Procedure file

Basic information

COD - Ordinary legislative procedure (ex-codecision procedure) Regulation	2018/0328(COD)	Procedure completed
European Cybersecurity Competence Centre Subject 3.30.07 Cybersecurity, cyberspace policy 3.50.20 Scientific and technological cooperation and agreements 8.40.08 Agencies and bodies of the EU Legislative priorities Joint Declaration 2021		

Key players

European Parliament	Committee responsible	Rapporteur	Appointed
	ITRE Industry, Research and Energy		02/09/2019
		ANDRESEN Rasmus	
		Shadow rapporteur	
		DEL CASTILLO VERA Pilar	
		GEIER Jens	
		GAMON Claudia	
		TOŠENOVSKÝ Evžen	
	Former committee responsible		
	ITRE Industry, Research and Energy		07/11/2018
		REDA Felix	
	Former committee for opinion		
	BUDG Budgets	The committee decided not to give an opinion.	
	IMCO Internal Market and Consumer Protection		24/09/2018
		KOHN Arndt	
Council of the European Union			
European Commission	Commission DG	Commissioner	

European Economic and Social Committee European Committee of the Regions	Secretariat-General	JUNCKER Jean-Claude

Key events

12/09/2018	Legislative proposal published	COM(2018)0630	Summary
01/10/2018	Committee referral announced in Parliament, 1st reading		
19/02/2019	Vote in committee, 1st reading		
22/02/2019	Committee report tabled for plenary, 1st reading	A8-0084/2019	Summary
11/03/2019	Debate in Parliament		
13/03/2019	Results of vote in Parliament		
13/03/2019	Decision by Parliament, 1st reading	T8-0189/2019	Summary
13/03/2019	Matter referred back to the committee responsible		
17/04/2019	Decision by Parliament, 1st reading	T8-0419/2019	Summary
25/09/2019	Committee decision to open interinstitutional negotiations after 1st reading in Parliament		
09/10/2019	Committee decision to enter into interinstitutional negotiations announced in plenary (Rule 72)		
14/01/2021	Approval in committee of the text agreed at early 2nd reading interinstitutional negotiations	PE662.119 PE662.120	
23/04/2021	Council position published	05628/2/2021	Summary
26/04/2021	Vote in committee, 2nd reading		
17/05/2021	Committee referral announced in Parliament, 2nd reading		
17/05/2021	Committee recommendation tabled for plenary, 2nd reading	A9-0166/2021	
19/05/2021	Debate in Parliament		
19/05/2021	Decision by Parliament, 2nd reading	T9-0246/2021	Summary
20/05/2021	Final act signed		
20/05/2021	End of procedure in Parliament		
08/06/2021	Final act published in Official Journal		

Technical information

Procedure reference	2018/0328(COD)
Procedure type	COD - Ordinary legislative procedure (ex-codecision procedure)

Procedure subtype	Legislation
Legislative instrument	Regulation
Legal basis	Treaty on the Functioning of the EU TFEU 173-p3; Treaty on the Functioning of the EU TFEU 188 -a1; Rules of Procedure EP 59-p4
Other legal basis	Rules of Procedure EP 159
Mandatory consultation of other institutions	European Economic and Social Committee European Committee of the Regions
Stage reached in procedure	Procedure completed
Committee dossier	ITRE/9/01206

