the National Coordination Centres in promoting specific projects;		

(5) promote and disseminate the relevant outcomes of the activities and projects carried out within the community.	**SE**: promote and disseminate the ~~relevant~~ outcomes of the activities and projects carried out within the community in benefit for the competitiveness that follows with principles of open science and open innovation	**SE**: See above
Article 10 **Cooperation of the Competence Centre with Union institutions, bodies, offices and agencies**	*Article 10* **Cooperation of the ~~Competence~~ Centre with Union institutions, bodies, offices and agencies** **(EE)**	**EE:** There should be clear provisions on how different Union institutions, bodies, offices and agencies will co-exist with the Centre to avoid unnecessary overlaps. **PL:** Following the EE comment, there should be clear provisions on how different Union institutions, bodies, offices and agencies will co-exist with the Centre in order to avoid unnecessary overlaps. Moreover, there is a need to set up cooperation baseline with Competence Centre between different Union institutions, bodies, offices and agencies. **CZ:** Concerning this article, we agree with EE.

1.	The Competence Centre shall cooperate with relevant Union institutions, bodies, offices and agencies including the European Union Agency for Network and Information Security, the Computer Emergency Response Team (CERT-EU), the European External Action Service, the Joint Research Centre of the Commission, the Research Executive Agency, Innovation and Networks Executive Agency, European Cybercrime Centre at Europol as well as the European Defence Agency		**SE:** How is the cooperation with ENISA intended to function? **EE:** Accordingly, we suggest to map the most problematic and crucial overlaps (not just list them) and explain how the Centre complements each of those bodies. If necessary, even describe concrete division of tasks, especially with ENISA. These provisions, explanations or task divisions can be listed as sub-paras: a) ENISA …; b) JRC …, c) Etc. **DE:** The cooperation with the mentioned organizations has to be defined in more detail. It has to be ensured that the new Competence Centre does not intervene in existing tasks/competences of those organizations. **CZ:** We propose to clarify and describe, how should ENISA cooperate with Competence Centre (agree with SE and EE comment on this para). **FR:** French authorities would like to know which type of cooperation with the executive agencies (eg. the Research ExecutiveAgency and the Innovation and Networks Executive Agency) is foreseen and in which respect would the missions and tasks of the Center differ from the tasks and missions of the executive agencies.

2.	Such cooperation shall take place within the framework of working arrangements. Those arrangements shall be submitted to the prior approval of the Commission.		
	CHAPTER II **ORGANISATION OF THE COMPETENCE CENTRE** *Article 11* **Membership and structure**		
1.	The members of the Competence Centre shall be the Union, represented by the Commission, and the Member States.		

2. The structure of the Competence Centre shall comprise:		
(a) a Governing Board which shall exercise the tasks set out in Article 13;		
(b) an Executive Director who shall exercise the tasks set out in Article 16;	**LV:** an Executive Director who shall exercise the tasks set out in Article ~~16~~ 17;	
(c) an Industrial and Scientific Advisory Board which shall exercise the functions set out in Article 20.		**FR:** There should be clarification from the European Commission on the future of ECSO as if ECSO continues its work, this board could create duplication

SECTION I **GOVERNING BOARD** *Article 12* **Composition of the Governing Board**		
1. The Governing Board shall be composed of one representative of each Member State, and five representatives of the Commission, on behalf of the Union.	**FR:** The Governing Board shall be composed of one representative of each Member State, and five representatives of the Commission, on behalf of the Union. ***Representatives of the Commission shall represent the different Directorate generals of the Commission involved in cybersecurity to ensure coordination and joint actions***	**FR:** Should the Commission have five representatives at the Governing board, they should come from the different DGS carrying out actions for cybersecurity, from the research, digital single market, justice and home affairs, growth, to the user's side. **EE:** We do not support having five Commission representatives in the Governing Board. It is uneven compared to the Member States. **DE:** Why should five representatives of the COM be sent to the Governing Board when the vote of the COM cannot be divided anyway (cf. Art 15(1))? This is especially critical as some quota (e.g. Art 14(2)) refer to the number of members of the board. **PL:** PL supports EE comment: five members appointed by the EC should be considered as a disproportionate representation in comparison to MSs. **CZ:** We propose to compose the Governing Board only of **one** representative of the Commission.

2.	Each member of the Governing Board shall have an alternate to represent them in their absence.		
3.	Members of the Governing Board and their alternates shall be appointed in light of their knowledge in the field of technology as well as of relevant managerial, administrative and budgetary skills. The Commission and the Member States shall make efforts to limit the turnover of their representatives in the Governing Board, in order to ensure continuity of the Board's work. The Commission and the Member States shall aim to achieve a balanced representation between men and women on the Governing Board.	**LV:** Members of the Governing Board and their alternates shall be appointed by the Member State in light of their knowledge in the field of technology as well as of relevant managerial, administrative and budgetary skills. The Commission and the Member States shall make efforts to limit the turnover of their representatives in the Governing Board, in order to ensure continuity of the Board's work. The Commission and the Member States shall aim to achieve a balanced representation between men and women on the Governing Board. **NL:** ~~Members of the Governing Board and their alternates shall be appointed in light of their knowledge in the field of technology as well as of relevant managerial, administrative and budgetary skills.~~ The Commission and the Member States shall make efforts to limit the turnover of their representatives in the Governing Board, in order to ensure continuity of the Board's work. The Commission and the Member States shall aim to achieve a balanced representation between men and women on the Governing Board.	**NL:** As this is the decision of each Member State, no further definition is necessary **DE:** Who should appoint the members of the Governing Board?

4.	The term of office of members of the Governing Board and of their alternates shall be four years. That term shall be renewable.		
5.	The Governing Board members shall act in the interest of the Competence Centre, safeguarding its goals and mission, identity, autonomy and coherence, in an independent and transparent way.	**SE:** The Governing Board members shall act in the interest of the ~~Competence Centre~~ European Union, safeguarding the Centres ~~its~~ goals and mission, identity, autonomy and coherence, in an independent and transparent way. **NL:** The Governing Board members shall act in the interest of the Competence Centre, safeguarding its goals and mission, identity, autonomy and coherence, ~~in an independent and transparent way~~.	**NL:** Would the MS representatives not primarily represent their member state In line with the above, can they be indepent? They represent their government **LV:** Here it should also be noted that the members are delegated by the Member States. Therefore, they inherently represent the interests of their respective countries. **PL:** PL supports EE comment, that all members of the Governing Board should have the right to invite observers, not only the Commission. **CZ:** We agree upon the LV remark. This requirement can be unrealizable.

6.	The Commission may invite observers, including representatives of relevant Union bodies, offices and agencies, to take part in the meetings of the Governing Board as appropriate.	**SE:** The ~~Commission~~ governing board may invite observers, including representatives of relevant Union bodies, offices and agencies, to take part in the meetings of the Governing Board as appropriate. **EE:** The Members of the Governing Board may invite observers, including representatives of relevant Union bodies, offices and agencies, to take part in the meetings of the Governing Board as appropriate. **NL:** The ~~Commission~~ Chair of the Governing Board may invite observers, including representatives of relevant Union bodies, offices and agencies, to take part in the meetings of the Governing Board as appropriate. **FR:** The Commission may invite observers, including representatives of relevant Union bodies, offices and agencies, **or on a proposal from the Member States,** to take part in the meetings of the Governing Board as appropriate.	**EE:** All Members of the Governing Board should have the right invite observers, not only the Commission. **CZ:** MS should have the same as the Commission to invite observers. **FR**: It is suggested that Member States could propose observers too.
7.	The European Agency for Network and Information Security (ENISA) shall be a permanent observer in the Governing Board.		**PL:** The role of ENISA as an observer should be defined in a more clear way.

