European Cybersecurity Competence Centre

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

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.