Documentation gateway

Legislative proposal		COM(2018)0630	12/09/2018	EC	Summary
Document attached to the procedure		SWD(2018)0403	12/09/2018	EC	Summary
Document attached to the procedure		SWD(2018)0404	12/09/2018	EC	Summary
Committee draft report		PE631.940	07/12/2018	EP	
Economic and Social Committee: opinion, report		CES5208/2018	12/12/2018	ESC	
Amendments tabled in committee		PE632.973	17/01/2019	EP	
Economic and Social Committee: opinion, report		CES4805/2018	23/01/2019	ESC	
Committee opinion	IMCO	PE630.409	31/01/2019	EP	
Committee report tabled for plenary, 1st reading/single reading		A8-0084/2019	22/02/2019	EP	Summary
Text adopted by Parliament, partial vote at 1st reading/single reading		T8-0189/2019	13/03/2019	EP	Summary
Text adopted by Parliament, 1st reading/single reading		T8-0419/2019	17/04/2019	EP	Summary
Commission response to text adopted in plenary		SP(2019)440	08/08/2019	EC	
Committee letter confirming interinstitutional agreement		PE662.120	14/01/2021	EP	
Committee draft report		PE689.669	30/03/2021	EP	
Council position		05628/2/2021	23/04/2021	CSL	Summary
Commission communication on Council's position		COM(2021)0225	03/05/2021	EC	
Committee recommendation tabled for plenary, 2nd reading		A9-0166/2021	17/05/2021	EP	
Text adopted by Parliament, 2nd reading		T9-0246/2021	19/05/2021	EP	Summary
Draft final act		00028/2021/LEX	20/05/2021	CSL	

Additional information

Research document	Briefing

Final act

Regulation 2021/887
OJ L 202 08.06.2021, p. 0001

Final legislative act with provisions for delegated acts

European Cybersecurity Competence Centre

PURPOSE: to pool resources and expertise in the field of cybersecurity technologies.

PROPOSED ACT: Regulation of the European Parliament and of the Council.

ROLE OF THE EUROPEAN PARLIAMENT: the European Parliament decides in accordance with the ordinary legislative procedure and on an equal footing with the Council.

BACKGROUND: cybersecurity is an issue of common interest of the Union. 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.

Following the 2013 cybersecurity strategy, the Union has continued to increase its activities to meet the growing challenges of cybersecurity:

- in 2016, the Union adopted its first measures in the area of cybersecurity through Directive (EU) 2016/1148 of the European Parliament and of the Council on security of network and information systems;
- the creation in 2016 of the Public-Private Partnership (cPPP) on cybersecurity in the Union was a solid first step bringing together the research, industry and public sector communities to facilitate research and innovation in cybersecurity and within the limits of the 2014-2020 financial framework should result in good, more focused outcomes in research and innovation. It will have triggered up to EUR 1.8 billion of investment by 2020;
- in September 2017, the Commission and the High Representative of the Union for Foreign Affairs and Security Policy presented a joint Communication on Resilience, Deterrence and Defence: Building strong cybersecurity for the EU to further reinforce the Unions resilience, deterrence and response to cyber-attacks;
- at the Tallinn Digital Summit in September 2017, Heads of State and Government called on the Union to become a global leader in the field of cybersecurity by 2025.

With more than 660 cyber security competence centres throughout the EU, the EU already has considerable expertise in this area. However, the efforts of the research and industry communities are fragmented, lacking alignment and a common mission, which hinders the EU's competitiveness in this field.

The Commission considers that 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.

IMPACT ASSESSMENT: among the main arguments in favour of the selected option were:

- the ability to create a real cybersecurity industrial policy by supporting activities related not only to research and development but also to market deployment;
- the flexibility to allow different cooperation models with the community and the network of competence centres to optimise the use of existing knowledge and resources;
- the ability to structure cooperation of the public and private stakeholders coming from all relevant sectors, including defence.

CONTENT: this Regulation proposes to establish the European Cybersecurity Industrial, Technology and Research 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.

The Competence Centre: its role would be to facilitate the work of the Network of National Coordination Centres and to enhance the cybersecurity competences, by driving the cybersecurity technological agenda and facilitating access to the expertise so gathered.

To this end, it would coordinate the use of cybersecurity funds under the EU's next long-term budget for the period 2021-2027 under the Digital Europe Programme and the Horizon Europe Programme. Its objectives would be:

- to enhance cybersecurity capabilities, knowledge and infrastructures at the service of industries, the public sector and research communities;
- to contribute to the wide deployment of the latest cyber security products and solutions across the economy;
- to improve the understanding of cybersecurity and contribute to reducing skills gaps in the Union related to cybersecurity;
- to contribute to the reinforcement of cybersecurity research and development in the Union;
- to enhance synergies between the civilian and defence dimensions of cybersecurity.

