BRIEFING

Initial Appraisal of a European Commission Impact Assessment

European Parliament

Improving the common level of cybersecurity across the EU

Impact assessment (SWD(2020) 345, SWD(2020) 344 (summary)) accompanying a Commission proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148

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 16 December 2020 and referred to Parliament's Committee on Industry, Research and Energy (ITRE). With this proposal, the Commission puts forward a package of measures to improve further the resilience and incident response capacities of the European Union in the field of cybersecurity and critical infrastructure protection.[1]

The proposed measures are designed to improve the existing EU cybersecurity framework, primarily the Network and Information Systems (NIS) Directive[2] adopted in 2016. The NIS Directive established a European cybersecurity certification framework to promote certification schemes for specific information and communication technology (ICT) products and services, provided for mutual recognition of certificates so as to avoid further market fragmentation in Europe, and also reformed the European Union Agency for Network and Information Security (ENISA), to enhance its supporting functions for Member States in achieving cybersecurity resilience.[3]

The NIS Directive is subject to review by 9 May 2021. In this context, the Commission conducted an evaluation (see Annex 5 of IA) on the functioning of the directive and, simultaneously (rather than sequentially), an impact assessment (IA) of potential measures for improvement. The analysis in the IA focuses in particular on possible ways to widen the scope of the existing directive,[4] improve supervision and enforcement, and level out Member States' cybersecurity capabilities. The review of the NIS Directive was included in the Commission's adjusted work programme for 2020 as part of its key policy objective to make 'Europe fit for the digital age'.

Problem definition

The IA presents a very clear definition of the problem, which consists of three aspects: (1) low level of cyber-resilience of businesses operating in the European Union, (2) inconsistent resilience across Member States and sectors, (3) low level of joint situational awareness and lack of joint crisis response. According to the Commission, this three-pronged problem stems from the shortcomings of the existing NIS Directive as identified in the evaluation. These shortcomings include the limited scope of the NIS Directive in terms of sectors and companies covered, divergent security and reporting requirements, ineffective supervision and enforcement, uneven resources for competent authorities and limited information sharing between Member States.

Consequently, the IA identifies the costs to companies directly and indirectly hit by a cybersecurity incident, and the externalities (e.g. costs of an incident) for suppliers and customers, which are becoming even greater owing to the interdependencies between Member States and limited EU incident response capacity (p.15). The section in the IA that describes how the problem will evolve is convincing on cybersecurity being a major concern for the EU in the coming years, as the number

Author: Vadim Kononenko
Ex-Ante Impact Assessment Unit

PE 662.606 – February 2021

of incidents is likely to increase because of 'malicious actors' (for example organised crime groups) rapidly increasing in sophistication. However, according to the IA, in the absence of further regulatory intervention, 'discrepancies in Member States' capacities' will not disappear (p. 28). The IA points out that the shortcomings of the existing framework – divergent reporting requirements and limited information-sharing across the EU – make it difficult to assess precisely the scope of the problem.[5]

Subsidiarity / proportionality

The legal basis for the NIS Directive is Article 114 of the Treaty on the Functioning of the European Union, which confers upon the EU the competence to enact measures for the approximation of national rules whose objective is the establishment and functioning of the internal market. The decision of the EU to intervene is explained on the basis of three factors, namely: (i) the increasingly cross-border nature of NIS-related threats and challenges; (ii) the potential of Union action to improve and facilitate effective and coordinated national policies; and (iii) the contribution of concerted and collaborative policy actions to effective protection of data protection and privacy.

In discussing the proportionality of the intervention, the IA states that the measures under Options 2 and 3 do not go 'beyond the necessary' and 'do not impose disproportionate costs'. The IA clarifies that the security measures and reporting obligations set out in both these options correspond to the Member States' requests to further clarify and harmonise the requirement level and would help ensure a level playing field for similar entities across the EU, while at the same time levelling and raising the level of cyber resilience across Member States (IA, pp. 89-90). In terms of the choice of legal instrument, the IA explains that a significant number of Member States were in favour of a directive rather than a regulation.