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.		
	new 2a FR: The Commission, in its role on the Governing Board, shall seek to ensure coordination between the activities of the Center and the relevant activities of Horizon Europe, Digital Europe and other relevant programmes or instruments, with a view to promoting synergies	**FR:** It is suggested to add a new paragraph to stress the need for the Commission to ensure coordination between the activities of the Center and other Union programmes.
3. The Governing Board shall take the necessary strategic decisions, in particular:		**SE:** Requirements, responsibilities and accountability for security/ managing of sensitive/ EUCI is missing. Needed regardless if no military cyber issue is to be address. Defence would most likely require further requirements.

(a) adopt a multi-annual strategic plan, containing a statement of the major priorities and planned initiatives of the Competence Centre, including an estimate of financing needs and sources;		**FR**: It seems very necessary to make a clear link between the strategic plan and the deliverables of both Horizon Europe and Digital Europe programmes**.**
(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;		**FR:** It seems very necessary to make a clear link between the work plan and the deliverables of both Horizon Europe and Digital Europe programmes.
(c) adopt the specific financial rules of the Competence Centre in accordance with [Article 70 of the FR];		
(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;	**LV:** Within [time] of establishment of the Governing Board, adopt the criteria and procedures for assessing and accrediting the entities as members of the Cybersecurity Competence Community;	**LV** No entities can be assessed and accredited before this point has been completed, meaning that the rest of the project can not move forward. Therefore, this should be a priority and a deadline should be established by when these criteria are developed. **PL:** Similarly to the comment of LV after agreeing of the proposal there will be an urgent need of adoption of these criteria and procedures in order to move forward with the establishment of the Cybersecurity Competence Community. **CZ:** We agree with LV.

(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 regarding conflicts of interest;		
(i) establish working groups with members of the Cybersecurity Competence Community;		**FR:** If the community is managed at national level by the National coordination center, it seems that the EU added value would be the facilitation by the network of the participation of different national communities in crossborder projects ; Therefore it seems rather unclear what would be the outcome of national communities participating in working groups set up by the Competent center. It creates the risk to duplicate existing structures or working groups ;In addition, we see a clear risk of duplication if in parallel there are working groups of ECSO and working groups set up by the Center

(j) appoint members of the Industrial and Scientific Advisory Board;		**FR:** There should be clarification from the European Commission on the future of ECSO as if ECSO continues its work, this board could create duplication
(k) set up an Internal Auditing Function in accordance with Commission Delegated Regulation (EU) No 1271/2013[14];		
(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.		

[14] 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).

(o) where appropriate, establish implementing rules to the Staff Regulations and the Conditions of Employment in accordance with Article 31(3);		
	SE: **(new p)** Ensure that a gender perspective is applied in the preparation, implementation, monitoring and evaluation of the program.	
(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;		**SE:** See comments above, this need to be made in line with relevant regulations, which should be indicated in this regulation.
(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 financial contribution from Member States;	**EE:** ~~adopt the methodology to calculate the financial contribution from Member States~~	**EE:** The methodology to calculate the financial contribution from Member States shall be decided during the negotiation phase of the proposal and should not be left for the Governing Board to decide. Member States cannot reach a general approach to a proposal that does not clarify how much they will each need to

		contribute. This issue should be tackled under Chapter III Financial Provisions. **FI:** Although it may still be pre-mature to estimate the divide of costs at this stage of the MFF-negotiations, it is important for MSs to have impact on the mechanism. What would be the alternatives and are there examples on how to calculate the MS financial contribution? **PL:** PL supports EE that the methodology to calculate the financial contribution from Member States shall be decided during the negotiation phase of the proposal and should not be left for the Governing Board to decide. Member States cannot reach a general approach to a proposal that does not clarify how much they will each need to contribute. This issue should be tackled under Chapter III Financial Provisions. **CZ:** We agree upon the EE comment – the calculation of financial contribution should be defined in the regulation, before it will come into force.
	SK: adopt the methodology to calculate the financial contribution from participating Member States;	**SK:** In Article 13 Para 3 letter s) we propose to insert the word "participating" after the word "contribution". This is to clarify the meaning and the difference between the participating Member State and the Member State as such. **FR:** To avoid ambiguity, the finality of this financial contribution should be specified

(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;		
Article 14 **Chairperson and Meetings of the Governing Board**		
1. The Governing Board shall elect a Chairperson and a Deputy Chairperson from among the members with voting rights, for a period of two years. The mandate of the Chairperson and the Deputy Chairperson may be extended once, following a decision by the Governing Board. If, however, their membership of the Governing Board ends at any time during their term of office, their term of office shall automatically expire on that date. The Deputy Chairperson shall *ex officio* replace the Chairperson if the latter is unable to attend to his or her duties. The Chairperson shall take part in the voting.		

2.	The Governing Board shall hold its ordinary meetings at least three times a year. It may hold extraordinary meetings at the request of the Commission, at the request of one third of all its members, at the request of the chair, or at the request of the Executive Director in the fulfilment of his/her tasks.	**DE:** Proposal: "... or at the request of one third of the members sent by the MS"	**DE:** As long as COM has the proposed number of 5 seats in the Board, it would have too much influence on this possibility otherwise.
3.	The Executive Director shall take part in the deliberations, unless decided otherwise by the Governing Board, but shall have no voting rights. The Governing Board may invite, on a case-by-case basis, other persons to attend its meetings as observers.		
4.	Members of the Industrial and Scientific Advisory Board may take part, upon invitation from the Chairperson, in the meetings of the Governing Board, without voting rights.		
5.	The members of the Governing Board and their alternates may, subject to its rules of procedure, be assisted at the meetings by advisers or experts.		
6.	The Competence Centre shall provide the secretariat for the Governing Board.		

Article 15 **Voting rules of the Governing Board**		**FI:** As regards the role of the EU in voting and the share of control, some further information would be useful whether this is in line with other similar type of regulations and entities. In practice, the 50% of the EU control over the ECCC means a veto right of the EU on the ECCC decisions. It is important to ensure that there will be a significant role for the MSs in the decision making. Moreover, the interest of the European industry towards the ECCC and NNCC could be higher with a more balanced voting rights and the participation of the European industry in the Governing Board. **DE: <u>The voting rights are unacceptable for Germany</u>**. The COM would have 50% of the voting rights. The COM thereby has a right of veto which is not acceptable. **CZ:** The 50% of the EU control over the ECCC means a veto right of the EU on the ECCC decisions. This is the fact we cannot agree with. Especially because the national security, which is substantially related to the concern of this regulation, is national interest. Therefore, Member States should be primarily able to decide without to be overrated by Commission. Furthermore, the MS are participating on the budget of Horizon Europe and other funding programs. This means, there is a double financial contribution of MS. Under this circumstances, a distribution of voting rights, as proposed, would be unfair. We agree upon FI and EE remarks.

		We propose to change the voting system as following: Union has 20% of voting rights, MS have 80% of voting rights. **NL:** NL maintains general scrutiny reservation and on this article **SE:** Please see comment above requesting examples of how the voting procedure could pan out in reality.
	New 1 SE: The representatives of the members of the Governing Board shall make every effort to achieve consensus. Failing consensus, a vote shall be held.	**SE:** New §1 for voting rules, like the one in the JU of the EuroHPC
1. The Union shall hold 50 % of the voting rights. The voting rights of the Union shall be indivisible.	**EE:** ~~The Union shall hold 50 % of the voting rights.~~ Every member of the Governing Board shall have one vote. The voting rights of the Union shall be indivisible. **FR:** **~~The Union shall hold 50 % of the voting rights. The voting rights of the Union shall be indivisible.~~** **„Each representative of t~~-~~he Union shall have one vote. The voting rights of t~~-~~he Union shall be ~~indivisible.~~“**	**EE:** We do not agree to the Commission having 50% of the voting rights. Despite the Commission being the “guardian” of the Union budget, Member States are the ones who fill the budget, so indirectly they are also responsible for it. Additionally, each Member State also needs to contribute directly. **FR:** We do not support that the Union would have 50% of the votes and Member states the other 50%. What is more, cybersecurity is a sensitive national interest that requires Member States to have a majority vote in the Governing Board. **PL:** Following previous PL comments, 50% of the votes for EC represent disproportionate representation in comparison to MSs. EC can block any decision made by MSs, which raises our concerns, among other things, due to the fact

		that MSs contribute to the budget for example through programs such as Digital Europe. **NL:** Further clarification and study is needed here. NL at this point is not convinced we should deviate here from established rules in for example the Horizon 2020 program What are the exact arguments for 50% voting rights for the Commission **New IT:** Italy welcomes further discussions aimed at evaluating possible review of the voting system within Governing Board in order to provide Member States with more voting power.
2. Every participating Member State shall hold one vote.	**SE:** Every ~~participating~~ Member State shall hold one vote.	**SE:** Since money is taken from the MFF programs (Horizon Europe and Digital Europe) all MS should have a vote. **PL:** Following previous comments each MS should hold the vote right as all of them contribute to the budget that will cover Competence Centre expenses. We support SE position in this point. **NL:** Union funds come from the Member States so naturally they should have a vote in how those funds are spent, regardless of any additional voluntary contributions.

