European Cybersecurity Competence Centre

2018/0328(COD) - 12/09/2018 - Document attached to the procedure

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 Union’s 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.