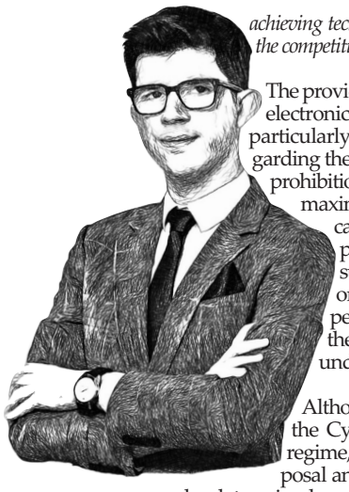
New EU cybersecurity package : digital sovereignty without saying it

By Vincent WELLENS, Avocat à la Cour & Ottavio COVOLO, Avocat à la Cour, NautaDutilh Avocats Luxembourg S.à r.l.



On 20 January 2026, the EU Commission published a new legislative package targeted at cybersecurity within the EU, taking the form of amendments made to EU Regulation 2019/881 (the "Cybersecurity Act"), as well as to Directive n°2022/2555 ("NIS2"). This package has garnered considerable attention, being characterised as the EU Commission's attempt to respond to foreign tech creating weaknesses in the EU's cyber resilience. Why has such package been adopted? What is inside it ? and what does it mean for entities already handling their NIS2 or DORA compliance?

Current state of affairs

Back in December 2003, the European Network and Information Security Agency ("**ENISA**") was initially established on a temporary basis with the mandate of developing standards and coordinating efforts in the field of cybersecurity. Since its inception, ENISA's responsibilities have expanded considerably, particularly entrusting it with the implementation of the first Network and Information Security Directive 2016/1148 (the "**NIS**" Directive). The Cybersecurity Act made further institutional changes by further increasing the roles of the ENISA, removing time limits for its mandate.

The Cybersecurity Act also introduced a European cybersecurity certification framework (notably the published EU cybersecurity certification scheme on common criteria or "**EUCC**"). Such schemes are intended to enable public and private entities to achieve compliance in cybersecurity matters through certification schemes, as evidenced by references thereto in the Cyber Resilience Act,[1] the NIS2 Directive,[2] or even – albeit more implicitly – DORA for the financial sector.[3]

The rationale underlying this evolution reflects a global trend towards heightened focus on cybersecurity as a (geo)political challenge, particularly in recent years where resilience has become an increasingly important topic for governments and even the market. It is noteworthy that, contrary to certain beliefs, these rules follow a bottom-up approach ; the European certification scheme in the Cybersecurity Act for instance stems from a pilot programme between multiple member States.[4]

The thorny issue of the 'kill-switch' in supply-chains

National cybersecurity incidents have attracted significant attention across the EU, including airports shutting down due to a failed anti-virus update at the kernel level or a widely used 2-factor authentication tool being unavailable. Moreover, public scrutiny has extended to systemic vulnerabilities even before incidents happen, such as the widely shared piece on buses in Norway from a Chinese company which is capable of shutting them down remotely,[5] and similar concerns can be traced back to the implementation of 5G networks relying on foreign tech.

This 'kill-switch' has also found its way in public discourse in early February, shortly after the unveiling of the Commission's package, with certain outlets voicing concerns regarding the capacity of US technology companies to, in principle, disable a substantial portion of the EU market infrastructure to the latter's (over)reliance on foreign tech, a hypothesis increasingly considered in the current political climate.[6]

A 'Cybersecurity Act 2' to respond

The Commission proposes to repeal the Cybersecurity Act with a new regulation building upon it. The structure now is comprised of the functioning of the ENISA, the European certification mechanism (rebranded as the European Cybersecurity Certification Framework), and a new component regarding the security of ICT supply chains.

To tackle the above issue of 'kill-switches', the proposal introduces the notion of "Key ICT Assets", defined as software and hardware assets used by entities falling in the scope of NIS2 and identified by the Commission in delegated acts. The Commission has the power to draw up a list of "high-risk suppliers" from which the procurement of Key ICT Assets would become prohibited, and/or require Key ICT Assets to be subject to transparency requirements, limitation in terms of transfers of data to third countries, disabling features, and other limitations.

From an institutional perspective, this may be construed as enabling the EU Commission to create a sanctions-like regime targeting assets in ICT supply chains on the grounds of the functioning of the internal market pursuant art. 114 of the Treaty on the Functioning of the EU ("**TFEU**"). This marks a non-negligeable shift as it is otherwise for the competence of the Council (i.e., the member State governments) to adopt such restrictive measures per art. 215 of the TFEU. Whilst the proposal does not expressly invoke sovereignty considerations, the Commission acknowledges that this represents a "*strategic*" tool "*for achieving technological sovereignty and boosting the competitiveness within Europe*".