3.	The Governing Board shall take its decisions by a majority of at least 75% of all votes, including the votes of the members who are absent, representing at least 75% of the total financial contributions to the Competence Centre. The financial contribution will be calculated based on the estimated expenditures proposed by the Member States referred to in point c of Article 17(2) and based on the report on the value of the contributions of the participating Member States referred to in Article 22(5).		**SE:** The calculation of the financial contribution must be clarified. **PL:** The voting procedure should be discussed only when all the details regarding voting rights are clarified. This means, following SE comment, that the calculation of the financial contribution must be clarified. **CZ:** We agree with SE. **NL:** This needs further clarification and study, **FR:** We do not support that the Union would have 50% of the votes and Member states the other 50% and the majority rule proposed. The linkage between the majority rule and the financial contribution is not acceptable as it stands given the lack of clarity regarding the contribution that would be expected from each member state. In addition, the voting rules as proposed would make it very difficult to agree on non-consensual topics and would not encourage Member states to work together since the Commission would hold so much voting power.

4. Only the representatives of the Commission and the representatives of the participating Member States shall hold voting rights.	**SE:** ~~Only the representatives of the Commission and the representatives of the participating Member States shall hold voting rights.~~ **NL:** ~~Only the representatives of t~~**T**he Commission and the representatives of the ~~participating~~ **every** Member States shall hold voting rights.	**SE:** The initiative is too big and important not to involve all MS. **NL:** Inconsistent with para 1 of this article. The commission vote is indivisible and quantified at 50%. Not every representative of the Commission can therefore vote separately. **PL:** See above comments.
5. The Chairperson shall take part in the voting.		**ES:** A rationale is needed.
SECTION II **EXECUTIVE DIRECTOR** *Article 16*		
Appointment, dismissal or extension of the term of office of the Executive Director		
1. The Executive Director shall be a person with expertise and high reputation in the areas where the Competence Centre operates.		
2. The Executive Director shall be engaged as a temporary agent of the Competence Centre under Article 2(a) of the Conditions of Employment of Other Servants.		

3.	The Executive Director shall be appointed by the Governing Board from a list of candidates proposed by the Commission, following an open and transparent selection procedure.	**FR:** The Executive Director shall be appointed by the Governing Board from a list of candidates proposed by the Commission, following an open and transparent selection procedure **defined in collaboration with the Member states**	**PL:** MSs and EC should keep the same right to propose a candidate as both are financially contributing to the initiative.
4.	For the purpose of concluding the contract of the Executive Director, the Competence Centre shall be represented by the Chairperson of the Governing Board.		
5.	The term of office of the Executive Director shall be four years. By the end of that period, the Commission shall carry out an assessment which takes into account the evaluation of the performance of the Executive Director and the Competence Centre's future tasks and challenges.		
6.	The Governing Board may, acting on a proposal from the Commission which takes into account the assessment referred to in paragraph 5, extend once the term of office of the Executive Director for no more than four years.		
7.	An Executive Director whose term of office has been extended may not participate in another selection procedure for the same post.		

8.	The Executive Director shall be removed from office only by decision of the Governing Board, acting on a proposal from the Commission.		**NL:** Is it correct that this decision making procedure is still to be established in the rules of the procedure of the Governing Board?
	Article 17 **Tasks of the Executive Director**		
1.	The Executive Director shall be responsible for operations and for the day-to-day management of the Competence Centre and shall be its legal representative. The Executive Director shall be accountable to the Governing Board and perform his or her duties with complete independence within the powers assigned to him or her.		
2.	The Executive Director shall in particular carry out the following tasks in an independent manner:		
	(a) implement the decisions adopted by the Governing Board;		
	(b) support the Governing Board its work, provide the secretariat for their meetings and supply all information necessary for the performance of their duties;		

(c) after consultation with the Governing Board and the Commission, prepare and submit for adoption to the Governing Board the draft multiannual strategic plan and the draft annual work plan 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 plan and the corresponding expenditure estimates as proposed by the Member States and the Commission;		**PL:** To increase and balance the powers also the Industrial Advisory Board should be consulted by the Director. This way industry will make a significant input in the draft multiannual strategic plan and the draft annual work plan. The final decision to include comments remains with the Governing Board.
(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 plan and report to the Governing Board thereon;		
(f) prepare the draft annual activity report on the Competence Centre, including the information on corresponding expenditure;		

(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		
(i) prepare, negotiate and conclude the agreements with the National Coordination Centres;		**SE**: What agreements? Give example please. What is the reason behind negotiating different agreements with national coordination centres? **PL:** The idea was to have one standard agreement in order to make the process more transparent and equal. Why then negotiate a form of an agreement agreed before? **CZ:** We agree with SE.
(j) be responsible for administrative, financial and staff matters, including the implementation of the Competence Centre budget, taking due account of advice received from the Internal Auditing Function, within the limits of the delegation by the Governing Board;		

(k) approve and manage the launch of calls for proposals, in accordance with the work plan 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;		**PL:** Please elaborate more on the subject and way of procedure. It is unclear now.
(m) approve and manage the launch of calls for tenders, in accordance with the work plan 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;		
(x) perform any other tasks entrusted or delegated to him or her by the Governing Board.		

SECTION III **INDUSTRIAL AND SCIENTIFIC ADVISORY BOARD** *Article 18* **Composition of the Industrial and Scientific Advisory Board**	**DE:** Erase Articles 18-20	**DE:** Comments on Art. 18-20: The Industrial and Scientific Advisory Board is **not necessary** in addition to the Cybersecurity Competence Community. Any necessary advice the Centre should need, ought to be available throught this Network (by informal working groups e.g.). Moreover the fact that not all MS can be represented in the Board might lead to unnecessary conflicts. It should be sufficient that the Competence Centre in accordance with Governing Board establishes working groups for subject-specific tasks. If the Competence Centre should ever express the need for a more sustainable structured general advisory board, this could be impelemented through the Governing Board and, thus, has not to be regulated here. **NL:** A proper discussion on how to involve the expertise of the private sector is necessary. As it is set up through this article, it would involve only a very small part of the Community in any kind of significant way. **FR:** There should be clarification from the European Commission on the future of ECSO as this board could create duplication with their existing work. The four pilots projects selected also have as objective to gather the industrial and research community, in particular to develop a research roadmap. We should therefore see whether it would be possible to use the existing before creating something new.

1.	The Industrial and Scientific Advisory Board shall consist of no more than 16 members. The members shall be appointed by the Governing Board from among the representatives of the entities of the Cybersecurity Competence Community.	**SE**: The Industrial and Scientific Advisory Board shall consist of no more than 16 members. The members shall be appointed by the Governing Board from among the representatives of the entities of the Cybersecurity Competence Community, with consideration of a gender balance.	**SE:** Why 16 and not 27? **FI:** The number of the Advisory Board members appears relatively low when considering the expertise required. **FR:** The number of members shall be adapted to the variety of cybersecurity activities and know-how at European level
2.	Members of the Industrial and Scientific Advisory Board shall have expertise either with regard to cybersecurity research, industrial development, professional services or the deployment thereof. The requirements for such expertise shall be further specified by the Governing Board.		

