Council of the European Union

Brussels, 13 September 2018
(OR. en)

12104/18
ADD 5

Interinstitutional File:
2018/0328(COD)

CYBER 187
TELECOM 282
CODEC 1456
COPEN 290
COPS 313
COSI 190
CSC 252
CSCI 123
IND 239
JAI 874
RECH 374
ESPACE 39

COVER NOTE

From:	Secretary-General of the European Commission, signed by Mr Jordi AYET PUIGARNAU, Director
date of receipt:	12 September 2018
To:	Mr Jeppe TRANHOLM-MIKKELSEN, Secretary-General of the Council of the European Union
No. Cion doc.:	SWD(2018) 404 final
Subject:	COMMISSION STAFF WORKING DOCUMENT EXECUTIVE SUMMARY OF THE IMPACT ASSESSMENT Accompanying the document 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

Delegations will find attached document SWD(2018) 404 final.

Encl.: SWD(2018) 404 final

EUROPEAN
COMMISSION

Brussels, 12.9.2018
SWD(2018) 404 final

COMMISSION STAFF WORKING DOCUMENT

EXECUTIVE SUMMARY OF THE IMPACT ASSESSMENT

Accompanying the document

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

{COM(2018) 630 final} - {SEC(2018) 396 final} - {SWD(2018) 403 final}

Executive Summary Sheet

Impact assessment on: Proposal for creation of the Network of Competence Centres and European Cybersecurity Research and Competence Centre

A. Need for action

Why? What is the problem being addressed?

Today 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. The present initiative aims to contribute to tackling the following problems and related drivers of this situation:

Problem 1: 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;

Problem 2: Sub-scale investment and limited access to cybersecurity know- how, skills and facilities across Europe;

Problem 3: Few European cybersecurity research and innovation outcomes translated into marketable solutions and widely deployed across the economy.

These problems have a number of underlying drivers including insufficient level of trust between different actors of cybersecurity market, inherent limitations of existing cooperation and fund pooling mechanisms, the lack of framework for joint procurement for costly cybersecurity infrastructure and cybersecurity products/solutions as well as the unused potential of market push-pull mechanisms.

What is this initiative expected to achieve?

The initiative aims to ensure that the EU retains and develops the essential (technological and industrial) capacities to autonomously secure its digital economy, society and democracy, and that Member States benefit from the most advanced cybersecurity solutions and cyber defence capabilities. The initiative also aims at increasing the global competitiveness of EU cybersecurity companies and ensuring that European industries across different sectors have access to the capacities and resources to turn cybersecurity into their competitive advantage. This should be achieved by developing effective mechanisms for long-term strategic cooperation of all relevant actors (public authorities, industries, research community from both civil and defence areas), pooling knowledge and resources to provide leading-edge capabilities and infrastructures, stimulating wide deployment of European cybersecurity products and solutions across the economy and the public sector, supporting cybersecurity start-ups and SMEs as well as helping to close the cybersecurity skills gap.

What is the value added of action at the EU level?

The initiative would add value to the current efforts on the national level by helping to create an inter-connected, Europe-wide cybersecurity industrial and research ecosystem. It should encourage 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. It should help the EU and Member States take a proactive, longer-term and strategic perspective to cybersecurity industrial policy going beyond research and development only. This approach should help not only to come up with breakthrough solutions to the cybersecurity challenges which the private and public sectors are facing but also support the effective deployment of these solutions. It will also allow relevant research and industrial communities as well as public authorities to gain access to key capacities such as testing and experimentation facilities, which are often beyond the reach of individual Member States due to insufficient financial and human resources. It will also contribute to closing the skills gap and to avoiding brain drain by ensuring access of the best talents to large-scale European projects and therefore providing interesting professional challenges. All of the above is also seen as necessary for Europe to be recognised globally as a leader in cybersecurity.

B. Solutions

What legislative and non-legislative policy options have been considered? Is there a preferred choice or not? Why?

A number of policy options have been considered, both legislative and non-legislative. The following options were retained for an in-depth assessment:

1. **Baseline scenario** - Collaborative Option - assumes the continuation of the current approach to building cybersecurity industrial and technological capacities in the EU through supporting research and innovation and related collaboration mechanisms under Horizon Europe Programme;
2. **Option 1:** Cybersecurity Competence Network with a European Cybersecurity Industrial, Technology and Research Competence Centre entity empowered to pursue measures in support of industrial technologies as well as in the domain of research and innovation;
3. **Option 2:** Cybersecurity Competence Network with a European Cybersecurity Research and Competence Centre limited to research and innovation activities only;

The options discarded at an early stage included 1) No action at all; 2) Network of existing competence centres only and 3) Using an existing agency (ENISA, REA, or INEA).