No national parliament had submitted a reasoned opinion at the time of writing of this initial appraisal.

Objectives of the initiative

The IA includes **three general objectives**. They are linked to the three aspects of the problem described above.

- Increase the level of cyber-resilience of a comprehensive set of businesses operating in the EU across all relevant sectors.
- Reduce inconsistencies in resilience across the internal market in the sectors already covered by the NIS Directive.
- Improve the level of joint situational awareness and collective capabilities to prepare and respond to incidents.

The IA specifies that these general objectives are inter-related because they include synergies and trade-offs. As an example of synergy, the IA mentions increased level of cooperation between competent authorities in Member States. As for trade-offs the IA notes that enhancing security could bring additional costs to businesses, in particular small and medium-sized enterprises (SMEs). This is explained in more detail in the section on SMEs.

The **specific objectives** outlined in the IA relate to (in summary, full wording on p. 31 of IA), 1) proper uptake of cybersecurity measures by entities in all sectors that are dependent on network and information systems; 2) proper reporting of incidents; 3) more effective enforcement of the rules laid down by the legal instrument; 4) ensuring a comparable level of resources across Member States allocated to competent authorities; 5) ensuring that essential information is exchanged between Member States by introducing clear obligations for competent authorities to share information and cooperate when it comes to cyber-threats and incidents and by developing an EU joint operational crisis response capacity.

According to the Commission's Better Regulation Guidelines, objectives should be SMART (specific, measureable, achievable, realistic and time-bound).[6] The objectives described in the IA, including

the operational objectives outlined in Annex 12 appear neither specific nor time-bound. Furthermore, the operational objectives are not specific about deliverables that the preferred policy option is expected to achieve.

Range of options considered

The Commission explains that the policy options were designed based on the potential for intervention in the main areas of the NIS Directive (where the problem was identified as the most acute): 1) sectoral scope and coverage of entities, 2) security requirements and reporting obligations, 3) supervision and enforcement, 4) cooperation and information-sharing. The policy options are said to have been developed 'as a unified set of actions and measures which function as a whole: the policy choice in one area being dependent on the choices made in the others'.

Altogether, the Commission formulated four policy options including the status quo option. The options range from non-legislative (Option 1) to an option with limited changes (Option 2) and an option with substantial changes (Option 3). The IA provides a detailed overview of policy Options 2 and 3 and their correspondence to the specific objectives in Annex 8. The options are summarised in the box below:

Box 1 – A summary of policy options

Option 0: baseline (status quo):

In this scenario the NIS Directive remains unchanged. The Commission envisages that the fragmented approach to cybersecurity across the EU will be maintained, 'with more ad hoc solutions and less coherent responsibility sharing' (IA, p.35). In particular, the status quo option would not improve reporting of incidents by Member States, and the level of supervision and enforcement would remain low. Finally, Member States would not be likely to develop their capabilities evenly, while cooperation and information-sharing would remain largely voluntary.

Option 1: Non-legislative measures to align implementation of the NIS Directive (discarded option)

In this scenario, there would be no change at legislative level. Instead, the Commission would issue recommendations and guidelines. Option 1 closely resembles the baseline scenario. The IA notes some changes however, namely that the Commission would issue more recommendations on sector-specific aspects, as well as on security requirements and thresholds for incident reporting. For the other problematic aspects (supervision and enforcement, cooperation and information-sharing), no major improvement is envisaged, as with the baseline scenario.

