Non-paper on the principles of a Cyber Resilience Act
Governments of Denmark, Germany and the Netherlands

Introduction

It is of the utmost importance that the digital products, processes and services which we use in our economy and society can be trusted to be digitally secure. Currently, users of the digital products, processes and services bear most of the responsibility for securing their digital activities. Market incentives are lacking for the manufacturers and providers to make their digital products, processes and services more secure and inform users about cybersecurity. To be most effective, we need a European and holistic approach, with a mix of policy tools across various areas of European legislation. Therefore, we welcome the upcoming Cyber Resilience Act (CRA) to establish and harmonise cybersecurity requirements for digital products, processes and services in the EU. The CRA should aim to raise the baseline of cybersecurity for all digital products, processes and services.

By means of this non-paper, we intend to contribute to the upcoming act, outlining the necessary steps to ensure a safe and secure European Digital Single Market. And to let the EU play a leading role globally, by setting common standards through European legislation, including through the CRA. This will contribute to the security and resilience of the EU.

Main goals of the Cyber Resilience Act

We believe the Cyber Resilience Act should:

1. Be an essential building block in a European and holistic approach to the cybersecurity of digital products, processes and services in which a mandatory horizontal approach can be complemented by sectoral regulation in specialized domains.

2. Propose security requirements for digital products, processes and services, which should
   - cover all forms of digital products, processes and services including stand-alone software, apps and software as a service ("SaaS");
     - irrespective if they are offered for consumer or business/industrial purposes;
     - irrespective if they are linked to a tangible product.
   - cover the entire lifecycle of digital products, processes and services;
   - target all manufacturers and suppliers of digital products, processes and services in the supply chain;
   - include product requirements as well as vendor requirements.

3. Align the methods of conformity assessment with the methods of conformity assessment in the Cybersecurity Act. In general, the choice for the method of conformity assessment should be left to manufacturers and providers. In addition, the CRA should designate a limited list of digital products, processes and services for which conformity assessment by a certified body is required.

4. Inform users about the cybersecurity of the products and services they buy.

---

1. The CRA is an essential building block in a European and holistic approach, with mandatory horizontal requirements, to be complemented by sectoral regulation in specialized domains

The EU has already established legislation to raise cybersecurity throughout the Single Market.[1] However, as the preliminary study of the Commission demonstrates: we currently have a legislative gap with regard to cybersecurity requirements for digital products.[2] Fragmented

[1] This legislation includes the Cyber Security Act, the Radio Equipment Directive, the Directive on Security of Network and Information Systems, the General Safety Regulation, as well as the Machinery Directive and General Product Safety Directive.
[2] Study on the need of cybersecurity requirements for ICT products | Shaping Europe's digital future (europa.eu) .

regulation and standards on cybersecurity could lead to a weakened competitiveness of EU businesses and to less security for consumers and business users.

We envision the CRA to serve as a horizontal regulation containing mandatory horizontal cybersecurity requirements for manufacturers and suppliers of digital products, processes and services. The CRA should ensure an adequate baseline of cybersecurity for all digital products, processes and services. Additional cybersecurity requirements can be set for specific digital products, processes and services (e.g. in sector-specific legislation). We envision that all digital products, processes and services should fulfill the cybersecurity requirements of the CRA, and only when (sector-)specific legislation entails a higher security level, this legislation can serve as a lex specialis (for example in the automotive sector). Ideally, the sector-specific legislation would build on the system of the CRA, setting the specific cybersecurity requirements taking into account sectoral needs and characteristics, on top of the CRA requirements. The CRA should also serve as a bridge between different cybersecurity (related) legislation, ensuring consistency and coherence by harmonizing terminology and processes.

As such, the CRA has the potential to have a comparable function as the General Product Safety Directive in the New Legislative Framework (NLF).[3] Using the NLF and thereby well-known methods for new product rules is a cornerstone to make it easier to run a business in the EU. It is therefore our opinion that the NLF approach should be used in the CRA, with the minimum cybersecurity requirements and the NLF principles and processes serving as the basis for any (future) cybersecurity regulation.

2. The CRA should propose cybersecurity requirements for all forms of digital products, processes and services, covering the entire lifecycle and targeting the manufacturers and suppliers, building on international standards

Broad scope: all digital products, processes and services

We call for a broad scope of the CRA: the CRA must include all digital products, processes and services, including stand-alone software, apps and software as a service ("SaaS").

Firstly, it makes sense to align the scope of the CRA to the scope of the CSA. The CSA covers ICT products, processes and services[4]. It would be a missed opportunity for the CRA to only focus on ICT products and their associated services. Aligning the scope of the CRA to the CSA would also contribute to the coherence of European legislative frameworks related to cybersecurity and emphasize the horizontal character of de CRA.

Many digital products depend on, and interlink with, a wide array of other digital products, processes and services, even when this is not immediately visible. With continued digitization, this will only increase. The distinction between different digital services such as SaaS, apps, software and cloud services is not always clear. Considering that the CRA is intended as horizontal legislation, it is therefore impracticable and undesirable, to apply to only a part of these digital services. Moreover, the cybersecurity of these digital services is very important and the impact of unsafe services is potentially very high.

Furthermore, we would like to emphasize the importance of also including stand-alone software in the scope of the CRA. As there are tens of thousands of software vulnerabilities each year, and market incentives to apply adequate cyber security are lacking.[5]

Entire lifecycle

The requirements should apply from the design phase, when a product is put on the market, while it is used during its expected (economic) life span, up to and including its decommission and disposal. In this context, the end-of-life gap is a specific policy challenge, when end-users continue

[3] The New Legislative Framework is a toolbox of measures that improves market surveillance and enhances the quality of conformity assessment via product legislation. Information available at : https://ec.europa.eu/growth/single-market/goods/new-legislative-framework_en.
[4] Article 2 of the CSA provides a definition of 'ICT product', 'ICT service' and 'ICT process'.
[5] Dutch Continuity Board.

to use digital products, services and processes while supply-side actors cease to provide, cybersecurity by design and cybersecurity updates, making products less secure.

