Council of the European Union
General Secretariat

Brussels, 24 June 2022

WK 9175/2022 INIT

LIMITE

CYBER
TELECOM

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

WORKING DOCUMENT

From:	General Secretariat of the Council
To:	Horizontal Working Party on Cyber Issues
Subject:	Belgian non-paper on the upcoming Cyber Resilience Act (CRA)

Delegations will find attached a non-paper from the Belgian delegation on the upcoming Cyber Resilience Act.

Last updated: 21/06/2022

Belgian Non-Paper on the Cyber Resilience Act (CRA)

I. Objectives

Several studies, including the EU Commission Study on the need of cybersecurity requirements for ICT products published in December 2021[1], have identified two major gaps in terms of the cybersecurity of digital products:

- **a high level of vulnerabilities** in many connected devices from smartwatches to medical devices,
- **a low awareness of cybersecurity risks among users**, especially retail customers.

Belgium believes that the upcoming Commission Proposal for a European Cyber Resilience Act (CRA) can be a useful tool to enhance the overall level of basic cybersecurity by establishing minimum cybersecurity requirements for all digital products and services in the EU, including internet-connected devices or so-called IoT (the "Internet of Things"). These requirements should primarily focus **on informing users about the level of cybersecurity of the products and services they buy.**

We have to keep in mind however that such legislation will only make our digital environment more trustworthy and resilient if we simultaneously address cybercrime in an efficient manner. Moreover, it is worth noting that most attacked systems have security patches available which could have prevented the exploitation of vulnerabilities but which have not been installed by users.

Key benefits of the CRA would be:

- **a higher level of consumer trust and informed users,** and more generally a higher level of confidence for citizens, businesses and organisations in products and services sold in the EU thanks to better protection from cyber fraud, abuse and malfunctions,
- **reduced opportunities for malicious actors** to exploit vulnerabilities in widely used products and services,
- **establishing a level playing field** for manufacturers of digital products and providers of digital services in the internal market by fostering competition and innovation, while stimulating the digital transition.

II. Scope

In line with the Non-Papers issued by the Netherlands in December 2021 and by Germany (BSI - Bundesamt für Sicherheit in der Informationstechnik) in March 2022, Belgium supports a **horizontal scope** for the CRA. In terms of products and services, basic cybersecurity requirements should not only cover "connected devices" but also **all digital products and services[2],** whether for individual, professional or industrial use. In other words, the CRA should not restrict itself to consumer products and services, but should also include business-to-business (B2B) goods and services, as well as public services.

[1] See https://ec.europa.eu/newsroom/dae/redirection/document/82006

[2] We note that the European Commission Public consultation on the Cyber Resilience Act published on 16 March 2022 uses the term « digital products » instead of « ICT products ». We assume this is meant to ensure a broad scope – an approach we support.

A **clear definition of what constitutes a digital "product" or "service" will be needed to ensure consistency with existing EU legislation** (e.g. the e-Commerce Directive, the DSA[3], the CSA[4], NIS[5], etc.) and in national implementation. The situation of **products containing both hardware and software elements, as well as that of products containing service elements,** will also have to be taken into account.

The CRA should establish a limited number of basic requirements on which various specific regulatory requirements can build. Unlike the NIS Directive or existing sectoral legislation, however, the CRA would apply to non-critical, essential or important sectors, and include all products or services. Moreover, the CRA will focus on the products and services themselves rather than only the networks of the service providers or of the product manufacturers, as NIS does. It is nonetheless crucial to clearly define how the CRA will relate to NIS-2 obligations to ensure consistency, especially since many digital service providers will have to abide by both pieces of legislation.

The security level of ICT products varies a lot depending on the sector under consideration. Belgium believes that the CRA should be seen as the minimum baseline for products and services across all sectors. Having a "default regime" means that the CRA requirements may be completed by additional requirements in specific sectors. For instance, as regards the need for regular software updates to ensure a continuous level of cybersecurity for digital products and services, a mere reference to the legal provisions contained in the Radio Equipment Directive (RED)[6] and medical devices legislation does not appear sufficient. Indeed, the scope of the CRA should extend beyond radio-connected devices to cover all internet-connected devices, as well as digital services.

The CRA should take into account the fact that most cyberattacks occur because of unpatched systems. Users should be well informed about the following security aspects:

- Security patch regime (automated default, manual, none…),
- Security update expiration date (updates will be provided until…),
- Supported password policy (forced strong password policies of not),
- Multi Factor Authentication (MFA) support,
- Vulnerability disclosure policy provided (what is the point of contact and constraints…).