Option 2: Limited changes to the current NIS Directive for further harmonisation

This scenario would entail targeted amendments to the NIS Directive, including the extension of the scope to subsectors of those already covered and several other amendments that would aim at guaranteeing 'certain immediate solutions'. In order to be able to work out these solutions, PO2 envisages bringing under the scope of the NIS Directive additional sectors, subsectors and services. The IA provides a list of these services on pp. 41-52. The list of services includes a brief explanation as to why these additional sectors were chosen. The choice was based on the criteria of Member States national risk evaluations, results of stakeholder consultation and the considerations gained during the Covid-19 pandemic. For example, for the waste management sector, the IA explains that damaging or even catastrophic environmental releases may be triggered by cyber-attacks. The table does not however specify whether this was the conclusion of the stakeholder consultation or a national risk assessment. The IA mentions despite this expansion of the scope, the overall identification of incidents would remain complex and would not essentially improve. On reporting obligations, Option 2 does not envisage a centralised EU-level reporting system other than establishing more stringent definitions (deadlines, content) for reporting of incidents. On supervision, enforcement and cooperation, Option 2 relies on a voluntary approach by Member States, as in the current framework. Should national authorities need to impose sanctions on operators of essential services and digital service providers, as part of enforcement, the size of the penalties would be at the Member States' discretion.

Option 3. Systemic and structural changes to the NIS Directive (new directive) **(preferred option).**

This scenario would entail repealing the existing NIS Directive. A new directive would cover an even wider segment of economic entities across the EU, establish more focused supervision, streamline obligations and build a basis for enhanced shared responsibilities between Member States.

In detail, this entails that, unlike Option 2, a new directive would have clear-cut scope, dividing the entities into 'essential' and 'important' categories. Both categories would be subject to the same security requirements and reporting obligations, however, their supervision and penalty regimes would differ. This would allow the competent authorities to focus on compliance of the 'essential' entities (see IA, Table 4, p. 59 for the list of these 'essential' entities). For reporting purposes, Member States would be obliged to send more frequent (monthly) reports to ENISA, including data on cybersecurity incidents, threats and vulnerabilities. Under Option 3, supervisory measures and penalties are defined (with a maximum of at least €10 million, IA, p. 65). As regards cooperation and information-sharing, in addition to the provisions of Option 2 (the obligation of the Member States to ensure that competent authorities have the necessary powers and means to assess compliance with the NIS obligations and that they can require entities under the extended NIS scope to provide any information necessary to assess their cybersecurity measures), the new directive (among other things) requires Member States to develop a common policy framework on coordinated vulnerability disclosure. A registry of such disclosures would be kept by ENISA.

Source: Author, based on IA, pp. 32-69

It should be noted that as Option 1 was discarded and not retained for full assessment, the choice of realistic options was narrowed down to only two in addition to the baseline (status quo). The IA compares the two remaining options on the basis of all the criteria of the Better Regulation Guidelines. The options are compared for effectiveness, efficiency, and coherence with other legislation, initiatives or policy measures. The comparison could have been more thorough however. For example, the options are compared only superficially on proportionality despite the latter being one of the compulsory criteria for comparison according to Better Regulation Guidelines. The IA argues that Option 3 is more effective because it 'goes beyond immediate fixes' and moves towards 'a more pragmatic and hands-on framework for operational cooperation, supervision and enforcement' (IA, p. 88). Following this logic, the effectiveness of Option 3 is indeed likely to be greater than the other options, however a more detailed reasoning and assessment would have benefited the analysis.

Likewise, when comparing the options for efficiency, the IA logically notes that Option 3 entails higher costs owing to the extension of the sectoral scope. However, the IA concludes that this option is more efficient because the administrative burden would be balanced by increased cooperation between Member States including mutual assistance and peer-review mechanisms and a 'better overview of and interaction with key businesses'.

With regard to coherence, the IA notes that Option 3 would ensure coherence with the upcoming cybersecurity certification schemes being prepared by ENISA on the basis of the Cybersecurity Act, as well as with specific instruments such as the EU toolbox on security of 5G networks. Regarding the choice of instrument – EU directive – the IA mentions more leeway for Member States in preparation, compliance costs and expenses, which should ease the administrative burden.

The IA defines Option 3 as the preferred option (IA, Table 5, p. 91). The estimated costs and benefits of the preferred option in this initiative are summarised in the quantification tables in Annex 10 of the IA. The estimation of costs and benefits generally follows the EU Better Regulation Guidelines (Tool #59). Owing to a lack of data, the estimation is based on a linear extrapolation using the most conservative assumptions.