3.	Procedures concerning the appointment of its members by the Governing Board and the operation of the Advisory Board, shall be specified in the Competence Centre's rules of procedure and shall be made public.		**EE:** We believe it should be clarified how the appointment of the Advisory Board will take place, considering that they play quite a huge role in defining the agenda for the Centre. There could be different criteria for the appointment of the Advisory Board Members, such as 1) geographical balance (making sure all regions of Europe are represented) and 2) scientific vs industrial members (balanced number of advisors from academia and private sector). **PL:** The balance between: regions and sizes of the company should be achieved. The Advisory Board should consist of members, among others, from start-ups, small and medium companies. In this point we support EE position. **CZ:** We agree with EE.
4.	The term of office of members of the Industrial and Scientific Advisory Board shall be three years. That term shall be renewable.	**NL:** The term of office of members of the Industrial and Scientific Advisory Board shall be three years. That term shall be renewable **once**.	**NL:** There should a term limit to ensure rotation and new perspectives.

5. Representatives of the Commission and of the European Network and Information Security Agency may participate in and support the works of the Industrial and Scientific Advisory Board.		**SE:** Access rights etc to sensitive information? Confidentiality requirements?
Article 19 **Functioning of the Industrial and Scientific Advisory Board**		**CZ:** We propose to grant ESCO one chair in the Industrial and Scientific Advisory Board, as it is an important authority with plenty of experiences and ability to qualified contribute to this board.
1. The Industrial and Scientific Advisory Board shall meet at least twice a year.		
2. The Industrial and Scientific Advisory Board may advise the Governing Board on the establishment of working groups on specific issues relevant to the work of the Competence Centre where necessary under the overall coordination of one or more members of the Industrial and Scientific Advisory Board.		
3. The Industrial and Scientific Advisory Board shall elect its chair.		
4. The Industrial and Scientific Advisory Board shall adopt its rules of procedure, including the nomination of the representatives that shall represent the Advisory Board where relevant and the duration of their nomination.		

Article 20 **Tasks of the Industrial and Scientific Advisory Board**		
The Industrial and Scientific Advisory Board shall advise the Competence Centre in respect of the performance of its activities and shall: (1) provide to the Executive Director and the Governing Board strategic advice and input for drafting the work plan and multi-annual strategic plan within the deadlines set by the Governing Board;		
(2) organise public consultations open to all public and private stakeholders having an interest in the field of cybersecurity, in order to collect input for the strategic advice referred to in paragraph 1;		
(3) promote and collect feedback on the work plan and multi-annual strategic plan of the Competence Centre.		

CHAPTER III **FINANCIAL PROVISIONS**		**SK:** SK has reservations regarding the method of compulsory collection of contributions to cover administrative and operating costs from the participating Member States, which should not exceed the amount of approximately 23.75 million Euro from 2021 to 2027. We believe that the MS should not be compelled to make a mandatory contribution to the functioning of the system and structure in the EU, in addition to own resources outside the budget of EU, which is to be up to 50%. In addition, the arrangement also includes sanctioning the MS for non-fulfillment of financial obligations by withdrawal of voting rights or other sanctions. SK understands the reason for the complementarity and additionality of MS payments to maintain the system, but we would like to look into the possibility that the operation of the European Competence Centre can be secured in other ways. We would therefore like to get an explanation why the Commission did not go any further. Another unknown element is the method of determining the level of proportional payments of MS. Which key will be determined? The Commission's references for determining this key by Article 17 Para 2 letter c) and Article 22 Para 4 does not seem sufficient to us. Nor does it seem appropriate for us to vote at least 75% of all votes, including abstentions, of at least 75% of the total financial contributions to the European Competence Centre. We are afraid that in this way larger countries, which could contribute even more, could simply denounce smaller MSs. We would therefore prefer a more

		proportionate and fairer mechanism.

Article 21 **Union financial contribution**		**LV** Regarding finances, Latvia would like to get a clarification on the following: According to the regulation, the Competence Centre is financed both from the EU budget and bilaterally by the Member States. Yet, only the Member States, which have made bilateral contributions, will have voting rights in the Governing Board. This can potentially create a situation where only Member States, which have made separate contributions, will be able to make decisions on resource distribution, even though the Competence Centre is also financed from the EU's budget, to which all Member States contribute. **EE:** As a general remark, the Union financial contribution should focus on enhancing research, development and innovation done by the Network of the Competence Centres and amplify the contributions of the Member States and other relevant stakeholders not vice versa. National contributions (especially voluntary ones) shall benefit and amplify the Member State's own ongoing R&D and PPP activities, as well as support the local ecosystem. **DE:** On what budgetary basis can a fixed sub-budget (a) from Horizon Europe be allocated to the competence centre, which is then to be supplemented by a sub-budget (b) from the same programe (!) that has not yet been fixed? Note: The level of the budget for Horizon Europe depends on the negotiations on the EU's Multiannual Financial Framework (MFF).

		Negotiations on the MFF are currently ongoing. **PL:** PL supports LV comment. Money comes from programs to which MSs contribute. More clarification is needed. **CZ:** We agree with LV. **SK:** SK has doubts that setting out this mechanism on financial contribution is perceived as inadequate. That provision of Article 21 is confusing and not sufficiently formalized because the financial limits given here are only indicative and not realistically approved. **NL:** This article cannot be completed before the discussions on the Multi-Annual Financial Framework are completed Next to a general MFF decision, the discussions in the two sectoral programme s Digitale Europe and Horizon 2020 should be completed first, this regulation should be in line with that outcome
1. The Union's contribution to the Competence Centre to cover administrative costs and operational costs shall comprise the following:		**SE:** Would not funds from DEP be able to help fund National Competence Centres and activities they will be involved, for example with cross-border dimensions? **NL:** See also Article 2, a clear definition of what this is is necessary

(a) EUR 1 981 668 000 from the Digital Europe Programme, including up to EUR 23 746 000 for administrative costs;	**SE:** EUR 1 981 668 000 from the Digital Europe Programme, ~~including~~ and above that up to EUR 23 746 000 for administrative costs; **DE: [**EUR 1 981 668 000**]** from the Digital Europe Programme, including up to **[**EUR 23 746 000**]** for administrative costs; **NL:** EUR 1 981 668 000 from the Digital Europe Programme, including ~~up to EUR 23 746 000 for~~ the full administrative costs of the Competence Centre; **FR: A part of** EUR 1 981 668 000 from the Digital Europe Programme, including up to EUR 23 746 000 for administrative costs;	**SE:** How is this in line with proportionality? How is the big amount motivated? All specified amounts are the subject of negotiations in the special working party on budget affairs and are not to be negotiated here. The regulation should be drafted in a way as to be able to accommodate different outcomes from those negotiations. **DE:** Scrutiny reservation. The actual numbers have to be discussed within the MFR group. However, we ask the COM to explain how the share of administrative costs has been calculated and why it is necessary to have a specific number in the text. Until a final decision about the MFF 2021-2017 is reached, any information about the unions financial contribution has to be put in brackets. **NL:** As this entire proposal cannot work without the Competence Centre is funding cannot be based partly on voluntary contributions, but needs to be guaranteed. **FR:** Without prejudice of Multiannual Financial Framework 2012-2017 discussions.

(b) An amount from the Horizon Europe Programme, including for administrative costs, to be determined taking into account the strategic planning process to be carried out pursuant to Article 6(6) of Regulation XXX [Horizon Europe Regulation].	**FR:** An amount from the Horizon Europe Programme, including for administrative costs, to be determined ~~taking into account~~**by** the strategic plan~~ning process~~as **defined in Article 4a of Decision XXX** ~~to be carried out pursuant to Article 6(6) of Regulation XXX~~ [Horizon Europe ~~**Regulations**~~**specific programme Decision],**	**FR:** The specific amount should be determined by the Strategic plan. At the Competitivity Council of September, it was decided by the Ministers that the strategic planning process would be followed up by a strategic plan adopted as an implementing act **DK:** The proposal of this regulation should not prejudge the negotiations on the next MFF, including sectoral proposals on Horizon Europe and Digital Europe **DE:** The strategic planning process has not yet started - relying on its results therefore seems premature. **CZ:** We agree with DK.

