CENTER FOR DATA INNOVATION

Feedback to the European Commission on the Cyber Resilience Act initiative

The Center for Data Innovation (Transparency Register #: 367682319221-26) is pleased to submit this feedback on the European Commission's consultation and call for evidence regarding the Cyber Resilience Act initiative. The Cyber Resilience Act initiative seeks to work in conjunction with existing legislation, like the Cybersecurity Act and the Directive on the security of Network Information Systems, to improve cybersecurity by addressing gaps in the existing regulatory framework for digital products and services.[1]

We would like to commend the European Union (EU) for focusing on the growing threat of cybersecurity incidents. In 2020, global cybercrime cost €5.5 trillion, and global cybercrime is predicted to cost $10.5 trillion by 2025.[2] As cybersecurity vulnerabilities continue to grow, the EU can play an important role in bolstering cybersecurity practices.

The Commission has outlined five broad policy options it is considering at this stage. In response to the Commission's call for evidence for its impact assessment, the following discusses these options as well as their potential benefits and drawbacks. We caution against both maintaining the status quo or pursuing broad horizontal regulation and offer suggestions on how the Commission may pursue the other options.

OPTION ONE: MAINTAIN THE STATUS QUO

The first option proposed by the Commission focuses on maintaining the current supranational legislation regarding the cybersecurity of tangible products:[3]

> Maintaining the status quo – this would involve existing legislation (e.g. the Delegated Regulation under the Radio Equipment Directive, legislation on medical devices, motor

[1] European Parliament and European Council, "Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)," April 17, 2019, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32019R0881. European Parliament and European Council, "Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union," July 6, 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016L1148.

[2] Joint Research Centre, "Cybersecurity – Our Digital Anchor" (European Commission, 2020), https://publications.jrc.ec.europa.eu/repository/handle/JRC121051. Steve Morgan, "Cybercrime To Cost The World $10.5 Trillion Annually By 2025" (Cybercrime Magazine, November 13, 2020) https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/.

[3]

> vehicles, machinery or product safety, etc.) partially addressing the cybersecurity of tangible products.[4]

Choosing to rely on existing legislation is not an adequate response to the current cybersecurity landscape. The EU faces many advanced cyber threats and its existing regulatory framework leaves significant gaps in coverage, such as with regard to certain types of hardware and non-embedded software. Existing regulations will not adequately address cybersecurity threats across all digital products and services. Further, there would be value in addressing cybersecurity at the EU level rather than by member states. Completion of the Digital Single Market also suggests that European institutions should address cybersecurity threats at the supranational level to level the main obstacles to a functioning European-wide digital market.

Supranational approaches to cybersecurity regulation exist in the radio, medical devices, and motor vehicle sectors, but it is largely up to the EU member states to determine their national cybersecurity policies. This has led to legislative fragmentation and the lack of consistent cybersecurity standards across the EU, which makes it harder for businesses to scale across the European market.[5] While maintaining the status quo would give more autonomy to the member states, it would come at the expense of the EU Digital Single Market, limiting the digital products and services available to some EU users and raising costs for EU users as companies comply with multiple legal standards.

We strongly recommend the Commission not pursue the maintenance of the status quo because it would be antithetical to the goals of the EU Digital Single Market and fail to address cybersecurity vulnerabilities.

OPTION TWO: INTRODUCE VOLUNTARY OR SOFT LAW MEASURES LIKE CERTIFICATION SCHEMES

The second option delineated for the Cyber Resilience Act initiative focuses on creating a voluntary scheme to guide member states as they work towards more robust cybersecurity schemes:

> Introducing voluntary measures – voluntary certification schemes under the Cybersecurity Act could be further developed and applied. Soft law measures such as guidelines or

[4] Directorate-General for Communications Networks, Content and Technology/Unit H2 for Cybersecurity and Digital Privacy Policy, "Call for evidence for an impact assessment: Cyber Resilience Act" (European Commission, March 17, 2022), https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13410-Cyber-resilience-act-new-cybersecurity-rules-for-digital-products-and-ancillary-services_en.

[5] Ciaran Martin, "Cyber Security and European Strategic Autonomy: Coherence and Capability Challenges" (Dublin: Institute of International and European Affairs, May 2022), https://www.iiea.com/publications/cyber-security-and-european-stragetic-autonomy-coherence-and-capability-challenges.

recommendations could also be considered, in particular on the cybersecurity of non-embedded software.[6]

Choosing voluntary certification schemes and soft law measures is a sensible step toward improving cybersecurity but is insufficient to establish uniform cybersecurity standards and strengthen the Digital Single Market.

Certification schemes can address many of the information asymmetries the Commission has identified in the market that contribute to suboptimal cybersecurity, such as a lack of information available to consumers to compare the security of digital products or services and insufficient economic incentives for many companies to invest in cybersecurity.