Assessment of impacts

The impact analysis of the options is rather brief. The IA mentions that for economic impact, there is no available comparable economic data to measure the actual impact of the NIS Directive.

Therefore, all options, including the baseline scenario were assessed against other available indicators (e.g. level of investment in ICT security). For the economic impact, the IA concludes that while Options 2 and 3 both aim to increase cybersecurity, Option 3, being more effective, may have a bigger positive economic impact on the single market because it would ensure a level playing field across Member States. The IA clarifies that there are costs currently borne by competent authorities. These costs stem from the current NIS obligation relating to development, monitoring and implementation of national strategies, the identification process depending on the system chosen at national level, processing of incident reporting, and interactions with companies. There are also costs linked to participation in the cross-border operational cooperation body (Cooperation Group) and exchanges. Under Option 3, the EU agency for cybersecurity ENISA will face additional tasks and incur additional administrative costs. This will require reshuffling of the existing resources of ENISA and supplementary posts.

Furthermore, according to the IA, the preferred policy Option 3 (as compared with Option 2) would lead to certain compliance and enforcement costs for the relevant entities and Member State authorities (an overall increase of about 20 to 30 % of resources is estimated).[7] However, the IA points out that the new framework would also bring substantial benefits through a better overview of and interaction with key businesses, enhanced cross-border operational cooperation, and also mutual assistance and peer-review mechanisms. This would lead to an overall increase in cybersecurity capabilities across Member States.

As far as social impact is concerned, the IA applies the same logic by stating that Option 3 would generate a more extensive positive impact on society. The IA does not specify what positive social impacts this entails in practice. The IA does not envisage significant environmental impacts of any options. Finally, the impact on fundamental rights is understood to be positive because strengthened cybersecurity would 'most likely lead to improved personal data protection' (IA, p. 67).

Overall, a fuller impact analysis might have been expected, particularly in terms of cost implications (because of increased compliance costs for companies but also public costs) and impacts on fundamental rights.

SMEs / competitiveness

According to the Eurostat data used in the IA, most SMEs already use some cyber-protection measures (e.g. regular updates of software and a two-step authentication procedure). However, when it comes to stronger cyber-protection measures, SMEs vary significantly. This means that the more stringent policy option would entail a greater burden on SMEs. Cybersecurity is considered a problem by SMEs but they consider difficulty accessing ICT services to be an even bigger problem. This is due to the fact that ICT security relies primarily on external suppliers. Large companies normally have their own cybersecurity departments. Under the baseline option and Option 2, SMEs would bear greater administrative and compliance costs than under Option 3. This is because the latter option would remove small and micro-businesses from the scope of the NIS framework. At the same time, in terms of benefits, raising the level of security requirements for these entities would also incentivise their cybersecurity capabilities and help improve their ICT risk management.

With regard to competiveness, the IA specifies that Option 2 is likely to have a positive albeit limited impact on ensuring a level playing field across Member States. Option 3 is stated as being likely to have a positive direct impact because it would probably reduce cybersecurity information asymmetries among undertakings and incentivise the cybersecurity capabilities of SMEs. Option 3 focuses on harmonising security requirements, which could in turn lead to improvements in the development of cybersecurity markets in Europe, increasing competitiveness and investment in start-ups.

Simplification and other regulatory implications

As a REFIT initiative that should aim to reduce regulatory costs and burdens, the IA explains that Option 3 provides for the general exclusion of micro- and small entities from the scope of the

NIS Directive and a lighter supervisory regime for a large number of new entities (in the 'important entities' category). This is likely to have a simplification effect for those entities. As further simplification measures, the IA lists six different steps (IA, pp. 92-93). Of all these measures, the establishment of a central registry operated by ENISA for all providers of digital services, the inclusion of electronic communication networks within the scope of the revision of the NIS Directive and the repeal of networks' security obligations from the EIDAS Regulation and the European Electronic Communication Code would seem likely to have the greatest impact in terms of simplification. The IA also implies that simplification would happen under the provisions of Option 3 concerning cross-border cooperation. The IA states that quantification of the actual effects of the harmonisation measures would not be possible, owing to wide cross-sector and cross-country differences (IA, p. 94).