2.	The maximum Union contribution shall be paid from the appropriations in the general budget of the Union allocated to [Digital Europe Programme] and to the specific programme implementing Horizon Europe, established by Decision XXX.		**ES:** Digital Europe and Horizon Europe Programmes are currently under discussion in different Council configurations (Telecom and Competitiveness). Furthermore, the strategic committee on Horizon2020 has set up a working group to review any kind of Joint Undertaking, before launching any other in Horizon Europe. **DE:** Scrutiny reservation. It is unclear to us, how the financial mix adds up to a final sum and how much money will actually be assigned to the center and its activities. We ask the COM to provide more information on that article. **NL:** This should be in line/ a decision should be taken after a decision of the Horizon 2020 Strategic group and DEP as in article 21.1
3.	The Competence Centre shall implement cybersecurity actions of [Digital Europe Programme] and [Horizon Europe Programme] in accordance with point (c) (iv) of Article 62 of Regulation (EU, Euratom) XXX[15] [the financial regulation].	**FR:** The Competence Centre shall implement specific cybersecurity actions of [Digital Europe Programme] and of the [Horizon Europe Programme] in accordance with point (c) (iv) of Article 62 of Regulation (EU, Euratom) XXX [the financial regulation]	**FR:** Similar to our comments to recital 15, article 1 paragraph 2 and article 4 paragraph 2 the French authorities would like to ask the Presidency to clarify what is meant with the "term" implementation to better understand whether it means that the Center would perform the tasks related to the evaluation, follow-up and management of projects
4.	The Union financial contribution shall not cover the tasks referred to in Article 4(8)(b)		

[15] [add full title and OJ reference]

Article 22 **Contributions of participating Member States**		**EE**: The methodology to calculate the financial contribution from Member States should be decided and described here. **ES:** The Member States' co-funding proposal described in this article may imply some inconvenience for certain Member States that won't be able to face the financial commitments to participate in the initiative, due to national budgetary restrictions. **DE:** COM should provide an overview of the cost distribution of the funding of the Center of Competence between the Member States and the EU. How is the Competence Centre's steering structure compatible with the different control structures of the "Horizon Europe" and the "Digital Europe" programs, from which funds are also being taken? **PL:** Following previous comments PL supports DK in their comment to para 1. It should be clarified whether the separate MSs contributions are included in contribution to existing proposals of Horizon and Digital Europe. **IT:** Financial contributions in cash and in-kind from Member States should be better specified into the text of the regulation. A chart detailing financial impact for single Member State -as discussed in the HWP meetings- would be necessary. **New IT:** Financial amounts in cash from Member States should be specified into the text.

		Contributions in-kind should also be better detailed. More details on financial impact for single Member State are necessary. **SK:** SK is of the opinion that provision of Article 22 in direct connection with Article 21 is confusing and not sufficiently formalized. Regarding Member States it is double financial burden because the Union budget is made up of Member States' financial contributions, and this provision makes the Member State conditional on a contribution to cover the operational and administrative costs of the European Competence Centre if the Member State wants to play an active role in management.
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.	**SE**: The participating Member States ~~shall~~ are anticipated to 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. **NL:** 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.	**SE**: The participating Member States' financial participation should be *commensurate* to the Union's financial contribution to this initiative. SE questions why in this case the commensurate contribution must be "at least the same amounts" as the Union financial contribution. **NL:** We would like to have more clarification in the text and recitals: 1. The way this is formulated , contribution is not voluntary at all. If you participate, you pay at least some amount. 2. In this way, the less MSs participate, the more each participant pays. This is not a favourable set-up if you want to stimulate

		participation, 3. This set-up opens a whole new arena of negotiations (that is, between potentially participating MSs). This means costs, this means less inclination to participate. See above. Full funding for the Centre needs to be guaranteed **FI:** Cf. comments to art 13.3 s) **DK:** It should be clarified whether the contribution is a separate MS contribution or included in contributions to existing proposals of Horizon 2020 and Digital Europe. Furthermore it should be clarified whether the administrative costs of national coordination centres should be subtracted from members states' contributions, or whether this is an additional cost covered by member states themselves. **EE:** The calculation of the total contribution of the Member States should be based on [XX methodology]. **DE:** The Centre's expenditure should be taken into account in the financial programming of the EU budget and not co-financed from national budgets. **PL:** First the decision should be made on a mechanism of contribution and next it should be decided who and how much contribute. PL supports EE comment requesting methodology and SE comment asking for more clarification. **CZ:** We propose to clarify whether the

		contribution is a separate MS contribution or included in contributions to existing proposals of Horizon 2020 and Digital Europe. Same way it is necessary to clarify the methodology of calculation of the financial contribution.

2.	For the purpose of assessing the contributions referred to in paragraph 1 and in point (b)ii of Article 23(3), the costs shall be determined in accordance with the usual cost accounting practices of the Member States concerned, the applicable accounting standards of the Member State, and the applicable International Accounting Standards and International Financial Reporting Standards. The costs shall be certified by an independent external auditor appointed by the Member State concerned. The valuation method may be verified by the Competence Centre should there be any uncertainty arising from the certification.		**SE**: Please clarify how member states contribution can be calculated. **PL:** Presented methodology does not increase the level of clarity and generates additional cost for MSs. It also does not describe verification procedure by the Competence Centre.

3.	Should any participating Member State be in default of its commitments concerning its financial contribution, the Executive Director shall put this in writing and shall set a reasonable period within which such default shall be remedied. If the situation is not remedied within that period, the Executive Director shall convene a meeting of the Governing Board to decide whether the defaulting participating Member State's right to vote is to be revoked or whether any other measures are to be taken until its obligations have been met. The defaulting Member State's voting rights shall be suspended until the default of its commitments is remedied.		**PL:** Please see previous comments on voting rights and financial contribution.

4. The Commission may terminate, proportionally reduce or suspend the Union's financial contribution to the Competence Centre if the participating Member States do not contribute, contribute only partially or contribute late with regard to the contributions referred to in paragraph 1.		
5. The participating Member States shall report by 31 January each year to the Governing Board on the value of the contributions referred to in paragraphs 1 made in each of the previous financial year.		**PL:** A used term "value of the contributions" is unclear and it can potentially create challenges in assessment of the value of each report.
Article 23 **Costs and resources of the Competence Centre**		**PL:** Please see previous comments on financial contributions.
1. The Competence Centre shall be jointly funded by the Union and Member States through financial contributions paid in instalments and contributions consisting of costs incurred by National Coordination Centres and beneficiaries in implementing actions that are not reimbursed by the Competence Centre.		**FI:** Would this mean that implementing national cybersecurity research and development actions could be considered as a contribution for these actions? **DE:** To what extent can additional expenditure be incurred by the national coordination centres?

2.	The administrative costs of the Competence Centre shall not exceed EUR [number] and shall be covered by means of financial contributions divided equally on an annual basis between the Union and the participating Member States. If part of the contribution for administrative costs is not used, it may be made available to cover the operational costs of the Competence Centre.	**NL:** The administrative costs of the Competence Centre shall not exceed EUR [number] and shall be covered by means of financial contributions ~~divided equally on an annual basis between~~**from** the Union ~~and the participating Member States.~~ If part of the contribution for administrative costs is not used, it may be made available to cover the operational costs of the Competence Centre.	**NL:** The proposed calculation should be further described and specified in this artcile (in the regulation itself , not in the recitals)
3.	The operational costs of the Competence Centre shall be covered by means of:		
	(a) the Union's financial contribution;		
	(b) contributions from the participating Member States in the form of:		
	(i) Financial contributions; and (ii) where relevant, in-kind contributions by the participating Member States of the costs incurred by National Coordination Centres and beneficiaries in implementing indirect actions less the contribution of the Competence Centre and any other Union contribution to those costs;		**SE**: What can in-kind contributions be? Working hours, technical infra? **DK:** It should be further clarified what is meant by in-kind contributions. Would that include co-financing in terms of hours spent on a relevant project? **PL:** PL supports DK and SE comment. The issue of « in-kind » contributions in unclear for us. **CZ:** We ask for further clarification of what "contributions" mean.

