BRIEFING

Initial Appraisal of a European Commission Impact Assessment

European Parliament

Establishing a cybersecurity competence centre and a network of national coordination centres

Impact assessment SWD(2018) 403 final, SWD(2018) 404 (summary)) accompanying the Commission's 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.

This briefing provides an initial analysis of the strengths and weaknesses of the European Commission's impact assessment (IA) accompanying the above-mentioned proposal, submitted on 12 September 2018 and referred to the Parliament's Committee on Industry, Research and Energy.

The proposal for which the above-mentioned impact assessment was prepared, follows on from the steps recently undertaken by the European Commission with regard to cybersecurity, including the adoption of the cybersecurity strategy in 2013, the creation of the public-private partnership on cybersecurity in 2016 and the implementation of the 2018 Directive on Security of Network and Information Systems (NIS). With these measures, the Commission aims to achieve EU cyber resilience by means of building an industrial and technological base for the EU's cybersecurity. The European Parliament also called for pursuing this goal in its June 2018 resolution on cyber defence. The Parliament specifically called for making the critical infrastructure resilient to cybersecurity threats, by means of stronger cooperation between industry, civil society and the EU Member States' governments.

With the current proposal, the Commission aims to create a new structure – a European cybersecurity competence centre with a network of national coordination centres – to pool and share cybersecurity research capacities and competence across the EU, which it regards as 'considerable but still fragmented'. Therefore, the creation of a European cybersecurity competence centre would, in the Commission's view, allow to tackle a series of problems related to the EU's insufficient cybersecurity technological and industrial capacities. In addition, the initiative would foster a regular dialogue with the private sector, consumers' organisations and other relevant stakeholders through the set-up of an industrial and scientific advisory board that would be building on and scaling up the existing public-private partnership on cybersecurity (cPPP).[1]

Problem definition

The IA describes the wider political and legal context of the proposal, namely the opportunities that fast-growing digitalisation brings to society and the economy, but also the many new cybersecurity risks accompanying it. In this regard, the EU is said to lack sufficient technological and industrial capacities 'to autonomously secure its economy and critical infrastructures and to become a global leader in the cybersecurity field' (IA, pp. 3-7). The report identifies three main problems affecting the EU's capacities with regard to cybersecurity: 1) an 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; 2) sub-scale investment and limited access to cybersecurity know-how, skills and facilities across Europe; and 3) few European cybersecurity research and innovation outcomes being translated into marketable solutions and widely deployed across the economy.

Author: Vadim Kononenko with Robin Stenstrom
Ex-Ante Impact Assessment Unit

PE 631.733 – February 2019

Four factors ('problem drivers') are identified as triggering the above problems:

- an insufficient level of trust between the different players in the cybersecurity ecosystem;
- Inherent limitations of the existing cooperation mechanisms applied to the highly complex cybersecurity ecosystem;
- lack of a framework for the joint procurement of costly cybersecurity infrastructure;
- unused potential of the push-pull mechanism for ensuring an effective market deployment of European cybersecurity products and solutions (IA, pp. 8-20).

Overall, the report's description of the problem, drivers and potential consequences is satisfactory. Each problem is examined in its interplay with its drivers as a way to explain how this interplay affects negatively the capacity of the EU to 'autonomously secure its economy, society and democracy as well as its ability to become a global leader in the cybersecurity field' and to take full advantage of the opportunities that are presented by the fast-growing information and communications technology (ICT) market (IA, p. 20). This interplay is clearly illustrated in the problem tree in the IA (p. 7).

At the same time, one could have expected a better mapping of the existing initiatives, agencies and programmes, as would have given a clearer and more comprehensive picture about where the need for EU action is felt the most. This would have been particularly helpful, given the IA's claim that without policy intervention, the problems faced by European cybersecurity are likely to increase and eventually result in a lack of access to security products and solutions produced in Europe – a situation that could undermine European citizens' trust and pose a certain level of security risk (IA, p. 20). The IA proceeds to argue that without any policy intervention, significant economic opportunities in the cybersecurity supply and demand sectors will be largely missed, leaving the European cybersecurity industry, especially SMEs, exposed to acquisitions and mergers by non-European companies, and potentially leading to a brain-drain (IA, p. 21). The report does not provide substantive quantitative data or concrete evidence to support this claim.