The Competence Centre would be set up as a European partnership to facilitate joint investment by the Union, Member States and/or industry. Therefore, the proposal requires Member States to contribute a commensurate amount to the actions of the Competence Centre and Network. The principal decision-making body is the Governing Board, in which all Member States take part but only those Member States which participate financially have voting rights.
The Network of National Coordination Centres: each Member State would nominate a national coordination centre to lead the Network, which would focus on developing new and expanded cybersecurity capabilities and expertise. The Network would identify and support the most relevant cybersecurity projects in Member States.

The Cybersecurity Competences Community: this would contribute to the mission of the Competence Centre by enhancing and disseminating cybersecurity expertise throughout the Union. It would involve a large and diverse group of actors involved in the development of cybersecurity technologies, such as research organisations, supply and demand side industries and the public sector.

BUDGETARY IMPLICATIONS: the Union's contribution to the Competence Centre to cover administrative and operating costs includes the following elements:

- EUR 1 981 668 000 from the Digital Europe Programme, of which up to EUR 23 746 000 for administrative costs;
- EUR 2.8 billion from the Horizon Europe programme, including for administrative costs; this contribution will be proposed by the Commission during the legislative process and, in any case, before a political agreement is reached.

European Cybersecurity Competence Centre

The Commission staff working document presents the impact assessment accompanying 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 European Union has already put in place a number of policy and regulatory instruments to address fast evolving cyber threats and to secure its society, economy and democracy against them.

However, at present, the EU still lacks sufficient technological and industrial capacities to autonomously secure its economy and critical infrastructures and to become a global leader in cybersecurity field. There are still problems relating to the EU's insufficient cybersecurity technological and industrial capacities.

To this end, it aims to address the following problems:

- insufficient level of strategic and sustainable coordination and cooperation between industries, cybersecurity research communities and governments to shield economy, society and democracy with leading-edge European cybersecurity solutions;
- sub-scale investment and limited access to cybersecurity know- how, skills and facilities across Europe;
- few European cybersecurity research and innovation outcomes translated into marketable solutions and widely deployed across the economy.

The following options were looked at:

- Option 1: Cybersecurity Competence Network with a European Cybersecurity Industrial and Research Competence Centre entity empowered to pursue measures in support of industrial technologies as well as in the domain of research and innovation.
- Option 2: Cybersecurity Competence Network with a European Cybersecurity Research and Competence Centre limited to research and innovation activities only.

Preferred option: the chosen option (option 1) is the creation of a Network of Cybersecurity Competence Centres with a European Cybersecurity Industrial, Technological and Research Competence Centre empowered to take action in favour of industrial technologies as well as in the field of research and innovation. According to the Commission, it represents the best instrument capable to implement the goals of the initiative while offering the highest economic, societal, and environmental impact and safeguarding the Unions interests.

The main arguments in favour of setting the European Cybersecurity Industrial and Research Competence Centre supporting the Network as an EU entity based on art. 173 and 187 TFEU (autonomous EU legal entity, with its own budget, staff, structure, rules and governance) are:

- it ensures flexibility to allow different cooperation models with the network of competence centres to optimise the use of existing knowledge and resources including financial tools and other incentives supporting members of the network;
- it provides a visible legal, contractual and organisational common framework to structure the joint commitments of the public and private stakeholders coming from all relevant sectors, including defence;
- it allows for the creation of a real cybersecurity industrial policy by supporting activities related not only to research and development but also to market deployment activities;
- it can act as an implementation mechanism for different EU cybersecurity funding streams under the next Multi-annual financial framework (Digital Europe Programme, Horizon Europe) and enhance synergies between the civilian and defence dimensions of cybersecurity in relation to the European Defence Fund.

European Cybersecurity Competence Centre

The Commission staff working document summarises the impact assessment accompanying 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.

To this end, it aims to address the following problems:

- insufficient level of strategic and sustainable coordination and cooperation between industries, cybersecurity research communities and governments to shield economy, society and democracy with leading-edge European cybersecurity solutions;
- sub-scale investment and limited access to cybersecurity know- how, skills and facilities across Europe;
- few European cybersecurity research and innovation outcomes translated into marketable solutions and widely deployed across the economy.