When used to augment or support domestic legislation, guidelines or recommendations can be quite helpful in ensuring market uniformity. For example, the International Organisation for Standardisation creates labelling and technical standards that are used globally, like the uniformity of the QR code.[7] Governments have even started to look to e-labelling—the display of regulatory compliance and product information electronically—to convey cybersecurity information to users of connected products, devices, and services. These e-labels provide consumers more information before making a purchasing decision, foster trust in devices that have been certified, and can empower cybersecurity-based competition in the marketplace.[8]

The Commission can use voluntary soft law measures to guide member states towards more robust cybersecurity measures and provide a recommended roadmap. These measures can draw on best practices from member states with solid cybersecurity capabilities like Estonia, Spain, and France, which rank in the top 10 of the Global Cybersecurity Index.[9] But because they are not legally building, voluntary soft law measures cannot harmonize regulations across member states or mandate vendors' compliance.[10] Not all hardware manufacturers, software developers, distributors, and importers will likely adhere to the prescribed guidelines without complementary hard law measures.

---

[6] Directorate-General for Communications Networks, Content and Technology, "Call for evidence for an impact assessment: Cyber Resilience Act."

[7] International Organisation For Standardisation, "ISO/IEC 18004:2015 Information technology — Automatic identification and data capture techniques — QR Code bar code symbology specification," February 2022, https://www.iso.org/standard/62021.html.

[8] Nigel Cory, "How E-labels Can Support Trade and Innovation in ICT, Medical, and Other Products" (ITIF, October 2021), https://itif.org/publications/2021/10/27/how-e-labels-can-support-trade-and-innovation-ict-medical-and-other-products.

[9] International Telecommunication Union, "Global Cybersecurity Index 2020" (Geneva: United Nations, 2022), https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E.

[10] European Center For Constitutional And Human Rights, "Hard law/soft law," accessed May 17, 2022, https://www.ecchr.eu/en/glossary/hard-law-soft-law/.

We recommend using soft law measures to help EU firms improve their cybersecurity practices, respond quickly to new risks, and provide strategic direction to EU member states to potentially mitigate legislative fragmentation. But we recommend the Commission only pursue this option if it complements the use of voluntary certification schemes and other soft law measures with further guidance on supranational legislation.

OPTION THREE: USE 'AD HOC' REGULATORY INTERVENTIONS

The midway option in the Commission's spectrum of policy options for the Cyber Resilience Act focuses on only regulating when needed to tackle cybersecurity threats:

> 'Ad hoc' regulatory interventions for cybersecurity of digital products and ancillary services – the intervention would be limited to adding and/or amending the cybersecurity requirements in the already existing legislation and regulating new risks as they emerge, including potentially on non-embedded software.[11]

Applying regulatory interventions on an as-needed basis for cybersecurity offers policymakers the greatest degree of flexibility to address different risks in different sectors. As-needed and sector-specific intervention could allow regulators, for example, to concentrate attention on industries like financial services and health services, which need to protect more sensitive personally identifiable information, and require some sectors to comply with more robust cybersecurity standards. Focusing on critical sectors also pushes the Commission to provide member states with unified cybersecurity standards industry by industry. Clear, sector-specific standards will mitigate the legislative fragmentation caused by the lack of cohesion between member states while still providing member states with the room to regulate industries the EU does not. Additionally, legally-binding rules on cybersecurity should be at the EU level as the Digital Services Act package—the Digital Services Act and the Digital Markets Act—are about to heavily regulate the Digital Single Market and already integrate cybersecurity concerns into the proposal. [12] Regulating cybersecurity at the EU level ensures that cybesecurity will be properly integrated into the regulation of the Digital Single Market and will not unduly be given more weight than other legal requirements.

The success of this option would depend on how responsive policymakers are to new risks and the effectiveness of future interventions. If cybersecurity standards become too fast of a moving target,

[11] Directorate-General for Communications Networks, Content and Technology, "Call for evidence for an impact assessment: Cyber Resilience Act."
[12] European Parliament and European Council, "Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on contestable and fair markets in the digital sector (Digital Markets Act) (Text with EEA relevance) 2020/0374(COD) (Leaked)," April 8th, 2022, https://antitrustlair.files.wordpress.com/2022/04/dma-4-column-leaked-text.pdf.

this approach may introduce regulatory uncertainty and discourage investment in digital products and services for the European market. On the other hand, if these standards move too slowly, they could leave EU users open to known vulnerabilities. Likewise, if 'ad hoc' interventions only respond to immediate needs, legislation may overlook new vulnerabilities tied to changes in hardware and software or new risks related to a changing threat environment. Waiting to legislate supranationally would also let member states continue to regulate industries as they wish and perpetuate an overly burdensome and fragmented regime for vendors and businesses to navigate. Given the EU created the General Data Protection Regulation to harmonize data protection laws across the member states, it would seem odd then to allow legislative fragmentation to fester in the cybersecurity space.[13]

We recommend using 'ad hoc' interventions to address specific sectoral risks and update existing EU sectoral legislation in response to compelling evidence of shortcomings. Targeted interventions can maintain harmonized cybersecurity standards in the EU and mitigate legislative fragmentation caused by the member states. Targeted interventions can also avoid imposing unnecessarily burdensome cybersecurity standards on low-risk digital products and services. We do not recommend 'ad hoc' interventions to address cross-industry cybersecurity risks, given the complexity involved and the potential for poorly timed interventions.