Objectives of the legislative proposal

The IA has identified **three general objectives** (p. 23), namely, to:

- ensure that the EU retains and develops essential (technological and industrial) capacities to autonomously secure its digital economy, society and democracy, and to ensure that Member States benefit from the most advanced cybersecurity solutions;
- increase global competitiveness of EU cybersecurity companies;
- ensure European industries' access to capacities and resources that would enable them to turn cybersecurity to their competitive advantage.

To achieve the general objectives, the following **five specific objectives** have been identified (IA, p. 23):

- develop effective mechanisms for long-term strategic cooperation among all relevant players (public authorities, industries, both the civil and the defence branch of the research community) with a view to setting and implementing a mission-driven, strategic cybersecurity agenda that reflects industrial and public authorities' needs;
- pool knowledge and resources to provide leading-edge capabilities and infrastructures to support the industry and the research community in developing and validating new technologically advanced products and solutions;
- stimulate wide deployment of European cybersecurity products and solutions across the economy and the public sector through joint procurement, among other things;
- support cybersecurity start-ups and SMEs to attract investment, including venture capital.
- support the closing of the cybersecurity skills gap by aligning cybersecurity skills programmes, adapting them to specific sectorial needs and facilitating access to targeted specialised training courses.

The general and specific objectives align well with the problems, as do the specific objectives, although these do not fully correspond to the S.M.A.R.T. criteria (requiring objectives to be specific, measureable, achievable, relevant and time-bound), outlined in the better regulation guidelines. However, the IA does not appear to have formulated operational objectives, which is contrary to the said guidelines.

The objectives section of the IA also contains an analysis of the 'functionalities and governance elements' of the proposed competence centre (IA, p. 23). These functionalities include:

- flexibility of cooperation between the coordination centres in the Member States;
- the role of the competence centre as the main implementation mechanism for cybersecurity activities within the next MFF;
- the competence centre's governance structure consisting of the governing board and the industrial and scientific board.

The length of existence of the competence centre and the network is to be linked to the duration of the MFF (2021-2027). These parameters appear to have been pre-set in the impact assessment and applied for defining the framework of the (consequently limited) policy options. The report does not explain why these parameters were formulated upfront and how they link with the problem definition, despite the fact that they appear to have considerably shaped the range of options.

Range of options considered

The IA considered three policy options and discarded another three at an early stage. The discarded ones include: taking no action at all and stopping all activities; using the network of existing competences without any common governance structure; and delegating the functions of the competence centre to an existing EU agency such as ENISA, REA, or INEA.[2] These options were discarded because they were 'contrary to the existing objectives' and 'practically impossible' (IA, pp. 36-37). The options that the impact assessment considered as realistic include:

– Baseline Scenario – Collaborative Option. This scenario envisages the continuation of the current collaborative mechanisms under the Horizon Europe programme. This collaboration would take place as a cPPP within the projects funded by the EU. However, the IA considers the cPPP as having significant limitations as a legal construct, as 'it does not envisage resource pooling for direct co-investment in e.g. necessary infrastructures or demonstration projects' (IA, p. 30). Under the baseline scenario, 'the European industries and authorities will take up risky experimentation by themselves[,] with their own resources and based on limited available infrastructure' (IA, p. 30). Other limitations of the cPPP concern the lack of a mechanism for creating the capacity to provide multinational project management support, testing and stimulation services. Last but not least, the cPPP is open to non-EU actors with non-EU suppliers.

– 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. Under this option (created under Articles 173 and 187 TFEU), the proposed Competence Centre would have its own public-public governance structure, staff and dedicated budget. The private sector would have an advisory role in the industrial and scientific advisory board. The IA mentions that experience with similar governance bodies with the same legal basis shows that the latter affords the flexibility required to meet the objectives. This flexibility is defined in terms of various structures that need to be set up: a network organised along geographical lines, a community along thematic lines, or a combination of both. The IA does not include examples to illustrate this in more concrete terms. Furthermore, one is left to wonder whether these possibilities could not have been defined and assessed as sub-options of option 1.