Solutions: a number of policy options have been considered, both legislative and non-legislative.

The option chosen is the creation of a Network of Cybersecurity Competence Centres with a European Cybersecurity Industrial, Technological and Research Competence Centre empowered to take action in favour of industrial technologies as well as in the field of research and innovation.

The creation of the Competence Centre would be based on a dual legal basis due to its nature and specific objectives, namely Articles 187 and 173 TFEU.

The analysis showed that this option is the most appropriate to achieve the goals of the initiative, while ensuring the best economic, societal

and environmental benefits and safeguarding the best interests of the Union.

The initiative would add value to current national efforts:

- by helping to create an inter-connected, Europe-wide cybersecurity industrial and research ecosystem;
- by encouraging better cooperation between relevant stakeholders (including between cybersecurity civilian and defence sectors) to make the best use of existing cybersecurity resources and expertise spread across Europe.

Impacts of the preferred option: the expected benefits would be as follows:

- the possibility for public authorities and industries across Member States to more effectively prevent and respond to cyber threats by offering and equipping itself with more secure products and solutions. This is in particular relevant for the protection of access to essential services (e.g. transport, health, banking and financial services);
- the creation of a mechanism capable of building Member States' and Union's cybersecurity industrial capacities and effectively translating European scientific excellence into marketable solutions that could be deployed across the economy;
- pooling resources to invest in the necessary capacities at Member State level and develop common European assets while achieving economies of scale;
- the possibility for SMEs, industries and researchers to have increased access to infrastructure;
- the reduction of the costs of designing new products for SMEs and open up opportunities in terms of costs reduction for the design of new products and it will help them gain easier access to the investors' community and attract the necessary funding to deploy marketable solutions;
- allowing defence and civilian communities to work together on shared challenges;
- improving coherence and synergies between different funding mechanism;
- an indirect positive impact on the environment could be achieved through developing specific cybersecurity solutions for sectors having potentially huge environmental impact (e.g. nuclear power plants).

This initiative has a clear positive impact as it is likely to substantially increase Member States' capacities to autonomously secure their economies, including protecting the critical sectors, increasing competitiveness of European cybersecurity businesses as well as industries across different sectors. This should ultimately allow the EU to become a leader in the next-generation digital and cybersecurity technologies.

European Cybersecurity Competence Centre

The Committee on Industry, Research and Energy adopted the report by Julia REDA (Greens/EFA, DE) on the proposal for a regulation of the European Parliament and of the Council establishing the European Centre for Industrial, Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres.

The committee recommended that the European Parliament's position adopted at first reading under the ordinary legislative procedure should amend the Commission's proposal as follows:

Objectives and missions of the Competence Centre

The European Cybersecurity Industrial, Technology and Research Competence Centre should help increase the resilience and reliability of the infrastructure of network and information systems, including the internet and other critical infrastructure for the functioning of society such as transport, health, and banking systems.

Members clarified the missions and tasks of the Competence Centre, including:

- contribute to increasing the resilience and reliability of network and information systems infrastructure, including the Internet and other infrastructures critical to the functioning of society, such as transport, health and banking systems;
- raise the awareness for cybersecurity threats, and related societal and ethical implications and concerns and reduce the skills gap in cybersecurity in the Union;
- develop European leadership in cybersecurity and ensure the highest cybersecurity standards throughout the Union;
- strengthen Union competitiveness and capacities while reducing its digital dependence by increasing the uptake of cybersecurity products, processes and services developed within the Union;
- reinforce the trust of citizens, consumers and businesses in the digital world;
- provide financial support and technical assistance to start-ups, SMEs, microenterprises, associations, individual experts and civil technology projects in the field of cybersecurity;
- finance software security code controls and related improvements in free and open source software projects commonly used for infrastructure, products and processes;
- facilitate the sharing of cybersecurity knowledge and technical assistance among others to civil society, industry and public authorities, as well as to the academic and research communities;
- promote "safety by design" as a principle in the process of developing, maintaining, operating and updating infrastructure, products and services, in particular by supporting the latest safe development methods, appropriate safety tests and safety audits;
- ensure respect for fundamental rights and ethical behaviour in cybersecurity research projects supported by the Competence Centre;
- monitor reports of vulnerabilities discovered by the Community and facilitating the disclosure of vulnerabilities, the development of patches, fixes and solutions;
- support research in the field of cybercrime and the development of products and processes that can be freely studied, shared and developed;
- contribute to the Union's efforts to strengthen international cooperation on cybersecurity.