The Internet should remain an open and free cyber space where concepts like free information exchange and open source software are key drivers. In this context, users should be able to use systems and software from different sources and vendors, even beyond the security update expiration date. The CRA should ensure that users can still use their home Smart TVs, or any other digital product or service, even after the security update expiration date has been reached. We should also avoid that a point of sale ends up with a stock of devices it cannot sell because the security update expiration date is too close , or that a manufacturer or service provider is liable for a vulnerable system that was deliberately not updated by the user. **Most importantly, the CRA should take into account the importance of not undermining open source software.**

Finally, in terms of the minimum cybersecurity requirements contained in the CRA, it will be essential to **calibrate measures in a proportional way** to avoid putting SMEs (small and medium size manufacturers and service providers) at a disadvantage.

[3] Digital Services Act (Act), i.e. Proposal COM/2020/825 for a Regulation on a Single Market For Digital Services.

[4] Cyber Security Act (CSA), i.e. EU Regulation 2019/881 of 17 April 2019.

[5] EU Directive 2016/1148 of 6 July 2016 on network and information systems – currently being updated. The adoption of the new Directive (NIS-2) is expected in the fall of 2022.

[6] Directive 2014/53/EU of 16 April 2014 on the market of radio equipment.

III. Key measures

A. A new "duty to inform" for product manufacturers and service providers

The baseline cybersecurity requirements to be introduced by the CRA should apply to **all manufacturers and service providers while being predictable and proportionate to avoid discouraging innovation or driving SMEs out of the market.** Both hardware and software – which may be present within the device natively or through additional non-embedded software, as well as on backend services – should be designed, produced, configured, maintained and decommissioned with privacy and security in mind, i.e. privacy and **security by design and by default**.

Consumers and enterprises, including operators of essential services (OESs), often rely on third party manufacturers and service providers for the producing of their own products or for the provision of their own services. Currently, under legislation such as the RED, manufacturers do not indicate the way in which a product has been reviewed for security standards and do not bear any legal responsibility apart from possible contractual obligation for the cybersecurity of their products if these products are not proactively marketed in the EU.

Thanks to the CRA, responsibilities could be anchored both in terms of hardware and software, and in terms of applicable jurisdiction. We recommend that the CRA requirements should apply to products and services offered in the EU single market, including when manufacturers and service providers are established in non-EU countries, and irrespective of whether or the components of a given product or service are produced inside or outside the EU. This could enhance the resilience of the entire supply chain.

As regards the internet of things (IoT), to ensure a proportionate approach, we suggest that requirements could distinguish between IoT and IIoT (Industrial IoT, i.e. the use of IoT devices such as smart sensors to enhance manufacturing and industrial processes):

a) **For IIoT:** The guarantee of regular security updates (patching) in order to have a cyber-secure product or service should ideally be designed throughout the **entire lifecycle**. This is justified by the nature of the object/service and the high price usually associated with it. Furthermore, the economic potential of the country should be protected by ensuring that production capacities are cyber-secure.[7]
b) **For IoT** (non-IIoT): We believe that there can be no overall imposition of a minimum period for the provision of security updates and that any requirements would need to be carefully calibrated to avoid unintended effects such as penalising SMEs, open source software, and consumers (should some manufacturers and service providers decide to exit the EU market as a result). We suggest that foreseeing automatic updates by default for IoT products, without requiring a proactive action by users, is the most important step to achieve a higher level of patching.

Should any requirements be imposed on security updates, it will be very important to ensure a **proportional approach.** Most of all, i**t will be very important for the CRA to ensure that manufacturers and service providers clearly inform users about the length of the period during which security updates will be provided free of charge, and any potential change/extension thereof.** The majority of users (consumers and SMEs) are not trained in cybersecurity and may not have the necessary skills to ensure their own cybersecurity. This obligation to inform should be all the more extensive when the user is not a specialist. However, even towards a professional buyer, the manufacturer or service provider should be under an obligation to inform and advise properly. When selling IoT products or services in particular, mandatory recommendations and explanations on security should be included in the official sales contract in order to gradually increase the level of awareness of users.

[7] It is worth noting that, in theory, IPv6 provides a better way of identifying (I)IoT devices than IPv4. Imposing an EU sunset clause on IPv4 may thus need to be considered, although its feasibility in the medium term needs to be assessed.

Special attention should be given to open source software and products/services relying on open source components. We should indeed ensure that they are not put at a disadvantage by the future requirements on the minimum period for security updates, given the specific governance and financial models these solutions typically rely on.