– **Option 2: Cybersecurity Competence Network with a European Cybersecurity Research and Competence Centre limited to research and innovation activities**. This option envisages establishing a network of competence centres with the cybersecurity research and competence centre

as a Union body under Article 187 TFEU. The Commission points out that an entity created under this legal basis would not be 'best placed to create synergies with the defence sector', a consideration that is very important in the field of cybersecurity. Furthermore, option 2 would limit the intervention to the area of research and innovation, as the capacity of such an entity to support the large-scale development and take-up of new secure technologies would be limited (IA, p. 35).

The IA identifies option 1 as the **preferred option**. The report states that option 1 would (among other things) ensure flexibility to allow for different cooperation models; provide a visible legal, contractual and organisational common framework; and allow the creation of a real cybersecurity industrial policy related not only to research and development but also to market development activities. In other words, option 1 appears to follow very closely the modalities that were set up before the options were formulated.

Given that that the parameters were defined before the start of the impact assessment and that the range of options is limited to two, with the main difference between them being the legal basis, one would have expected a more detailed explanation of how options 1 and 2 compare to the baseline. Furthermore, a more detailed assessment of the baseline against the objectives would have made the choice of the preferred option more substantiated. Finally, a more precise description of the content of the preferred option would have been commendable.

Scope of the impact assessment

The IA compares the options against the criteria of effectiveness, efficiency, and coherence. Regarding effectiveness, both options 1 and 2 would be more effective than the baseline scenario; however, the Commission regards option 1 as more effective in achieving all of the objectives.

Regarding the efficiency of the options, the IA assesses them against three categories of impacts: social, economic, and environmental. As far as the impact on the economy is concerned, the IA considers only impacts related to SMEs and competitiveness. Without much evidence, option 1 is stated to have a positive impact on competitiveness, competition and SMEs, which would be higher than in the baseline scenario. Option 2 is also seen as having positive impacts on the EU economy, although impacts on SMEs, competitiveness and competition are seen to have a neutral-to-positive impact. The IA explains that this option would not have a direct positive impact on improving the EU's standing on the global market; furthermore, it would not be sufficient to directly support the market deployment of cybersecurity products and solutions.

As far as the social and environmental impacts are concerned, the IA describes them as being slightly weaker in option 2 than in option 1, without however specifying these impacts in any concrete terms. Overall, the assessment of impacts in the IA report appears to lack substantial quantitative and qualitative evidence and relies mostly on stakeholders' opinion and general assumptions. Importantly, the assessment of impacts pays only scant attention to the impact on fundamental rights, despite its significance for the policy realm of cybersecurity.

Subsidiarity / proportionality

The IA argues that the Competence Centre should be established on a double legal basis due to the specific objectives to be achieved. Article 187 TFEU (first legal basis) would provide the structures needed for the efficient execution of EU research, technological development and demonstration programmes (proposal, p. 6). In addition, to enable measures in support of industry and competitiveness, Article 173(3) TFEU would act as the second legal basis (IA, p. 21). The IA regards cybersecurity as a common issue of the EU-28 and therefore sees a common need to make sure that the EU attain the technological capacities to address this issue adequately and effectively. The IA also argues that the cybersecurity challenges and insufficient coordination within and across the public sector, industry and research communities require further support from the EU level (IA, p. 21).

Regarding the added value of EU action, the IA considers that the establishment of the Competence Centre and Network could add value to the European-wide cybersecurity ecosystem, something that

stakeholders from the industry and research communities have confirmed in the consultation (Annex 2 to the IA) (see section on Stakeholder Consultation further down). The IA underlines that the initiative does not target operational cooperation on cybersecurity, which is governed by the NIS Directive. The objective of the initiative is considered not to be achievable by Member States alone and to be better achieved at EU level by pooling efforts together. The IA therefore states that EU action is justified as far as subsidiarity and proportionality are concerned, even though it does not provide an assessment of proportionality (IA, p. 22).