Monitoring and evaluation

The IA envisages a review to evaluate how the objectives were achieved within 54 months of the proposal coming into force. A table with monitoring indicators, expected targets and frequency of monitoring per indicator can be found in Annexes 11 and 12 of the IA. The monitoring indicators appear to correspond to the specific and operational objectives. According to the IA, the Commission will conduct an assessment of indicators starting 54 months following the entry into force of the new NIS legal act. In practice, a significant part of the monitoring appears to be delegated to ENISA. It is envisaged that ENISA would be conducting systematic monitoring of the impact of the NIS framework through an annual business survey. It is not clear what the status of this survey is going to be as compared to the legal monitoring obligations.

Lack of available data and weak reporting obligations might pose an obstacle to successful monitoring of the proposed directive. The IA highlights in particular returns on security investments. Systematic EU-level indicators and data are currently missing. Another potential obstacle mentioned in the IA is knowledge of the new NIS Directive by the management of all essential and important authorities and entities.

Stakeholder consultation

The Commission organised a series of stakeholder consultation activities (for more details, see Annex 2 of the IA) including an **open public consultation** running for a 12-week period (7 July 2020 to 2 October 2020) and covering both the IA and the evaluation of the NIS Directive. The consultation triggered around 207 replies. In addition, a series of **targeted interviews** were conducted in 2019. The interviews assessed the consistency of approaches taken by Member States under the existing NIS Directive. Feedback was also gathered on the **inception impact assessment published in June 2020** (42 replies). ENISA conducted various surveys (the Commission identified the target groups and selected the questions) on three stakeholder groups: competent authorities, operators of essential services and digital service providers. **Workshops, in-depth interviews, country visits**, in all Member States and involving 117 national authorities, were also organised.

The IA covers the feedback received during these consultation activities well. It appears however that most of the respondents found it very difficult to identify precise measures for improvement of the NIS Directive. It would have been worth the IA providing a more precise explanation of how stakeholder feedback fed into the formulation of the policy options as it is not always clear what the views of stakeholders were regarding the options. Finally, given ENISA's central role in the functioning of the existing framework – and the proposed new directive – it would have been useful had the IA gathered feedback from ENISA.

Supporting data and analytical methods used

A description of the research process in support of the IA can be found in Annex 1, p.5 of the IA. The IA draws on the findings of an evaluation of the NIS Directive (Annex 5), supported by an external study contracted by the Commission to feed into both the evaluation and the IA process. The

support study, conducted by a consortium of Wavestone, Centre for European Policy Studies (CEPS) and a consulting company ICF, was launched in April 2020 but was not yet completed at the time the IA was published.[8] This could be explained by the fact that the Commission announced in its 2020 work programme that it would bring forward the review of the directive to the end of 2020 (see IA, Annex 5, p. 84). The Commission generally seems open about data limitations. The IA report admits that there are significant gaps in knowledge and data at EU level, partially owing to the shortcomings of the NIS Directive itself, but also due to the sensitivity of cybersecurity incidents.[9] This general limitation of data is also highlighted in the cost-benefit analysis, as it relies on the data available at Eurostat and from the Digital Economy and Society Index (DESI) that is not specific to cyber-threat accidents or cybersecurity investment.

Follow-up to the opinion of the Commission's Regulatory Scrutiny Board

On 18 November 2020, the Regulatory Scrutiny Board (RSB) issued a positive opinion with reservations. According to the RSB opinion, the problem analysis did not discuss sufficiently how enforcement has integrated cross-border spill-overs in risk assessments of entities in key sectors. Importantly, the IA did not explain what success would look like for the initiative. The RSB also noted that the list of options and justifications provided was not exhaustive, especially regarding the sectoral coverage. The impact analysis was also deemed lacking in depth, in particular regarding the costs assessment. The final IA report does not explain if and what comments of the RSB were addressed, nor does it provide the compulsory annex outlining the revisions made after the RSB comments. Overall, most of the RSB comments, for example regarding the limited analysis of impacts, remain valid in the final IA, including the comment relating to the need to give a better explanation of the criteria for sectoral coverage.