From the viewpoint of manufacturers and service providers, the existence of common baseline requirements across EU markets would facilitate compliance and **avoid price competition to occur at the detriment of security**. To ensure consistency with the Cybersecurity Act (2019/881), the CRA could foresee **a presumption of compliance** for several requirements in case manufacturers and service providers are in possession of a **valid certification under a scheme of the CSA**. In other words, we expect that the minimum cybersecurity requirements contained in the CRA will match the criteria assessed in the context of cybersecurity certifications under the CSA. In any event, we believe that further clarifications on the interplay between the CRA and the CSA is necessary.

It would be best to ensure that there is no "levelling down", with suppliers and producers counting on the bare minimum for the cybersecurity measures in order to provide a lower price. The product or service concerned should bear **a statement that is easily readable and understandable by users** so that they can make an informed choice. In other words, manufacturers and service providers should ensure that customers are informed about the level of cybersecurity of their product or service at the point of sale, including information about how long security updates will be provided. For example, the equivalent of a food "nutriscore" or energy "performance rating" could be proposed, indicating from a scale going from A to G the **cybersecurity level** of each (I)IoT. Such a label/rating would however most likely be voluntary and its modalities would require further discussions on the criteria to be used (e.g. actual level of resilience against cyberattacks, period of guarantee for security updates, sustainability aspects etc.), and how it would be implemented.

Manufacturers and service providers should **provide security updates ("patching") with an automatic roll-out by default** in order to ensure that the product or service is up-to-date and aligned with best practices, at least for non-industrial IoT. As IT vulnerabilities are often not physically noticeable, non-specialists users tend to ignore or delay updates, the risks being unknown to them. Furthermore, recent studies suggest that manufacturers provide too little publicly available information about the security features of their devices and rarely provide cyber hygiene advice to their users after purchase.[8] For each update, information should be provided to clearly explain the new features and ensure full transparency to users. Importantly, whereas security updates should be rolled out by default, **functionality updates should always remain optional.**

Nonetheless, despite some advantages of automatic updates by default **in the B2B sphere, some exceptions will have to be foreseen** to address particular circumstances. First, it is important to acknowledge that**,** in the professional (and especially the industrial) sphere, the higher level of complexity and sophistication of IT products, services and systems means that automatic updates are more likely to generate malfunctions (e.g. due to technical incompatibilities with other programs or systems) and to cause security risks if rolled out without prior testing and validation. This is especially the case for critical systems and critical operators. In some cases, security patches may even be used by malicious actors as a vector for a cyberattack. The CRA should thus focus on imposing an automatic update obligation *by default* for (normal) IoT (i.e. "opt-out" scheme), while giving consumers and organisations the opportunity to adjust their preferences to have their updates installed manually if they so wish ("opt-in").

It is also important to take into account special cases whereby updates may need to be deployed from a central system rather than from a specific device. Sensors embedded in a device (e.g. sensors used to measure temperature in nuclear power plants) may not have sufficient processing power to allow for the

[8] See for instance Blythe, John & Sombatruang, Nissy & Johnson, Shane. (2019). What security features and crime prevention advice is communicated in consumer IoT device manuals and support pages?. *Journal of Cybersecurity*. 5. 10.1093/cybsec/tyz005.

deployment of security updates and other (peripheral) mechanisms may be required which involve the installation of software via a connected system.

Concretely, **automatic security patching** by default for normal IoT (i.e. for consumers and SMEs) would require users to be informed of upcoming updates before they are automatically installed, so that:

- they may decide to opt out (e.g. if they have a specific reason to believe the security update would have a negative impact on their use of the product or service, such as in the case of incompatibilities with other, older devices),
- they may delay the update and choose another, more appropriate moment for the installation. Delaying security updates should however be discouraged as much as possible to avoid the risks created by the many unpatched devices connected to the internet.

In other words, **there should always be an option to overrule the automatic installation of an update** and to delay updates to a later, more convenient moment. If a user opts for a delay and subsequently does not take any action to carry out the update, the installation should eventually take place at the expiration of the delay.

Finally, the CRA will need to clearly define how manufacturers and service providers are to determine the "end of support date". Belgium believes that **the "end of support date" must be clearly indicated at the moment the product or service is sold**. For high risk products/IIoT, the end-of-support date should ideally match the (published) end-of-lifetime date whenever possible.

B. Requiring Privacy & Security by design and by default for consumer products and services

The CRA presents **a unique opportunity to set a high standard of consumer and enterprise protection for digital products (including the so-called "connected devices" or IoT) and digital services**, positioning the EU as a world leader for secure products and services.

