REACTION TO PUBLIC CONSULTATION CYBER RESILIENCE ACT
The Government of the Netherlands, 25 May 2022

Introduction

The government of the Netherlands is pleased to have the opportunity to respond to the consultation regarding the Cyber Resilience Act.

Firstly, we would like to refer to our non-paper on this matter, in which the Netherlands calls for the Cyber Resilience Act to create horizontal obligations, setting cybersecurity requirements for the manufacturers and providers of all forms of digital products, processes and services, throughout the entire life cycle of these products.[1]

In this reaction, we would like to build on this non-paper, and focus on several aspects of the Cyber Resilience Act.

Summary

- The CRA should have a broad scope and cover all digital products, processes and services;
- The CRA should be a horizontal regulation, with mandatory horizontal requirements;
- The CRA should include multiple levels of cybersecurity labels, with a basic label setting the standard with essential requirements and self-assessment, and a higher label entailing stricter requirements and third party conformity assessment.
- In general, the choice between a basic label and a higher label should be left to manufacturers and providers, with the possibility for the legislator to require a higher level cybersecurity label for certain categories of digital products, services and processes;
- The cybersecurity requirements should include product requirements as well as vendor requirements and should cover the entire lifecycle of digital products;
- The whole supply chain should be targeted: hardware manufacturers and software developers should have a duty of care for their own component, as well as the components of others they use in the digital product, process or service they provide or supply. Our proposed broad scope of the CRA will achieve inclusion of all possible market players.

Broad scope: all digital products, processes and services

The Netherlands calls 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”).

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. And in the future, 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 services.

Moreover, the cybersecurity of these digital services is very important and the impact of unsafe services is potentially very high. For example: SaaS applications are frequently used to control powerful energy devices. Many SaaS platforms have been integrated into directly switchable equipment on the electricity grid. Large-scale control of SaaS environments that are connected to charging stations or heat pumps or other devices, poses a significant risk to European grid stability. We therefore see these SaaS environments as a high-risk service, for which there currently is no legislation in place to ensure their cybersecurity.

Furthermore, we would like to emphasize the importance of also including stand-alone software in the scope of the CRA. The report of the Dutch Safety Board into the software vulnerabilities in Citrix and other software products and services has shown that not only are there tens of thousands of software vulnerabilities each year, it also showed that in an international competitive market without cybersecurity legislative requirements it is economically unviable for all software developers and suppliers to apply security by design and in the entire product life cycle. This also includes software developers and suppliers that are not cloud service providers. The CRA offers an opportunity to create the necessary legal cybersecurity requirements for these largely unregulated products and services and ensuring a level playing field in the EU.

[1] Non-paper on the principles of a Cyber Resilience Act | Tweede Kamer der Staten-Generaal

In addition, it makes sense to align the scope of the CRA to the scope of the Cybersecurity Act (CSA). The CSA covers ICT products, processes and services. It would be a missed opportunity for the CRA to only focus on digital 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.

Horizontal regulation: mandatory horizontal requirements, to be complemented by sectoral regulation in specialized domains

The Netherlands envisions the CRA as a horizontal regulation, with mandatory horizontal requirements. These mandatory horizontal requirements may be complemented by sectoral legislation in specialized domains that prescribe a higher level of cybersecurity.

The CRA should fill the current legislative gap with regard to cybersecurity requirements for ICT products, as identified in the Study on the need of Cybersecurity requirements for ICT products (December 2021).[2]

We envision the interaction between the horizontal CRA, and other (sector specific) legislation as follows. The CRA should ensure a certain level of cybersecurity for all digital products, processes and services. Additional (e.g. sector specific) cybersecurity requirements can be set for specific digital products, processes and services. We envision that all digital products, processes and services should fulfill the cybersecurity requirements of the CRA, and only when 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.

Conformity assessment: multiple levels of cybersecurity

Hardware manufacturers and software developers will need to demonstrate their compliance with cybersecurity requirements set in the CRA. The European Commission considers adopting the approach that is also applied in the New Legislative Framework (NLF).[3] It also considers the possibility of subjecting digital products and services with a higher risk to a stricter process of demonstrating conformity with the cybersecurity requirements.