No reasoned opinions from the national parliaments were received by the subsidiarity deadline of 13 November 2018.

The European Economic and Social Committee (EESC) adopted its opinion on the proposal on 23 January 2019. The opinion states that the EESC 'supports the general objectives of the proposal and is aware that specific aspects of how it will work will be dealt with at a later point. However, as this is a regulation, it considers that certain sensitive aspects related to governance, funding and achieving the objectives set should be outlined in advance. It is important that the future Network and the Centre should build as far as possible on the Member States' expertise and cyber skills, and that competences should not all be concentrated in the new Centre'.

Budgetary or public finance implications

With regard to implications for the EU budget, the preferred option would entail a recurrent annual cost of €15-20 million. This cost would be covered by the EU budget. Some savings can be expected for the Member States' budgets as a result of a reduction in costs related to cybersecurity incidents; however, the Commission does not provide exact figures in this regard.

SME test / Competitiveness

According to the IA report, options 1 and 2 have an equally positive impact on SMEs and competitiveness. However, the IA does not elaborate on this assumption; it expresses the view that SMEs would be well-positioned to benefit from the opportunities offered by the proposal, as their costs are likely to be reduced in relation to designing new products and as a result of their increased access to publicly funded testing and experimentation facilities. The IA also assumes that the proposal would open up new markets for European SMEs in the field of cybersecurity, but does not clearly identify these markets nor specify whether European SMEs would be able to compete with the established international players.

The report assumes that option 1 would have a positive impact on the EU's competitiveness and on SMEs, as this option would lead to creating a mechanism capable of building the Member States' and the Union's cybersecurity industrial capacities, and of effectively translating European scientific excellence into marketable solutions that could be deployed across the economy.

On the other hand, option 2 is considered to have a mixed neutral-to-positive impact on the economy, competitiveness and SMEs. The report argues that this option is likely to contribute to the increased competitiveness of the European cybersecurity industry, although it would not have a direct positive impact on improving the industry's global market position in terms of market share. This option, according to the IA, is also likely to help Member States get access to the outcomes of cybersecurity research and innovation projects, but would not be sufficient to help the wide deployment of these outcomes across key sectors relevant to the public domain. Without a detailed quantitative assessment, the differences between the two options as regards their impact on competitveness are not entirely clear.

Simplification and other regulatory implications

The IA mentions increased coherence and synergies between the proposal and different funding mechanisms, such as Digital Europe, the European Defence Fund and Horizon Europe, as having potential for simplification; however, given that the proposed centre is a novelty, such a claim is difficult to assess.

Quality of data, research and analysis

The Commission admits that the quality of the impact assessment was 'impacted by the overall scarcity of evidence in the field of cybersecurity as a whole' (IA, Annex 1 p.10). It is not clear, however, what evidence is scarce. The Commission lists various sources, such as official EU documents and various external analyses in Annex 2, but it is not clear which sections of the impact assessment were informed by these sources, and how.

Stakeholder consultation

Contrary to the requirements of the better regulation guidelines, an open public consultation was not carried out for this impact assessment, and the Commission provides no explanation for its decision. Several other stakeholder consultation activities were conducted, but these were not directly linked to the current proposal. Two general open public consultations were carried in 2018: one concerning a consultation on the EU funds in the areas of investment, research, innovation, SMEs and the single market, and one concerning security. Both of these consultations were conducted in preparation of the new multiannual financial framework for the 2021-2027 period and did not address the issue of cybersecurity in much detail.

The Commission conducted an online public consultation in January-April 2017, which was focused on the future of the European Union Agency for Network and Information Security (ENISA) Carried out for the purpose of evaluating and reviewing ENISA, this consultation could have not been very useful for the purposes of weighing the options in the IA, as the option of using ENISA as a competence centre was discarded at an early stage of the IA.