4.	The resources of the Competence Centre entered into its budget shall be composed of the following contributions:		
	(a) participating Member States' financial contributions to the administrative costs;		
	(b) participating Member States' financial contributions to the operational costs;		
	(c) any revenue generated by Competence Centre;		**SE:** From where can such revenue arise?
	(d) any other financial contributions, resources and revenues.		
5.	Any interest yielded by the contributions paid to the Competence Centre by the participating 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.		

7. The Competence Centre shall own all assets generated by it or transferred to it for the fulfilment of its objectives.		**SE:** SE pending competence and tasks of the CCCN. SE cannot accept ownership to any results generated in respect to defence related activities. This would require further elaborations if defence is included. Such rights within the defence are could intrude on the competence of MS, in contrary to the treaties. Any results generated within a defence framework would also need to be subject to relevant export control regulation. Any rights to the CCCN needs take into account and be without prejudice to MS competences in terms of defence, national security as well as export control.
8. Except when the Competence Centre is wound up, any excess revenue over expenditure shall not be paid to the participating members of the Competence Centre.	**SK:** Except when the Competence Centre is wound up, any excess revenue over expenditure shall not be paid to the participating Member States of the Competence Centre.	**SK:** Article 23 Para 8 speaks about the member involved, and it is not clear what the member is. This is probably the "participating Member State".
Article 24 **Financial commitments**		
The financial commitments of the Competence Centre shall not exceed the amount of financial resources available or committed to its budget by its members.		

Article 25 **Financial year** The financial year shall run from 1 January to 31 December.		
Article 26 **Establishment of the budget**		
1. Each year, the Executive Director shall draw up a draft statement of estimates of the Competence Centre's revenue and expenditure for the following financial year, and shall forward it to the Governing Board, together with a draft establishment plan. Revenue and expenditure shall be in balance. The expenditure of the Competence Centre shall include the staff, administrative, infrastructure and operational expenses. Administrative expenses shall be kept to a minimum.	**NL:** Each year, the Executive Director shall draw up a draft statement of estimates of the Competence Centre's revenue and expenditure for the following financial year, and shall forward it to the Governing Board, together with a draft establishment plan. Revenue and expenditure shall be in balance. The expenditure of the Competence Centre shall include the staff, administrative, infrastructure and operational expenses. ~~Administrative expenses~~**Expenses** shall be kept to a minimum.	**NL:** Why only administrative?
2. Each year, the Governing Board shall, on the basis of the draft statement of estimates of revenue and expenditure referred to in paragraph 1, produce a statement of estimates of revenue and expenditure for the Competence Centre for the following financial year.		

3.	The Governing Board shall, by 31 January each year, send the statement of estimates referred to in paragraph 2, which shall be part of the draft single programming document, to the Commission.		
4.	On the basis of that statement of estimates, the Commission shall enter in the draft budget of the Union the estimates it deems necessary for the establishment plan and the amount of the contribution to be charged to the general budget, which it shall submit to the European Parliament and the Council in accordance with Article 313 and 314 TFEU.		
5.	The European Parliament and the Council shall authorise the appropriations for the contribution to the Competence Centre.		
6.	The European Parliament and the Council shall adopt the establishment plan for the Competence Centre.		

7. Together with the Work Plan, the Governing Board shall adopt the Centre's budget. It shall become final following definitive adoption of the general budget of the Union. Where appropriate, the Governing Board shall adjust the Competence Centre's budget and Work Plan in accordance with the general budget of the Union.		
Article 27 **Presentation of the Competence Centre's accounts and discharge**		
The presentation of the Competence Centre's provisional and final accounts and the discharge shall follow the rules and timetable of the Financial Regulation and of its financial rules adopted in accordance with Article 29.		
Article 28 **Operational and financial reporting**		

1.	The Executive Director shall report annually to the Governing Board on the performance of his/her duties in accordance with the financial rules of the Competence Centre.		
2.	Within two months of the closure of each financial year, the Executive Director shall submit to the Governing Board for approval an annual activity report on the progress made by the Competence Centre in the previous calendar year, in particular in relation to the work plan for that year. That report shall include, inter alia, information on the following matters:		
	(a) operational actions carried out and the corresponding expenditure;		**ES:** Will the Member States receive a database on financial contributions/assignments per country and participant, such an e-CORDA –like database?
	(b) the actions submitted, including a breakdown by participant type, including SMEs, and by Member State;		
	(c) the actions selected for funding, including a breakdown by participant type, including SMEs, and by Member State and indicating the contribution of the Competence Centre to the individual participants and actions;		

(d) progress towards the achievement of the objectives set out in Article 4 and proposals for further necessary work to achieve these objectives.		
3. Once approved by the Governing Board, the annual activity report shall be made publicly available.		
Article 29 **Financial rules**		**SE:** Will there be a transparent and publicly available register of financial and in-kind contribution? Also: how will the Centre make transparent what applications get grants?
The Competence Centre shall adopt its specific financial rules in accordance with Article 70 of Regulation XXX [new Financial Regulation].		
Article 30 **Protection of financial interests**		**PL:** Following SE comment, we would like to request information on transparency towards MSs and public.

1.	The Competence Centre shall take appropriate measures to ensure that, when actions financed under this Regulation are implemented, the financial interests of the Union are protected by the application of preventive measures against fraud, corruption and any other illegal activities, by effective checks and, if irregularities are detected, by the recovery of the amounts wrongly paid and, where appropriate, by effective, proportionate and dissuasive administrative sanctions.		
2.	The Competence Centre shall grant Commission staff and other persons authorised by the Commission, as well as the Court of Auditors, access to its sites and premises and to all the information, including information in electronic format that is needed in order to conduct their audits.		

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[16] and Regulation (EU, Euratom) No 883/2013 of the European Parliament and of the Council[17] 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.		

[16] 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).

[17] 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).

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.		
CHAPTER IV **COMPETENCE CENTRE STAFF** *Article 31* **Staff**			

1.	The Staff Regulations of Officials and the Conditions of Employment of Other Servants of the European Union as laid down by Council Regulation (EEC, Euratom, ECSC) No 259/68[18] ('Staff Regulations' and 'Conditions of Employment') and the rules adopted jointly by the institutions of the Union for the purpose of applying the Staff Regulations and Conditions of Employment shall apply to the staff of the Competence Centre.		
2.	The Governing Board shall exercise, with respect to the staff of the Competence Centre, the powers conferred by the Staff Regulations on the Appointing Authority and the powers conferred by the Conditions of Employment on the authority empowered to conclude contract ('the appointing authority powers').		

[18] Regulation (EEC, Euratom, ECSC) No 259/68 of the Council of 29 February 1968 laying down the Staff Regulations of Officials and the Conditions of Employment of Other Servants of the European Communities and instituting special measures temporarily applicable to officials of the Commission (OJ L 56, 4.3.1968, p. 1).

3.	The Governing Board shall adopt, in accordance with Article 110 of the Staff Regulations, a decision based on Article 2(1) of the Staff Regulations and on Article 6 of the Conditions of Employment delegating the relevant appointing authority powers to the Executive Director and defining the conditions under which that delegation may be suspended. The Executive Director is authorised to sub-delegate those powers.		
4.	Where exceptional circumstances so require, the Governing Board may by decision temporarily suspend the delegation of the appointing authority powers to the Executive Director and any sub-delegation made by the latter. In such a case the Governing Board shall exercise itself the appointing authority powers or delegate them to one of its members or to a staff member of the Competence Centre other than the Executive Director.		
5.	The Governing Board shall adopt implementing rules as regards the Staff Regulations and the Conditions of Employment in accordance with Article 110 of the Staff Regulations.		