Apply to manufacturers and suppliers, including each actor in the supply chain

The CRA should impose a cybersecurity duty of care on the manufacturers and suppliers of digital products, processes and services. Cybersecurity requirements that target manufacturers and suppliers are a necessary addition as they are not targeted in other legislative initiatives. For instance, the NIS2 Directive targets the cybersecurity business continuity of essential services. However, the cybersecurity of the digital products, processes and services that their ICT suppliers provide are often not (or indirectly) regulated. This is a gap, as the operator and the integrity of the products, processes and services the entity delivers to its end-customers are also dependent on (the quality of the products, processes and services of) the ICT suppliers. Furthermore, consumers and companies (big and small) are all dependent on the cybersecurity that ICT manufacturers and suppliers provide in their products, processes and services.

We would like to highlight that each actor in the supply chain should have a responsibility in making sure their digital products, processes and services are as cybersecure as possible. Digital products, processes and services are often composed of several components and make use of other services. This means that several hardware manufacturers and software developers are involved in one digital product, process or service. As the NLF takes all economic operators into account we suggest to rely on the distribution of roles and responsibilities to the extent possible. Adjustments are, however, needed in order to cover the entire product life cycle.

We understand that the proposed essential requirements might require substantial changes of for example SMEs. However, small manufacturers do not necessarily make products with a lower impact or risk. We therefore argue that the cybersecurity requirements should be defined independent of the size of the manufacturer or supplier. That being said, the CRA requirements should be predictable and proportionate to avoid discouraging innovation or driving SMEs out of the market.

Cybersecurity requirements, building on international standards

CEPS and the European Commission have presented their early thinking on the possible essential requirements of the CRA.[6] We are pleased to see that not only product requirements are considered, but also vendor requirements relating to the organization. We agree that both these types of requirements are necessary to improve the level of cybersecurity throughout the European market. We especially welcome requirements that ensure life cycle management, responsible disclosure, and transparency in the supply chain[7].

European companies are competing in a global market where global standardisation organisations are developing global standards. It is essential that the European cybersecurity standards that will be developed under the CRA through the NLF procedure are aligned with and build upon international standards wherever possible, and that the actors in the European standardisation system actively seek to influence the global standardisation initiatives to reflect European values particularly regarding cybersecurity.

3. Multiple levels of cybersecurity

The European Commission considers the possibility of subjecting digital products, processes and services with a higher risk to a stricter process of demonstrating conformity with the cybersecurity requirements, which we support. We support a common set of essential requirements, but the assessment may differ (self-assessment or third party assessment in line with the CSA). Building on the same methods of conformity assessment used in the CSA would contribute to the coherence

[6] Public Consultation Cyber Resilience Act and Study supporting the Commission preparatory work for the Cyber Resilience Act by CEPS.
[7] i.e. "Define lifecycle duties and responsibilities for all stakeholders and ensure they are observed on the vendor side", "Manage third party components and guarantee the level of security of the supply chain" and "Define a vulnerability management process and deliver regular security".

of the framework. At the same time, it is important to make sure the requirements fit the risk potential and possible use-cases.

The main emphasis of the CRA should be on setting a shared baseline for *all* digital products, processes and services. This basic level should be setting the standard in terms of essential requirements, allowing conformity to be demonstrated with self-assessment. Self-assessment is an efficient and effective method to demonstrate conformity on a basic level. In addition to self-assessment, the CRA should facilitate and in some cases require conformity to be demonstrated with mandatory (periodic) third party assessment in accordance with the CSA. In general, the CSA EU Statement of conformity or certificate under the CSA should serve as a possible presumption of conformity. This would imply that the CSA certificates cover the essential requirements under the CRA.

We propose that in general the manufacturer or supplier should be able to choose the level and respective label for their digital products, processes and services. The label would enable users to decide what level of cybersecurity they need for the way they intend to use the digital product, process or service. In this, the users of ICT-products, software and services should select adequate products. In addition, the CRA should designate limited categories of digital products, processes and services for which a third party assessment is required. We propose an updatable annex to the CRA with a list of product categories that would require a third party assessment. This list could be an output of a well-informed discussion on risk implications.. Considering that the actual risks are often determined by the way they are used, this risk based approach should take into account the intended use. The list should be limited, and it should be considered whether sectoral legislation would be more appropriate. The list could for example include components dedicated to provide, support or enhance cybersecurity. The criteria for updating this list should be clear and transparent.

4. Consumer information and market surveillance

We propose that the products, processes and services falling under the scope of the CRA should bear a cybersecurity label that is easily understandable by users so that they can make an informed choice when acquiring them. Unfortunately, security is not static. Even a product that was certified can become suddenly insecure. Therefore, the label should provide (a link) to the product security status, providing information about known vulnerabilities and mitigations (e.g. updates), without laying the responsibility for the cybersecurity of the product on the user.

Especially when relying on self assessment, attention must be paid to effective market surveillance by a competent authority with the necessary expertise in the field of cybersecurity. It is very important to make sure that products placed on the European market indeed comply with the prescribed CRA essential cybersecurity requirements. (Periodic) third party assessments could also be helpful in ensuring conformity. This way, the NLF label will assure users that the labeled products, processes and services they acquire are indeed cybersecure.