A**ll manufacturers and providers marketing products or services in the EU** should fulfil at least basic cybersecurity requirements, including:

1. Duty to inform: Provide a **security information to users** (e.g. level and method of encryption used, key security recommendations, etc.) at the point of sale, including by being transparent about the **length of time** during which security updates are provided;
2. **Foresee automatic updates by default whenever possible, at least for security patches** (as opposed to functionality enhancements) until a specified "end of support" date or end of lifecycle. This date should be communicated transparently to users. However, enterprises and consumers should be given the opportunity to switch off the automatic setting or to defer the installation of the updates to a more suitable time (as is now already done in most computer operating systems, under a kind of "opt-out" mechanism). Manufacturers and service providers should also ensure that there is the possibility of a roll-back in case of an incident during the patching operation, and explain the corresponding procedure to their users.
3. Provide assurance that each device has a **strong password policy**. Refrain from using universal default passwords and use strong default passwords when marketing a product or service, while ensuring that those passwords can be reset by the user following a strong password policy. More generally, the default ("out of the box") configuration should not be such that anyone can access the device or service (e.g. allocation of random passwords). For password resets, there should be whenever possible a secure manual procedure to avoid that users become locked out of their own device/services due to security measures. This shall not prevent the imposition by manufacturers and providers of technical requirements to avoid weak passwords (e.g. minimum number of characters and inclusion of special characters);
4. **Provide a public point of contact as part of a vulnerability disclosure policy to report vulnerabilities** and act on these in a timely manner. Users should be informed of identified security vulnerabilities within a short timeframe and should be provided with clear instructions

on how to mitigate the risk that this/these vulnerability/ties be exploited until a security patch is available. Patching should also be put at their disposal within a given timeframe which may need to be specified in the CRA, e.g. a maximum of 3 months[9];

5. **Insofar as they are not already covered by the reporting obligation under the NIS(2) Directive report** significant cyber incidents and vulnerabilities **to the competent national authorities**, in a way that is consistent with NIS practice.

Overall, the CRA should ensure that the "default" settings of products and services sold in the EU are as secure as possible to reduce vulnerabilities, without putting European manufacturers and service providers at a competitive disadvantage or restricting European customers from accessing non-EU made products and services.

Regarding the environmental impact of digital products and services (e.g. "reparability" and provision of spare parts, take-back obligation promoting recycling, etc.), we recognise that the issue needs to be addressed. Consideration will need to be given to the refurbishment sector and the way in which relevant obligations apply to these stakeholders, both for products that have already been placed on the EU market and for products being marketed in the EU for the first time (but in a refurbished manner). Since resources (rare metals used in chips, etc.) are scarce, precious IoT components should thus be recyclable as much as possible. The take-back obligation (e.g. implemented through the Recupel levy in Belgium) should be explicitly extended to IoT products and the obligation of information must be provided at the point of sale[10].

The CRA should seek to find the right balance and **avoid placing excessive burden on small and medium-sized manufacturers and service providers**, yet without compromising on the basic level of security.

IV. Integration into the EU legal framework

We think it will be important to clarify:

- how the CRA relates to the New Legislative Framework (NLF), the new Market Surveillance Regulation (EU) 2019/1020, the Cyber Security Act (CSA), the Digital Services Act (DSA), the Network and information Systems Directive (NIS), among others,
- applicable sectoral legislation that complements/supersedes the CRA,
- whether it will provide for "CE marking" or an equivalent labelling scheme. The responsibility for assessing conformity with the CRA label could be entrusted to accredited bodies at national level, preferably in line with the mechanisms foreseen under the CSA. Such assessments would mirror the way traditional security labels are currently being assessed (cf. security labels for cars, elevators, etc.). Controllers could be required to perform some specific tests (e.g. against intrusions) prior to and after the products or services are put on the market, with a subsequent review at regular intervals,
- whether a clear exception to intellectual property rights will be foreseen to authorise, at least for competent authorities, the testing and assessment of security requirements in computer programs (software and hardware) for security purposes (cf. provisions of the Software Directive[11],whether it would have to be notified as a technical barrier to trade (TBT),
- whether a transition period will be foreseen to ensure a smooth implementation of the CRA requirements as regards the products and services already sold in the EU single market.

[9] In case of a « nutriscore » type of label, the length of the maximum period for providing a security patch could dépend on the scoring, e.g. Score A would guarantee patch availability within 1 week, B within 2 weeks, etc.

[10] This may be implemented through legislation outside the CRA but should be taken into account in the discussions. It would ensure consistency with the Circular Economy Action Plan of March 2020, see COM(2020) 98 final.

[11] Directive 2009/24/EC of 23 April 2009 on the legal protection of computer programs.