National Coordination Centres

A National Coordination Centre shall be set up in each Member State.

The relationship between the Competence Centre and the national coordination centres shall be based on a standard contractual agreement signed between the Competence Centre and each of the national coordination centres. The agreement shall consist of the same set of harmonised general conditions providing the rules governing the relationship and division of tasks between the Competence Centre and each

National Coordination Centre and special conditions tailored on the particular National Coordination Centre.

National Centres shall cooperate closely with national standards bodies to promote the adoption of existing standards and to involve all relevant stakeholders, in particular SMEs, in the development of new standards. They shall also promote and disseminate a minimum common curriculum on cybersecurity.

Cybersecurity Competence Community

The Cybersecurity Competence Community contributes to the mission of the Competence Centre and disseminates cybersecurity expertise across the Union.

The Competence Community shall include civil society, industry, both on the demand and supply side, including SMEs, academia and science, user associations, individual experts, relevant European standards bodies and other associations, as well as public entities and other entities dealing with operational and technical issues in the field of cybersecurity.

Governing structure

The Governing Board shall be composed of one representative from each Member State, one representative appointed by the European Parliament as an observer, and four representatives of the Commission, on behalf of the Union, and shall aim to achieve gender balance between the members of the Governing Board and their alternates.

The Centre and its bodies shall ensure that conflicts of interest are not only identified, but are resolved and addressed in a transparent and accountable manner. Member States shall ensure that the same applies to national coordination centres.

The Industry and Scientific Advisory Committee would regularly advise the Competence Centre on the execution of its activities.

Financial contribution of the Union

This shall amount to EUR 1 780 954 875 at 2018 prices (EUR 1 998 696 000 in current prices) from the Digital Europe programme, including up to EUR 21 385 465 at 2018 prices (EUR 23 746 000 in current prices) for administrative costs. It shall also include an amount from the European Defence Fund for the defence-related actions of the Competence Centre.

European Cybersecurity Competence Centre

The European Parliament adopted by 489 votes to 73, with 56 abstentions, amendments to the proposal for a regulation of the European Parliament and of the Council establishing the European Centre for European Cybersecurity Industrial, Technology and Research Competence Centre and Network of National Coordination Centres.

The matter was referred to the committee responsible for interinstitutional negotiations.

The main amendments adopted in plenary concern the following points:

Objectives and missions of the Competence Centre

Parliament recalled that in 2017, 80 % of the European companies experienced at least one cyber incident making it necessary to adopt the highest standards and comprehensive cyber security solutions by mobilising people, products, processes and technology at European level.

The European Competence Centre and the network of national coordination centres established by the Regulation shall contribute to overall resilience and awareness of cyber security threats in the Union, taking into account the implications for society.

Members clarified the missions and tasks of the Competence Centre, including:

- contribute to increasing the resilience and reliability of network and information systems infrastructure, including the Internet and other infrastructures critical to the functioning of society, such as transport, health and banking systems;
- develop the cybersecurity technological, industrial, societal, academic and research expertise capacities and capabilities;
- raise the awareness for cybersecurity threats, and related societal and ethical implications and concerns and reduce the skills gap in cybersecurity in the Union;
- develop European leadership in cybersecurity and ensure the highest cybersecurity standards throughout the Union;
- strengthen Union competitiveness and capacities while reducing its digital dependence by increasing the uptake of cybersecurity products, processes and services developed within the Union;
- reinforce the trust of citizens, consumers and businesses in the digital world;
- provide financial support and technical assistance to start-ups, SMEs, microenterprises, associations, individual experts and civil technology projects in the field of cybersecurity;
- finance software security code controls and related improvements in free and open source software projects commonly used for infrastructure, products and processes;
- facilitate the sharing of cybersecurity knowledge and technical assistance among others to civil society, industry and public authorities, as well as to the academic and research communities;
- promote "safety by design" as a principle in the process of developing, maintaining, operating and updating infrastructure, products and services, in particular by supporting the latest safe development methods, appropriate safety tests and safety audits;
- ensure respect for fundamental rights and ethical behaviour in cybersecurity research projects supported by the Competence Centre;
- monitor reports of vulnerabilities discovered by the Community and facilitating the disclosure of vulnerabilities, the development of patches, fixes and solutions;
- support research in the field of cybercrime and the development of products and processes that can be freely studied, shared and developed;
- enhance cooperation between the civil and defence spheres with regard to dual use technologies and applications in cybersecurity, by carrying out the following tasks, which shall be reactive and defensive cyber defence technology;
- contribute to the Union's efforts to strengthen international cooperation on cybersecurity.

National Coordination Centres

A National Coordination Centre shall be set up in each Member State.

The relationship between the Competence Centre and the national coordination centres shall be based on a standard contractual agreement signed between the Competence Centre and each of the national coordination centres.

National Centres shall cooperate closely with national standards bodies to promote the adoption of existing standards and to involve all relevant stakeholders, in particular SMEs, in the development of new standards. They shall also serve as a one-stop shop for products and processes funded by other EU programmes and provide a minimum common curriculum on cybersecurity.

Cybersecurity Competence Community

The Cybersecurity Competence Community contributes to the mission of the Competence Centre and disseminates cybersecurity expertise across the Union.

The Competence Community shall include civil society, industry, both on the demand and supply side, including SMEs, academia and science, user associations, individual experts, relevant European standards bodies and other associations, as well as public entities and other entities dealing with operational and technical issues in the field of cybersecurity.

Governing structure

The Governing Board shall be composed of one representative from each Member State, one representative appointed by the European Parliament as an observer, and four representatives of the Commission, on behalf of the Union, and shall aim to achieve gender balance between the members of the Governing Board and their alternates.

The Centre and its bodies shall ensure that conflicts of interest are not only identified, but are resolved and addressed in a transparent and accountable manner. Member States shall ensure that the same applies to national coordination centres.

The Industry and Scientific Advisory Committee, composed of a maximum of 25 members, would regularly advise the Competence Centre on the execution of its activities.

Financial contribution of the Union

This shall amount to EUR 1 780 954 875 at 2018 prices (EUR 1 998 696 000 in current prices) from the Digital Europe programme, including up to EUR 21 385 465 at 2018 prices (EUR 23 746 000 in current prices) for administrative costs. It shall also include an amount from the European Defence Fund for the defence-related actions of the Competence Centre.

European Cybersecurity Competence Centre

The European Parliament adopted by 480 votes to 70, with 60 abstentions, a legislative resolution on the proposal for a regulation of the European Parliament and of the Council establishing the European Centre for European Cybersecurity Industrial, Technology and Research Competence Centre and Network of National Coordination Centres.

The position of the European Parliament adopted at first reading in the framework of the ordinary legislative procedure amended the Commission proposal as follows:

Parliament recalled that in 2017, 80 % of the European companies experienced at least one cyber incident making it necessary to adopt the highest standards and comprehensive cyber security solutions.

The objectives of the proposed Regulation would be to strengthen the Union's competitiveness and capabilities in cybersecurity, and to reduce its digital dependency by improving the uptake of cybersecurity products, processes and services developed within the Union.

The European Competence Centre and the network of national coordination centres established by the Regulation shall contribute to overall resilience and awareness of cyber security threats in the Union, taking into account the implications for society.