Another 12-week online public consultation focused on the contractual PPP on cybersecurity was carried out in 2016. It appears that Member States were consulted on the proposal primarily through a high-level roundtable organised in December 2017, where they 'welcomed the intention to set up a cybersecurity competence network' and 'stressed the need for complementarity' (explanatory memorandum to the proposal, p. 8). According to the Commission, most Member States saw the added value in supporting industry through research and development. Given that the strengthening of the link between cybersecurity research and industry is a core difference between the two options and that this difference determined the choice of the preferred option, one could have expected a more detailed explanation of the stakeholders' position on this issue. It is also not clear which exactly industry stakeholders were consulted, as the report does not specify how many companies (including SMEs) were involved in the consultation activities.

The report mentions that the Commission also received feedback from stakeholders for the inception impact assessment (22 responses). As the results of the inception-stage consultation showed a clear division between stakeholders regarding the options, an open public consultation would have been all the more helpful for this impact assessment. The IA report includes the mandatory annex on the stakeholders' consultation (Annex 2). The lessons drawn from the consultation activities are helpful for understanding the problem but not specific enough to feed into the formulation of options, in particular regarding the governance of the proposed centre.

Monitoring and evaluation

The IA states that a monitoring clause with a set of key performance indicators (KPIs) would be included in the new legislative instrument. The report presents a list of seven overarching KPIs that 'could be used to monitor progress towards meeting the objectives, impact and success of the entity' (IA, pp. 46-47). The KPIs that the IA proposes include among others: cybersecurity infrastructure jointly procured; number of hours made possible for testing and experimentation for researchers and industry across the Network; European suppliers' global market share of cybersecurity technologies; and number of copyright patents, scientific publications and commercial products. It should be noted that without operational objectives, it is difficult to assess whether these KPIs provide the best tool for measuring the achievement of all the objectives of this proposal. Moreover, the proposal does not include these

indicators, although it closely follows the IA's recommendation to include an evaluation review clause, committing the Commission to conduct an independent evaluation (proposal, Article 38).

Commission Regulatory Scrutiny Board

The Commission's Regulatory Scrutiny Board (RSB) issued a positive opinion with reservations on the draft IA on 12 September 2018. The main reservations of the RSB concerned the need to better explain the specificity of the cybersecurity sector and the differences between the two policy options. In its comments, the RSB considered the IA's description of the proposed centre's governance as particularly needing improvement, especially when it comes to the practicalities of the co-investment scheme, the degree of centralisation, and the link to other bodies such as ENISA. The Commission explains the revisions it made in alignment with the comments of the RSB in a compulsory section of the IA report (Annex 1, p. 3). Overall, the reservations of the RSB remain valid, despite the revisions made in the final version. In particular, the differences between the two options, which the RSB noted as having been described in vague terms (except for the explanation that each requires a different legal basis), would still deserve further elaboration.

Coherence between the Commission's legislative proposal and IA

The proposal appears to correspond to the preferred policy option indicated in the IA.

Conclusions

The IA report describes the significance of cyber defence and the potential for improvement in this field for the EU in a logical way. However, the IA does not appear to have fully followed the requirements of the better regulation guidelines, in particular with regard to the holding of an open public consultation, as no such consultation was conducted. The IA presents a limited range of options selected on the basis of a number of pre-set parameters, which could have possibly constrained the scope of the IA. A more effective use of quantitative and qualitative evidence would have strengthened the analysis of the options' impacts. Furthermore, the report could have provided a more detailed and precise description of the preferred option.

ENDNOTES

[1] For further analysis of the proposal, see Negreiro M., The new European cybersecurity competence centre and network, legislative briefing, EPRS, 2019.

[2] European Union Agency for Network and Information Security (ENISA), Research Executive Agency (REA), and Innovation and Networks Executive Agency (INEA).

This briefing, prepared for the Committee on Industry, Research and Energy (ITRE), analyses whether the principal criteria laid down in the Commission's own Better Regulation Guidelines, as well as additional factors identified by the Parliament in its Impact Assessment Handbook, appear to be met by the IA. It does not attempt to deal with the substance of the proposal.

DISCLAIMER AND COPYRIGHT

eprs@ep.europa.eu (contact)

www.eprs.ep.parl.union.eu (intranet)

www.europarl.europa.eu/thinktank (internet)

http://epthinktank.eu (blog)