6.	The staff resources shall be determined in the staff establishment plan of the Competence Centre, indicating the number of temporary posts by function group and by grade and the number of contract staff expressed in full-time equivalents, in line with its annual budget.		
7.	The staff of the Competence Centre shall consist of temporary staff and contract staff.		
8.	All costs related to staff shall be borne by the Competence Centre.		
	Article 32 **Seconded national experts and other staff**		**PL:** PL supports SE request for clarification in reference to financial or in-kind contribution.
1.	The Competence Centre may make use of seconded national experts or other staff not employed by the Competence Centre.		**SE:** Will seconded national experts be considered as financial or/and in-kind contributions from Member States? **CZ:** We agree with SE.
2.	The Governing Board shall adopt a decision laying down rules on the secondment of national experts to the Competence Centre, in agreement with the Commission.		

Article 33 **Privileges and Immunities**		
Protocol No 7 on the Privileges and Immunities of the European Union annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union shall apply to the Competence Centre and its staff.		
CHAPTER V **COMMON PROVISIONS** *Article 34* **Security Rules**		**SE**: Pending negations concerning the regulation regarding the Digital Europe Programme.
1. Article 12(7) Regulation (EU) No XXX [Digital Europe Programme] shall apply to participation in all actions funded by the Competence Centre.		
	new 1a FR: « the center may limit the participation in the work programme to beneficiaries established in the Union in which Member states and/or nationals of Member states own more than 50% of the undertaking and effectively control it » ;	**FR:** Cybersecurity requires more specific rules of participation than other programmes
2. The following specific security rules shall apply to actions funded from Horizon Europe:		

(a) for the purposes of Article 34(1) [Ownership and protection] of Regulation (EU) No XXX [Horizon Europe], when provided for in the Work plan, the grant of non-exclusive licenses may be limited to third parties established or deemed to be established in Members States and controlled by Member States and/or nationals of Member States;	**SE:** ~~for the purposes of Article 34(1) [Ownership and protection] of Regulation (EU) No XXX [Horizon Europe], when provided for in the Work plan,~~ the ~~grant of non-exclusive licenses may be limited to third parties established or deemed to be established in Members States and controlled by Member States and/or nationals of Member States~~;	**SE:** Unions security issues is the important thing to considered not ownership etc. SE needs more time to look at this.
(b) for the purposes of Article 36(4)(b) [Transfer and licensing] of Regulation (EU) No XXX [Horizon Europe], the transfer or license to a legal entity established in an associated country or established in the Union but controlled from third countries shall also be a ground to object to transfers of ownership of results, or to grants of an exclusive license regarding results;		

(c) for the purposes of Article 37(3)(a) [Access rights] of Regulation (EU) No XXX [Horizon Europe], when provided for in the Work plan, granting of access to results and background may be limited only to a legal entity established or deemed to be established in Members States and controlled by Member States and/or nationals of Member States.	**SE**: ~~for the purposes of Article 37(3)(a) [Access rights] of Regulation (EU) No XXX [Horizon Europe], when provided for in the Work plan, granting of access to results and background may be limited only to a legal entity established or deemed to be established in Members States and controlled by Member States and/or nationals of Member States.~~	**SE:** Unions security issues is the important thing to considered not ownership. SE needs to analyze this further. These regulations and reference would need to be updated and rephrased to be able to address any defence related content. For example, this does not correspond to security regulation relevant in the EDF or potential even Space. Further any access rights to CCCN, national centre's, other entities need to be further regulated and when relevant limited if any defence related activities are to be discussed under the CCCN
Article 35 **Transparency**		
1. The Competence Centre shall carry out its activities with a high level of transparency.		
2. The Competence Centre shall ensure that the public and any interested parties are given appropriate, objective, reliable and easily accessible information, in particular with regard to the results of its work. It shall also make public the declarations of interest made in accordance with Article 41.		

3.	The Governing Board, acting on a proposal from the Executive Director, may authorise interested parties to observe the proceedings of some of the Competence Centre's activities.		
4.	The Competence Centre shall lay down, in its rules of procedure, the practical arrangements for implementing the transparency rules referred to in paragraphs 1 and 2. For actions funded from Horizon Europe this will take due account of the provisions in Annex III of the Horizon Europe Regulation.		
	Article 36 **Security rules on the protection of classified information and sensitive non-classified information**		

1.	Without prejudice to Article 35, the Competence Centre shall not divulge to third parties information that it processes or receives in relation to which a reasoned request for confidential treatment, in whole or in part, has been made.	**SK:** Without prejudice to Article 35, the Competence Centre shall not divulge to third parties classified information that it processes or receives in relation to which a reasoned request for confidential treatment, in whole or in part, has been made. The Competence Centre will respect the provisions applicable to the Union institutions as well as national legislation on the handling of information, in particular sensitive non-classified and classified information.	**SK:** In Article 36 Para 1 - we propose adding the word "classified " after words "third parties" and adding a new sentence at the end of the provision: " The Competence Centre will respect the provisions applicable to the Union institutions as well as national legislation on the handling of information, in particular sensitive non-classified and classified information." ***Justification:*** Additionally, the intention defined in recital 29 of the preamble will be normative in nature and emphasize the need to protect all classified information
2.	Members of the Governing Board, the Executive Director, the members of the Industrial and Scientific Advisory Board, external experts participating in ad hoc Working Groups, and members of the staff of the Centre shall comply with the confidentiality requirements under Article 339 of the Treaty on the Functioning of the European Union, even after their duties have ceased.	**SK:** Members of the Governing Board, the Executive Director, the members of the Industrial and Scientific Advisory Board, external experts participating in ad hoc Working Groups, and members of the staff of the Centre are obliged to observe professional secrecy ~~shall comply with the confidentiality requirements~~ under Article 339 of the Treaty on the Functioning of the European Union, even after their duties have ceased.	**SK:** In Article 36 Para 2 we suggest replacing the words "to meet the confidentiality requirements" by "are obliged to observe professional secrecy". Justification: This is to reconcile the used term with Article 339 TFEU

3.	The Governing Board of the Competence Centre shall adopt the Competence Centre's security rules, following approval by the Commission, based on the principles and rules laid down in the Commission's security rules for protecting European Union classified information (EUCI) and sensitive non-classified information including inter alia provisions for the processing and storage of such information as set out in Commission Decisions (EU, Euratom) 2015/443[19] and 2015/444[20].		**ES:** Horizon2020 programme only permits projects up to EU-SECRET classification level to be funded. However, given the possibility that this Competence centre funds projects related to defence, it may happen that certain projects may need higher classification levels, such as EU TOP SECRET. The Competence Centre must have specific provisions concerning this possibility. **PL:** Following ES comment, more clarification is needed with reference to civilian-military synergies and projects classified as TOP SECRET.
4.	The Competence Centre may take all necessary measures to facilitate the exchange of information relevant to its tasks with the Commission and the Member States and where appropriate, the relevant Union agencies and bodies. Any administrative arrangement concluded to this end on sharing EUCI or, in the absence of such arrangement, any exceptional ad hoc release of EUCI shall have received the Commission's prior approval.		**SE:** Please clarify the last sentence. Further regulation, clarity needs to be added if defence activities shall be addressed under the CCCN.

[19] Commission Decision (EU, Euratom) 2015/443 of 13 March 2015 on Security in the Commission (OJ L 72, 17.3.2015, p. 41).
[20] Commission Decision (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information (OJ L 72, 17.3.2015, p. 53).