Members clarified the missions and tasks of the Competence Centre, including:

- develop the technological, industrial, societal, societal, academic and research skills and expertise in cybersecurity necessary to secure its digital single market and strengthen data protection for EU citizens, businesses and public administrations;
- contribute to increasing the resilience and reliability of network and information systems infrastructure, including the Internet and other infrastructures critical to the functioning of society, such as transport, health and banking systems;
- develop the cybersecurity technological, industrial, societal, academic and research expertise capacities and capabilities;
- raise the awareness for cybersecurity threats, and related societal and ethical implications and concerns and reduce the skills gap in cybersecurity in the Union;
- develop European leadership in cybersecurity and ensure the highest cybersecurity standards throughout the Union;
- reinforce the trust of citizens, consumers and businesses in the digital world;
- provide financial support and technical assistance to start-ups, SMEs, microenterprises, associations, individual experts and civil technology projects in the field of cybersecurity;
- finance software security code controls and related improvements in free and open source software projects commonly used for infrastructure, products and processes;
- facilitate the sharing of cybersecurity knowledge and technical assistance among others to civil society, industry and public authorities, as well as to the academic and research communities;
- promote "safety by design" as a principle in the process of developing, maintaining, operating and updating infrastructure, products and services, in particular by supporting the latest safe development methods, appropriate safety tests and safety audits;
- ensure respect for fundamental rights and ethical behaviour in cybersecurity research projects supported by the Competence Centre;
- monitor reports of vulnerabilities discovered by the Community and facilitating the disclosure of vulnerabilities, the development of patches, fixes and solutions;
- support research in the field of cybercrime and the development of products and processes that can be freely studied, shared and

developed;
- provide specific support to SMEs by facilitating their tailor-made access to knowledge and training;
- enhance cooperation between the civil and defence spheres with regard to dual use technologies and applications in cybersecurity, by carrying out the following tasks, which shall be reactive and defensive cyber defence technology;
- contribute to the Union's efforts to strengthen international cooperation on cybersecurity.

National Coordination Centres

A National Coordination Centre shall be set up in each Member State.

The relationship between the Competence Centre and the national coordination centres shall be based on a standard contractual agreement signed between the Competence Centre and each of the national coordination centres.

National Centres shall cooperate closely with national standards bodies to promote the adoption of existing standards and to involve all relevant stakeholders, in particular SMEs, in the development of new standards. They shall also serve as a one-stop shop for products and processes funded by other EU programmes and provide a minimum common curriculum on cybersecurity.

Cybersecurity Competence Community

The Cybersecurity Competence Community contributes to the mission of the Competence Centre and disseminates cybersecurity expertise across the Union.

The Competence Community shall include civil society, industry, both on the demand and supply side, including SMEs, academia and science, user associations, individual experts, relevant European standards bodies and other associations, as well as public entities and other entities dealing with operational and technical issues in the field of cybersecurity.

Governing structure

The Governing Board shall be composed of one representative from each Member State, one representative appointed by the European Parliament as an observer, and four representatives of the Commission, on behalf of the Union, and shall aim to achieve gender balance between the members of the Governing Board and their alternates.

The Centre and its bodies shall ensure that conflicts of interest are not only identified, but are resolved and addressed in a transparent and accountable manner. Member States shall ensure that the same applies to national coordination centres.

The Industry and Scientific Advisory Committee, composed of a maximum of 25 members, would regularly advise the Competence Centre on the execution of its activities.

Financial contribution of the Union

This shall amount to EUR 1 780 954 875 at 2018 prices (EUR 1 998 696 000 in current prices) from the Digital Europe programme, including up to EUR 21 385 465 at 2018 prices (EUR 23 746 000 in current prices) for administrative costs. It shall also include an amount from the European Defence Fund for the defence-related actions of the Competence Centre.

European Cybersecurity Competence Centre

The Council adopted its position at first reading with a view to the adoption of 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 proposed regulation aims to help the EU maintain and develop the technological and industrial cyber security capacities needed to secure its digital single market. It provides for the creation of structures at three institutional levels:

1) a European Competence Centre for Cybersecurity Industrial, Technology and Research (at EU level),

2) a Network of National Coordination Centres (national level), and

3) a Cybersecurity Competence Community (at stakeholder level).