The Netherlands considers that the NLF approach is traditionally used for safety requirements that are assessed when products are placed on the market. However, attention must be paid to how to make sure that the digital products, processes and services remain cybersecure during the entire life cycle. In addition, consideration should be paid how to specifically fit in cybersecurity (instead of safety) requirements, and the fact that digital products, processes and services as well as cybersecurity requirements evolve over time. The Netherlands also argues that it is very important to make sure that products placed on the European market indeed comply with the prescribed CRA essential cybersecurity requirements. Therefore, the CRA should include effective market surveillance in each member state. (Periodic) third party assessments could also be helpful in ensuring conformity. This way, the NLF label will ensure users that their product is indeed cybersecure.

The Netherlands supports the view of the Commission that the NLF framework provides a good starting point for the CRA. We understand that stakeholders/businesses are hesitant to focus on a risk based approach. They argue that this is very difficult to implement, and that the actual risks are often associated with the use of certain products. For example, a sensor being used in a nuclear plant or in a swimming pool. The Netherlands suggests that the CRA builds a framework for at least two levels of cybersecurity, with respective labels. It would be worth considering the three levels and labels used in the CSA: if fitting and usable for the CRA, it would contribute to the coherence of the framework if the CRA would use the same levelling and labeling. The basic level should be setting the standard in terms of essential requirements, and conformity may be demonstrated with self-assessment. A higher level should entail stricter requirements, and conformity should be demonstrated with (periodic) third party assessment. In most cases, the choice could be left to the manufacturer or provider to place their digital products, processes and services on the market with either a basic CRA-label or a high CRA-label. In these cases 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 addition, the CRA should also make it possible to designate (on a European or national level) categories of digital products, processes and services for which, based for example on risks for essential services and

[2] Study on the need of cybersecurity requirements for ICT products | Shaping Europe's digital future (europa.eu).
[3] 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.

processes (comparable to categories defined in NIS2) or high impact (e.g. number of users), a high label is required.

As the Netherlands advocates a broad scope of the CRA, for many digital products, processes and services conformity to the cybersecurity requirements will need to be demonstrated. 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 third party assessment. In this regard, we should also take into account the certification under the CSA as a possible proof of conformity. The Netherlands argues that market players could benefit from the possibility to use the CSA EU Statement of conformity or certificate under the CSA as compliance tool for the CRA. This would imply that the CSA certificates should cover at least the essential requirements under the CRA. Additional to the CRA requirements, the CSA schemes could prescribe more elaborate cybersecurity requirements.

We understand that these conformity procedures have a large impact and might require substantial changes of manufacturers and providers, especially SME's. However, we argue that it is crucial to raise cybersecurity for all digital products, processes and services because they are the backbone of the digital transformation. Including the possibility of self-assessment should make it more proportionate to comply with the requirements. In addition, it might be possible to take the size of the company (in terms of revenue) into account when setting the fees for the third party conformity assessment.

Cybersecurity requirements

CEPS and the European Commission have presented their early thinking on the possible essential requirements of the CRA.[4] 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, such as "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".

We would like to highlight that each actor in the supply chain should have a responsibility in making sure their products 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. Our proposed broad scope of the CRA will achieve inclusion of all possible market players. The Netherlands argues that all these hardware manufacturers and software developers should have a duty of care for not only their own component, but also the components of others that they use in the product they supply and process and service they provide. The manufacturer of a product would be responsible for testing the integration of components (both functional and regarding the security) in the end product. This requires, for example, software suppliers to create insight in the components that make up the software they provide. The concept of assurance in accordance with the International Standard on Assurance Engagements (ISAE assurance standard) could be helpful in addressing the supply chain issue, especially for services, in a proportionate way. This concept allows manufacturers to rely on the certificates or other means of demonstrating conformity of their suppliers. More specifically, it should be possible to rely on assurance reports in conformity assessments.

In the case of software, transparency on used software components can play an important role in securing the supply chain. This is often referred to as a Software Bill of Materials. Furthermore, special attention should be given to the role of open source components and how the cybersecurity of those components, that are often reused in many other products, can be assured in a cost-effective way and benefit the whole open source software ecosystem. For tangible products, the concept of a Components Bill of Materials could be applied.

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.

[4] Public Consultation Cyber Resilience Act and Study supporting the Commission preparatory work for the Cyber Resilience Act by CEPS.