Article 37 **Access to documents**		
1. Regulation (EC) No 1049/2001 shall apply to documents held by the Competence Centre.		
2. The Governing Board shall adopt arrangements for implementing Regulation (EC) No 1049/2001 within six months of the establishment of the Competence Centre.		
3. Decisions taken by the Competence Centre pursuant to Article 8 of Regulation (EC) No 1049/2001 may be the subject of a complaint to the Ombudsman under Article 228 of Treaty on the Functioning of the European Union or of an action before the Court of Justice of the European Union under Article 263 of Treaty on the Functioning of the European Union.		

Article 38 **Monitoring, evaluation and review**		**ES:** This monitoring and evaluations should be submitted to the Member States; it should be specified in this article. **DE:** Can the Competence Center carry out this assessment itself or does this have to be an external evaluation? What role does the Governing Board play in the planning, implementation and monitoring of the evaluation?
1. The Competence Centre shall ensure that its activities, including those managed through the National Coordination Centres and the Network, shall be subject to continuous and systematic monitoring and periodic evaluation. The Competence Centre shall ensure that the data for monitoring programme implementation and results are collected efficiently, effectively, and in timely manner and proportionate reporting requirements shall be imposed on recipients of Union funds and Member States. The outcomes of the evaluation shall be made public.		

2.	Once there is sufficient information available about the implementation of this Regulation, but no later than three and a half years after the start of the implementation of this Regulation, the Commission shall carry out an interim evaluation of the Competence Centre. The Commission shall prepare a report on that evaluation and shall submit that report to the European Parliament and to the Council by 31 December 2024. The Competence Centre and Member States shall provide the Commission with the information necessary for the preparation of that report.		**DE:** Would it not make sense if the Governing Board of Directors were included in a transparent manner in the COM report?
3.	The evaluation referred to in paragraph 2 shall include an assessment of the results achieved by the Competence Centre, having regard to its objectives, mandate and tasks. If the Commission considers that the continuation of the Competence Centre is justified with regard to its assigned objectives, mandate and tasks, it may propose that the duration of the mandate of the Competence Centre set out in Article 46 be extended.		

4.	On the basis of the conclusions of the interim evaluation referred to in paragraph 2 the Commission may act in accordance with [Article 22(5)] or take any other appropriate actions.		
5.	The monitoring, evaluation, phasing out and renewal of the contribution from Horizon Europe will follow the provisions of articles 8, 45 and 47 and Annex III of the Horizon Europe Regulation and agreed implementation modalities.		
6.	The monitoring, reporting and evaluation of the contribution from Digital Europe will follow the provisions of articles 24, 25 of the Digital Europe programme.		
7.	In case of a winding up of the Competence Centre, the Commission shall conduct a final evaluation of the Competence Centre within six months after the winding-up of the Competence Centre, but no later than two years after the triggering of the winding-up procedure referred to in Article 46 of this Regulation. The results of that final evaluation shall be presented to the European Parliament and to the Council.		

Article 39 **Liability of the Competence Centre**		
1. The contractual liability of the Competence Centre shall be governed by the law applicable to the agreement, decision or contract in question.		
2. In the case of non-contractual liability, the Competence Centre shall, in accordance with the general principles common to the laws of the Member States, make good any damage caused by its staff in the performance of their duties.		
3. Any payment by the Competence Centre in respect of the liability referred to in paragraphs 1 and 2 and the costs and expenses incurred in connection therewith shall be considered to be expenditure of the Competence Centre and shall be covered by its resources.		
4. The Competence Centre shall be solely responsible for meeting its obligations.		

Article 40 **Jurisdiction of the Court of Justice of the European Union and applicable law**		
1. The Court of Justice of the European Union shall have jurisdiction:		
(1) pursuant to any arbitration clause contained in agreements, decisions or contracts concluded by the Competence Centre;		
(2) in disputes related to compensation for damage caused by the staff of the Competence Centre in the performance of their duties;		
(3) in any dispute between the Competence Centre and its staff within the limits and under the conditions laid down in the Staff Regulations.		
2. Regarding any matter not covered by this Regulation or by other Union legal acts, the law of the Member State where the seat of the Competence Centre is located shall apply.		

Article 41 **Liability of members and insurance**		
1. The financial liability of the members for the debts of the Competence Centre shall be limited to their contribution already made for the administrative costs. 2. The Competence Centre shall take out and maintain appropriate insurance.		**PL:** A clarification is needed in reference to the term "liability of the members". This provision, in current wording, may be interpreted, in such a way, that Member States will be responsible for unpaid obligations.
Article 42 **Conflicts of interest**		
The Competence Centre Governing Board shall adopt rules for the prevention and management of conflicts of interest in respect of its members, bodies and staff. Those rules shall contain the provisions intended to avoid a conflict of interest in respect of the representatives of the members serving in the Governing Board as well as the Scientific and Industrial Advisory Board in accordance with Regulation XXX [new Financial Regulation].		

Article 43 **Protection of Personal Data**		
1. The processing of personal data by the Competence Centre shall be subject to Regulation (EU) No XXX/2018 of the European Parliament and of the Council.		
2. The Governing Board shall adopt implementing measures referred to in Article xx(3) of Regulation (EU) No xxx/2018. The Governing Board may adopt additional measures necessary for the application of Regulation (EU) No xxx/2018 by the Competence Centre.		
Article 44 **Support from the host Member State**		
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		**PL:** Is it already decided that the Centre's location would be in Belgium (Brussels)? Were other locations taken into account?

CHAPTER VII **FINAL PROVISIONS** *Article 45* **Initial actions**		
1. The Commission shall be responsible for the establishment and initial operation of the Competence Centre until it has the operational capacity to implement its own budget. The Commission shall carry out, in accordance with Union law, all necessary actions with the involvement of the competent bodies of the Competence Centre.		
2. For the purpose of paragraph 1, until the Executive Director takes up his duties following his/her appointment by the Governing Board in accordance with Article 16, the Commission may designate an interim Executive Director and exercise the duties assigned to the Executive Director who may be assisted by a limited number of Commission officials. The Commission may assign a limited number of its officials on an interim basis.		

3.	The interim Executive Director may authorise all payments covered by the appropriations provided in the annual budget of the Competence Centre once approved by the Governing Board and may conclude agreements, decisions and contracts, including staff contracts following the adoption of the Competence Centre's staff establishment plan.		
4.	The interim Executive Director shall determine, in common accord with the Executive Director of the Competence Centre and subject to the approval of the Governing Board, the date on which the Competence Centre will have the capacity to implement its own budget. From that date onwards, the Commission shall abstain from making commitments and executing payments for the activities of the Competence Centre.		

Article 46 **Duration**		
1. The Competence Centre shall be established for the period from 1 January 2021 to 31 December 2029.		
2. At the end of this period, unless decided otherwise through a review of this Regulation, the winding-up procedure shall be triggered. The winding-up procedure shall be automatically triggered if the Union or all participating Member States withdraw from the Competence Centre.		**LV** The point mentions a possibility of withdrawal, yet nowhere in the document is a withdrawal process outlined. Therefore, it becomes unclear whether it is possible to withdraw from the Competence Centre and, if so, what are the procedures for withdrawal? **DE:** Proposal: to initiate the winding-up procedure already when a certain quorum has fallen below the MS's participation in terms of number and financial contribution. (In this formulation the Center could be operated by COM and only one MS, which obviously seems meaningless) **PL:** PL supports LV request for further clarification of withdrawal procedure.
3. For the purpose of conducting the proceedings to wind up the Competence Centre, the Governing Board shall appoint one or more liquidators, who shall comply with the decisions of the Governing Board.		

4. When the Competence Centre is being wound up, its assets shall be used to cover its liabilities and the expenditure relating to its winding-up. Any surplus shall be distributed among the Union and the participating Member States in proportion to their financial contribution to the Competence Centre. Any such surplus distributed to the Union shall be returned to the Union budget.		
Article 47 **Entry into force**		
This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*. This Regulation shall be binding in its entirety and directly applicable in all Member States. Done at Brussels, *For the European Parliament* *The President* *For the Council* *The President*		