European Cybersecurity Competence Centre

2018/0328(COD) - 12/09/2018 - Legislative proposal

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 Union's 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.