Mission of the Competence Centre and the Network

The mission of the Competence Centre and the Network is to help the Union to:

- strengthen its leadership and strategic autonomy in the area of cybersecurity by retaining and developing the Unions research, academic, societal, technological and industrial cybersecurity capacities and capabilities necessary to enhance trust and security, including the confidentiality, integrity and accessibility of data, in the Digital Single Market;

- support Union technological capacities, capabilities and skills in relation to the resilience and reliability of the infrastructure of network and information systems, including critical infrastructure and commonly used hardware and software in the Union; and

- increase the global competitiveness of the Unions cybersecurity industry, ensure high cybersecurity standards throughout the Union and turn cybersecurity into a competitive advantage for other Union industries.

Centre of Competence

The Centres aim would be to ensure closer coordination between research and innovation and the deployment of strategies at both national and EU level, and to enable Member States to take decisions on their financial contribution to joint actions.

The Competence Centre should:

- implement research and innovation actions (supported by the Horizon Europe programme) as well as capacity building actions (supported by the Digital Europe programme);

- support, together with Member States, the build-up and procurement of advanced cybersecurity equipment, tools and data infrastructure in Europe and ensure wide deployment of the latest cybersecurity solutions across the economy; to this end, the Competence Centre would also be able to facilitate the shared acquisition of capacities on behalf of Member States.

Organisation of the Centre of Competence

The Competence Centre would be based in Bucharest and would have a Governing Board composed of representatives of the Member States and the Commission, responsible for defining the general direction of the Competence Centres operations and should ensure that the Competence Centre carries out its tasks in accordance with this Regulation.

The Strategic Advisory Group - consisting of up to 20 members - would provide advice based on a regular dialogue between the Competence Centre and the cyber security competence community.

The European Union Agency for Cyber Security (ENISA) would be a permanent observer on the Governing Board of the Centre of Competence and may provide advice and input on the drafting of the strategy and the annual and multi-annual work programmes.

The Council position includes new articles on gender balance and on the legal personality of the Centre of Competence.

Voting rules

The Governing Board should use a consensual approach in its discussions. A vote should be held if the members of the Governing Board fail to achieve a consensus.

For certain decisions related to the implementation of the Union's budget, as well as for the annual work programme, the multi-annual work programme and the method of calculating Member States' contributions, the Commission would have 26% of the voting rights. The Governing Board would adopt its decisions by a majority of at least 75% of the votes of all its members.

National coordination centres

No later than six months after the date of entry into force of the Regulation, each Member State would designate an entity to act as its national coordination centre.

The national coordination centres would act as national contact points for the Community to assist the Competence Centre in fulfilling its mission and objectives, in particular, to coordinate the Community through coordination between its members in their Member State.

Cybersecurity Competence Community

The Community will contribute to the mission of the Competence Centre and the Network and will enhance, share and disseminate cybersecurity expertise across the EU.

The Community would be composed of collective bodies/organisations and would not include individuals. The Competence Centre and its bodies could draw on the expertise of individuals and natural persons as ad hoc experts.

European Cybersecurity Competence Centre

The European Parliament adopted a legislative resolution approving the Council position at first reading with a view to the adoption of 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 proposed regulation aims to help the EU maintain and develop the technological and industrial cyber security capacities needed to secure its digital single market.

The regulation:

- establishes the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres, and

- lays down rules for the designation of the national coordination centres and the establishment of the cybersecurity community of competences.

The Competence Centre, which will be based in Bucharest, will, inter alia, allocate cybersecurity-related funding from the Horizon Europe programme and the Digital Europe programme. It will be able to support, in connection with the Member States, the development and acquisition of advanced cybersecurity equipment, tools and data infrastructure in Europe and ensure wide deployment of the latest cybersecurity solutions across all economic sectors.

The European Cybersecurity Industrial, Technology and Research Competence Centre will work in cooperation with a network of national coordination centres designated by the Member States.

The Centre will also bring together key European stakeholders, including industry, academic and research organisations and other relevant civil society associations, to form a cybersecurity competence community to strengthen and disseminate cybersecurity expertise across the EU.