In view of the general commitment already made by the Commission for the present initiative as well as in view of the important role to be played by Member States, the main distinction between the two policy options analysed in detail lies in their scope as reflected in their legal base: an entity only based on article 187 TFEU (Option 2) would limit the initiative to the sphere of research and innovation, and would typically presume a financial contribution from private actors. On the other hand, an entity based on a double legal base - art. 187 TFEU and art. 173 TFEU (Option 1) - would mean a broader mandate covering also, inter alia, deployment and industrial support and creating stronger synergies with cyber defence. It would also give a more prominent role to Member States – both in terms of their role in the governance as well as in their role as potential procurers of cybersecurity technology.

The analysis showed that Option 1 is best suited to achieve 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 this Option included 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; ability to structure cooperation of the public and private stakeholders coming from all relevant sectors, including defence; ability to create a real cybersecurity industrial policy by supporting activities related not only to research and development but also to market deployment. Last but not least Option 1 allows as well increasing coherence by acting as an implementation mechanism for cybersecurity-related funding from the Digital Europe Programme and Horizon Europe, and enhancing synergies between the civil and defence dimensions of cybersecurity in relation to the European Defence Fund.

Who supports which option?

According to the outcome of the consultation and evidence gathering processes there is a clear demand for both industrial and research communities to have a mechanism allowing the EU to have a coherent cybersecurity industrial policy going beyond research and development activities only if Europe is to become a global leader in cyber-security. At the same time stakeholders emphasised that the key to success will be a well-defined role of the Centre in supporting and facilitating the efforts of the Network and relevant communities and an inclusive, collaborative approach to the network to avoid creating new silos. The structure should also be flexible so that it can be easily adapted given that cybersecurity is a fast-pace environment. Throughout the process Member States emphasised the need to be inclusive towards all Member States and their existing centres of excellence and competence and to pay special attention to complementarity of actions. Specifically with regard to the Centre, Member States stressed the importance of its coordinating role in support of the network. Therefore, any Commission initiative will have to find the right balance in the governance and implementation structures and reflect this balance in the governance and implementation structures to ensure effective European coordination while taking into account the developments at the national level.

C. Impacts of the preferred option

What are the benefits of the preferred option (if any, otherwise main ones)?

The preferred option will allow 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). It would also have a positive impact on EU's competitiveness and SMEs as it assumes creating 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. This option allows pooling resources to invest in necessary capacities at the Member States' level and develop European shared assets while achieving economies of scale. This is likely to result in increased access for SMEs, industries and researchers to such facilities, which will stimulate innovation and shorten the development processes. This will also cut costs for some demand-side businesses and help them turn cybersecurity into their competitive advantage. The Option allows taking advantage of the dual-use market opportunities by allowing defence and civilian communities to work together on shared challenges. It is also likely to add-value to the national efforts related to addressing the cybersecurity skills gap. At the EU level, this option also allows to improve coherence and synergies between different funding mechanisms.

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) helping them to avoid potentially devastating consequences of cybersecurity attacks on this type of infrastructure.

What are the costs of the preferred option (if any, otherwise main ones)?

The costs related to the preferred option are mainly related to the costs of the functioning of the Centre and the National Coordination Centres. The costs related to the implementation of different funding programmes (Digital Europe Programme and Horizon Europe Programme) are subject to separate Impact Assessments.

How will businesses, SMEs and micro-enterprises be affected?

European companies, both on the cybersecurity demand and the supply side, including SMEs and micro-enterprises operating in the cybersecurity field, will be among the most impacted stakeholder groups. While the set-up of the Competence Centre and the Network does not impose regulatory obligations upon them, it will 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. In the case of SMEs and micro-enterprises the access to publically funded testing and experimentation facilities is even more important as they are lacking resources to either purchase or to travel outside their market (and often outside the EU) to find the necessary infrastructure. It is also hoped that this initiative would open up new markets for European SMEs and micro-enterprises active in the field of cybersecurity. In addition, the chosen mechanism will ensure coordination between research and industry and therefore direct the research efforts towards concrete industrial needs. The provision of cutting-edge expertise and tools in cybersecurity will indirectly support economic operators in complying with the NIS Directive.

Will there be significant impacts on national budgets and administrations?

The initiative will enable Member States to coordinate investments in necessary cybersecurity infrastructure at the national and European levels. The mechanism will allow to pool resources for tools and infrastructures which would otherwise be more costly or not affordable for individual Member States. Such approach would allow economies of scale and rationalisation. The financial contribution by Member States to the Competence Centre and relevant actions should be commensurate to the Union contribution.

Will there be other significant impacts?

Yes, the 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, which will be able to appropriately secure their existing assets and design secure innovative products while reducing security related R&D costs. This should ultimately allow the EU to become a leader in the next-generation digital and cybersecurity technologies.

D. Follow up
When will the policy be reviewed?
An explicit clause to monitor the key performance indicators (KPIs) as well as an evaluation and review clause, by which the European Commission will conduct an interim evaluation in order to measure the impact of the instrument and its added value, will be included in the legal instrument. The European Commission will subsequently report to the European Parliament and the Council. Following this evaluation, the Commission may propose a review and extension of the Competence Centre and Network's mandate.