**Non-paper on the principles of a Cyber Resilience Act**

## Introduction

In her State of the Union speech of 2021, Commission President Ursula von der Leyen announced the need for a European Cyber Resilience Act to set common standards to improve the cybersecurity for products in the European internal market: *"If everything is connected, everything can be hacked. Given that resources are scarce, we have to bundle our forces. And we should not just be satisfied to address the cyber threat, we should also strive to become a leader in cybersecurity. This is why we need a European Cyber Defence Policy, including legislation setting common standards under a new European Cyber Resilience Act."*

The Netherlands couldn't agree more. 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 of ICT products, processes and services. To be most effective, we need a European and holistic approach, with a mix of policy tools across various areas of European legislation.

Therefore, the Netherlands welcomes the upcoming Cyber Resilience Act as a key horizontal layer to regulate the cybersecurity of the products, processes and services that we use. It provides the opportunity to take additional measures to ensure that digital products, processes and services can be trusted on all relevant aspects of cybersecurity (confidentiality, integrity and availability), including specifying the necessary conditions for the placement on the market[1], alongside existing or upcoming legislation such as Radio Equipment Directive (RED), General Product Safety Regulation, Machinery Directive, Cyber Security Act (CSA), and Network and Information Systems Directive 2 (NIS2D) and sectoral legislation like automotive.

By means of this non-paper, the Netherlands intends to contribute to a broad policy discussion on cybersecurity in general and the Cyber Resilience Act in particular, outlining the necessary steps to ensure a safe and secure European Digital Single Market. Moreover, there is true potential for the EU to play a leading role globally, by setting common standards through European legislation, including through the Cyber Resilience Act.

## Main goals of the Cyber Resilience Act

The Netherlands believes the Cyber Resilience Act should:

1. Be an essential building block in a European and holistic approach to the cybersecurity of digital products and services in which a mandatory horizontal approach is complementary to sectoral regulation in specialized domains.
2. Propose security requirements for digital products and services, which should
    - cover all forms of digital products, services and processes;
        - 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 and services;
    - target the manufacturers and providers of ICT products, processes and services.

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

Our societies are highly digitized and connected. Mainstreaming cybersecurity across the board in the EU is crucial. We need a comprehensive holistic that addresses all levels within all policy domains. It is therefore essential to take adequate legislative measures at the EU level to create a safe

[1] PCouncil conclusions of the Telecom Council of December 2020 on cybersecurity of connects products.

European Digital Single Market so we can all trust future digital developments and reap the societal and economic benefits they bring.

With the work already done by establishing the voluntary Cyber Security Act and the mandatory Radio Equipment Directive, new cybersecurity requirements have been set with regard to ICT products, processes and services. Other relevant legislation includes the revision of the Directive on Security of Network and Information Systems, the General Safety Regulation to implement UN measures with regards to automotive security, as well as the Machinery Directive and General Product Safety Directive.

The Netherlands welcomes these steps to strengthen the cybersecurity of the EU. However, an important piece of the puzzle for a holistic and comprehensive approach to cybersecurity is still missing with regard to the cybersecurity of digital products, processes and services since many initiatives take a sectoral approach or do not cover the entire digital domain.[2] The Cyber Resilience Act can fill these gaps and complement existing EU cybersecurity efforts. The Cyber Resilience Act should be an essential building block in a European and holistic approach to the cybersecurity of digital products and services in which a mandatory horizontal approach is complementary to sectoral regulation in specialized domains.

**Example of the need for a mandatory horizontal approach:**

While the RED delegated act is key to set mandatory security requirements in the short term for wirelessly connect devices (including many IoT devices), it only addresses wireless products when they enter the market and cannot encompass the broader scope of ICT products, processes and services. Also, at the time the RED was not created with cybersecurity in mind. The CSA on the other hand offers the benefits of a broader scope for ICT products, processes and services, but is a voluntary system. From this perspective, horizontal legislation can contribute to a desired horizontal and mandatory level of security and ensure consistency and legal certainty for both manufacturers and consumers (citizens and businesses).

The Netherlands envisions the Cyber Resilience Act to serve as a horizontal regulation containing harmonised cybersecurity requirements for manufacturers and suppliers of ICT products, processes and services. A lex specialis provision can ensure the necessary interplay with sectoral legislation in specialized domains. As such, the Cyber Resilience Act has the potential to have a comparable function as the General Product Safety Directive in the New Legislative Framework. In order to avoid overlap and unnecessary administrative burden for market players as well as regulatory authorities, careful consideration should be given to existing legislation and proposed and ongoing legislative initiatives. Targeted (sectoral) regulation should principally be the starting point in terms of public policy based on specific sectoral needs. As mentioned above, there are currently already EU initiatives underway to implement or review such targeted legislation. At the same time, sectoral legislation cannot encompass societal need to set cybersecurity requirements for the entire ICT industry. The CRA offers the opportunity to make explicit what gaps are already being addressed and for which reasons, and to determine how a horizontal approach in the form of a Cyber Resilience Act would add to existing or upcoming legislation.

## 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 providers of ICT products, processes and services

The focus of the Cyber Resilience Act should be on setting mandatory requirements for manufacturers and providers of ICT products, processes and services. As such, horizontal regulation can contribute to a state-of-the-art cybersecurity framework and ensure consistency and legal certainty for both manufacturers and customers.

The Netherlands would like to underline that the Cyber Resilience Act should:

- cover not only digital products, but also digital processes and services. In the current state of technological and market dynamics, digital products, processes and services are interlinked and almost inseparable. In the future, this will likely continue.

[2] Draft text revised GPSD (europa.eu)

- cover all forms of ICT products, processes and services, irrespective whether they are offered for consumer or business/industrial purposes. In this way, the Cyber Resilience Act can effectively complement sectoral regulation.
- cover ICT products, processes and services, irrespective whether or not they are linked to a physical product. In this way, software products, processes and services are included and horizontal cybersecurity requirements will apply. This is necessary, as society is increasingly dependent on a wide range of software products, processes and services.
- cover the entire lifecycle, i.e. from the design phase, before a product comes 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 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 of ICT products, processes and services. This is a necessary addition to other legislative initiatives. For instance, the NIS2D targets the cybersecurity business continuity of essential services. However, the cybersecurity of the ICT products, services and processes that their ICT suppliers provide are often not (or indirectly) regulated. This is a gap, as the operator and the integrity of the products and services the entity delivers to its end-customers are also dependent on (the quality of the products and services of) the ICT suppliers. Furthermore, companies (big and small) and consumers are all dependent on the cybersecurity that ICT manufacturers and suppliers provide in their products, services and processes. There is therefore a societal need to set cybersecurity requirements for the ICT industry through legislation. The Cyber Resilience Act can realize a duty of care for the cybersecurity of ICT products, processes and services. Certification schemes under the Cyber Security Act could then be used as a mandatory harmonized standard for the specification of the duty of care based on the latest state of technology.

**To conclude**

The Cyber Resilience Act should be an essential building block in a European and holistic approach to the cybersecurity of digital products and services in which a mandatory horizontal approach is complementary to sectoral regulation in specialized domains. Specifically, the Cyber Resilience Act should function as a horizontal regulation containing a lex specialis application with regard to sectoral and harmonised rules.

The focus of the Cyber Resilience Act should be on setting cybersecurity requirements that cover all forms of both digital products and services, irrespective if they are offered for consumer or business/industrial purposes and irrespective if they are linked to a physical product. It should cover the entire lifecycle of digital products, processes and services and target the manufacturers and providers of ICT products, processes and services through a duty of care based on the latest state of technology.