OPTION FOUR: COMBINE MANDATORY AND SOFT RULES

One option proposed by the Commission uses soft law rules to complement mandatory hard law forms of rule-setting and compliance:

> A mixed approach including mandatory and soft rules. This would entail:
>
> > (i). A horizontal regulatory intervention introducing cybersecurity requirements for a broad scope of tangible digital products and ancillary services.
> >
> > Different sub-options may be considered with regard to the conformity assessment procedure:
> >
> > - conformity self-assessment by default, where vendors may opt for a third-party conformity assessment when deemed appropriate; or

[13] Daniel Castro, Luke Dascoli, Gillian Diebold, "The Looming Cost of a Patchwork of State Privacy Laws" (ITIF, February 2022), https://itif.org/publications/2022/01/24/looming-cost-patchwork-state-privacy-laws.

- a third-party conformity assessment is prescribed for certain categories of products under a risk-based approach taking account of such factors as intended use, functionality or the nature of potential harm.

(ii). In addition, a staggered approach would be considered as regards cybersecurity of non-embedded software, with soft law measures such as guidelines or recommendations as a first step, potentially followed by regulatory intervention, depending on the results of implementing such measures.[14]

Option Four understands the advantages of using soft law in conjunction with hard law. It takes advantage of the greater flexibility of soft law to handle future uncertainty and the evolving nature of cybersecurity threats.[15] Further, it provides the credibility of binding supranational standards to solve cybersecurity problems and enforce healthy compliance.

Nonbinding soft law is a way to both guide institutions to hard law solutions and clarify current binding legislation.[16] In the case of the Cyber Resilience Act, nonbinding soft law could mean using guidelines and recommendations to begin a more extensive discussion of where the EU needs bolstered cybersecurity standards. In conjunction with regulatory intervention, standard-setting recommendations created through soft law can ensure that any legislation is flexible, can evolve with technological advancement, and can be narrowed for specific industry needs.

Unfortunately, Option Four proposes a horizontal approach that will create requirements for a broad scope of digital products. Using expansive definitions or overbroad horizontal frameworks can burden nascent industries or industries whose digital products might not need such stringent measures. Further, a broad horizontal framework is likely to burden businesses with large implementation and compliance costs that might not be necessary from a cybersecurity perspective. In fact, the EU has already seen the negative impact of overbroad horizontal legislation as a result of the General Data Protection Regulation, and it is likely to see the same if it enacts the Artificial Intelligence Act.[17]

---

[14] Directorate-General for Communications Networks, Content and Technology, "Call for evidence for an impact assessment: Cyber Resilience Act."

[15] Gregory C. Shaffer and Mark A. Pollack, "Hard vs. Soft Law: Alternatives, Complements, and Antagonists in International Governance" (Minnesota Law Review, 2010), https://www.minnesotalawreview.org/wp-content/uploads/2011/08/ShafferPollack_MLR.pdf.

[16] Gregory C. Shaffer and Mark A. Pollack, "Hard vs. Soft Law."

[17] Benjamin Mueller, "How Much Will the Artificial Intelligence Act Cost Europe?" (Center for Data Innovation, July 2021), https://www2.datainnovation.org/2021-aia-costs.pdf.

We recommend using soft law options, such as certification schemes and guidelines, in combination with limited hard law rules, such as transparency requirements, because this hybrid approach ensures that the Cyber Resilience Act is flexible enough to respond to future cybersecurity threats. However, we caution against overly broad or sweeping horizontal legislation that can burden low-risk digital products and services with unnecessary cybersecurity regulatory obligations. Instead, a combination of soft law and hard law that acknowledges sectoral differences in cybersecurity needs can minimize compliance costs and effectively tackle cybersecurity risks.

OPTION 5: INTRODUCE HORIZONTAL REGULATORY INTERVENTION OVER A BROAD SCOPE OF DIGITAL PRODUCTS

The final option proposed in the Commission's call for evidence regarding the Cyber Resilience Act discusses the exclusive use of broad horizontal legislation:

> A horizontal regulatory intervention introducing cybersecurity requirements for a broad scope of tangible and non-tangible digital products and ancillary associated services, including non-embedded software. Alternative sub-options could be considered regarding the categories of software to be covered, either only critical software or all software, and regarding the conformity assessment procedure, as in option 4 (i).[18]

We do not recommend the Commission use only horizontal regulatory intervention for a broad scope of digital products. As discussed in the previous section, such overbroad horizontal legislation will inflate compliance costs, make it harder for the legislative framework to evolve with cybercrime, and not consider sectoral cybersecurity needs and differences.

[18] Directorate-General for Communications Networks, Content and Technology, "Call for evidence for an impact assessment: Cyber Resilience Act."