Coherence between the Commission's legislative proposal and IA

The proposal appears to follow the general considerations of the IA. The preferred option identified in the IA is at the basis of the proposal. The monitoring provisions however do not appear to be described in the proposal in the same detail as they are laid out in the IA.

Drawing on the findings of an evaluation of the NIS Directive, the IA generally appears to provide a clear and relevant analysis of the shortcomings of the existing NIS Directive and the policy options available for their improvement by a new legal act. It appears that the IA's assumptions are based on a thorough stock-taking exercise involving the consultation of a large number of stakeholders. The IA could however have explained the practical implications of the proposed initiative in greater detail, in particular by giving examples of the already existing interaction between private entities and relevant authorities, and cross-border cooperation (or lack thereof) between Member States. The IA also demonstrated openness about data limitations and a sufficient degree of adherence to the Better Regulation Guidelines. However, it would have been useful if the IA had provided a fuller impact analysis, in particular of potential economic costs and fundamental rights implications, as noted in the RSB opinion. Finally, the range of options assessed is limited to two, in addition to the baseline. Given that the final recommendation of the assessment is a significant revision of the existing legal framework, a more granular formulation of the policy options set out in the IA might have been expected.

ENDNOTES

[1] See explanatory memorandum, p .1. The package includes a new strategy on cybersecurity with the aim of strengthening the Union's strategic autonomy to improve its resilience and collective response and build an open and global internet. Finally, the package contains a proposal for a directive on the resilience of critical operators of essential services, designed to mitigate physical threats against such operators.

[2] Directive (EU) 2016/1148 of the European Parliament and the Council of 6 July 2016 concerning measures for high common level of security of network and information systems across the Union.

[3] See also Katharina Eisiele, EU Cybersecurity agency and certification, Initial Appraisal Briefing, EPRS, European Parliament, December 2017; and from an ex-post perspective, Anna Zygierewicz, The European Union Agency for Network and Information Security (ENISA), EPRS, European Parliament, May 2017.

[4] The current directive covers seven sectors (including energy, transport and critical infrastructure). The European Parliament has called on the Commission 'to assess the need to further enlarge the scope of the NIS Directive', see Resolution of 12 March 2019 on security threats connected with the rising Chinese technological presence in the EU and possible action on the EU level to reduce them (2019/2575(RSP)).

[5] 'There is abundant anecdotal data of incidents or estimations but varies by scope (sectors, countries, regions), and data by sector can vary remarkably', Annex 10, p. 65.

[6] See Tool #16 of the Better Regulation Toolbox.

[7] It is estimated that the companies that would fall within the scope of the NIS framework would need an increase of a maximum of 22 % of their current ICT security spending for the first years following the introduction of the new NIS framework (this would be 12 % for companies already within the scope of the current NIS Directive). However, this average increase of ICT security spending would lead to a proportionate benefit of such investments, notably due to a considerable reduction in the cost of cybersecurity incidents (estimated at €11.3 billion over 10 years).

[8] Study to support the review of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive) – No 2020-665, Wavestone, CEPS and ICF.

[9] The provisions of the NIS Directive require Member States to provide the Commission with only a limited set of data. For instance, national authorities are not required to submit the names of the identified operators, which makes it difficult for Commission services to compare the results of the identification process in terms of the completeness of the list and the impact on companies of the same size and belonging to the same sector. See, Report from the Commission to the European Parliament and the Council assessing the consistency of the approaches taken by Member States in the identification of operators of essential services in accordance with Article 23(1) of Directive 2016/1148/EU on security of network and information systems, COM(2019) 546.

This briefing, prepared for the Industry, Research and Energy (ITRE) committee, analyses whether the principal criteria laid down in the Commission's own Better Regulation Guidelines, as well as additional factors identified by 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)