European Cybersecurity Competence Centre

2018/0328(COD) - 22/02/2019 - Committee report tabled for plenary, 1st reading/single reading

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.