The providers of mobile, fixed and satellite electronic communications networks are particularly targeted with stricter rules regarding their Key ICT Assets, limited to the prohibition of their use, and a phase out of maximum 36 months from the publication of the list of high-risk providers. Failure to abide by such prohibitions and restrictions on Key ICT Assets is subject to penalties of a maximum of 7% of the total worldwide turnover of the undertaking.

Although the proposal seeks to align the Cybersecurity Act with the NIS2 regime, the interplay between this proposal and other instruments remains to be determined, such as the aforementioned sanctions regime. T is also unclear how this will play out with the foreign direct investment rules ("**FDI**") already subjecting EU-based entities to screening and filtering procedures when contemplating foreign investments. It is also noteworthy that FDI was already identified as a key lever for supply-chain security by EU States which participated in the 5G toolbox programme, one if not the main source for the Commission's current proposal.

As for the changes to the other titles of the proposal, the ENISA receives an increase in size and funding, notably to better manage the newly established EU Cybersecurity Reserve, which is a collection of cybersecurity services to be offered and managed by ENISA (with key public tenders to be initiated by ENISA in this respect for interested cybersecurity providers). The certification framework has been amended with the goal of speeding up the creation and adoption of certification schemes, with specific deadlines or 12 months for their development upon request by the Commission. The framework is also completed with a European Cybersecurity Skills framework ("**ECSF**") designed to certify cybersecurity professionals (rather than entities).

A "simplified" NIS2 Directive

Echoing the drive of the Commission to "simplify" its regulatory framework through the Digital Omnibus,[7] the second part of the package is an amendment to the NIS2 Directive with the goal of achieving simplification with an alignment to the Cybersecurity Act 2.

As a reminder, the Digital Omnibus sought to introduce a single-entry portal for incident notifications, operated by ENISA (European Union Agency for Cybersecurity). This portal is designed to simplify overlapping reporting obligations under GDPR, NIS2, DORA, and the Cyber Resilience Act ("**CRA**") by applying the principle of "*report once, share many*."

The proposal now aims to take a step further with a new category of small mid-cap enterprises to be designated as important (rather than critical) entities, thus lightening their regulatory burden under the NIS2 Directive. Certain definitions have been clarified in response to challenges faced by healthcare providers, electricity producers, hydrogen undertakings and entities in the chemical sector when implementing the current NIS2 Directive.

Again looking at the concerns regarding 'kill switches', the proposal seeks to capture all aspects of submarine data transmission infrastructure (such as the transatlantic cables responsible for a substantial part of internet traffic), which the current NIS2 Directive does not in relation to private entities operating such infrastructure or leasing it.

A similar focus has been brought to ransomware attacks, instructing national computer security incident response teams ("**CSIRT**") to organise data collection efforts in this respect (in particular in terms of detection, attack vectors and implemented – but defeated – mitigation measures).

Key takeaways

The strategic importance of digital resilience, as reflected in these texts, raises fundamental questions concerning the extent to which controls may be imposed by the Commission and national authorities, particularly in light of entities required to implement such measures having to terminate their reliance on foreign but trusted commercial partners for a durable amount of time.

This may give rise to concerns regarding transitional arrangements and the mitigation of claims for wrongful termination, notably in agreements procuring ICT assets and services concluded at the group level on behalf and to the benefit of entities across the EU or even the globe. Such initiatives may necessitate the inclusion of carve-out provisions in global or international procurement contracts to accommodate local regulatory or sovereignty requirements (as can be seen in certain frameworks already, notably the CSSF Circular 22/806 requiring financial entities to negotiate an explicit termination right upon order by the CSSF thereto, on the grounds of ensuring its regulatory oversight).

More generally, entities may look to assess whether their ICT services do include kill-switches, or other similar vulnerabilities (e.g., back-doors) and try, to anticipate regulatory pressure and to safeguard their resilience, to negotiate for such vulnerabilities to be removed or rendered ineffective.

This proposal, in a manner similar to the Digital Omnibus, has attracted criticism from certain European legislators, and is likely to undergo substantial amendments prior to adoption by the European Parliament and the Council.

1) See recital 87 of the Cybersecurity Act.
2) See recital 80 of the NIS2 Directive.
3) Regrettably, DORA does not include the relevant certification recital present in the NIS2 Directive, with the only mention being a left-over of the EBA guidelines on outsourcing regarding the possibility to take into account third-party certifications regarding the auditing by financial entities of their third-party service providers.
4) Known as the SOGIS Agreement between 17 member States, including Luxembourg, Belgium and the Netherlands.
5) See AP, Chinese-made buses in Norway can be halted remotely, spurring increased security, available at : https://urls.fr/tN-NAs
6) See Politico, EU capitals say deleting US tech is not realistic, available at : https://urls.fr/yKvmFM
7) See our article in the December 2025 edition of the AGEFI for more detail