The EU Cybersecurity Strategy and the NIS 2 Directive
January 2021

By Francesca Maria Vidori

Source: New Europe

I/ Introduction

In today's world, no organization or enterprise is completely safe from cyber-attacks or their possible consequences. As a result, building cyber resilience have developed from a rather technical matter into an increasingly important strategic topic for businesses, on the one hand, and into a critical diplomatic challenge for States, on the other. Indeed, according to ENISA the ongoing public health crisis has shown that the EU's cybersecurity resilience has been pushed to the limit of its capacities.

As part of its key policy objective to make 'Europe fit for the digital age', and in light of the constantly evolving technological landscape, the Commission announced in its Work Programme 2020 that it would review the European cybersecurity strategy and legislative framework by the end of 2020.[1] On **16 December 2020**, the European Commission released its EU Cybersecurity strategy which includes updates to a key piece of legislation: a proposal for a directive **"on measures for a high common level of cybersecurity across the Union" – NIS 2 Directive.**

II/ NIS Directive

The new proposal builds on and repeals Directive (EU) 2016/1148 on security of network and information systems (NIS Directive), which was the first piece of EU-wide legislation on cybersecurity and provides legal measures to boost the overall level of cybersecurity in the Union. The original directive has developed a culture of risk managers within the companies, defining proportional regulatory thresholds through size criteria. The NIS makes two key distinctions between operators of essential services and digital service providers. The former are the primary focus of the NIS Directive.

[1] https://www.eurasiareview.com/26112020-europes-cyber-resilience-a-false-sense-of-security-analysis/

The NIS Directive is part of a package of measures to **improve further the resilience and incident response capacities** of public and private entities, competent authorities and the Union as a whole in the field of cybersecurity and critical infrastructure protection.

III/ The current review

The new Commission proposal aims to address the deficiencies of the previous NIS Directive, taking account of the increased digitisation of the internal market in recent years and an evolving cybersecurity threat landscape. Together with the **Critical Entities Resilience (CER) Directive** the goal is to raise cybersecurity standards across the board, covering both the online and offline world.

The Commission proposal significantly expands the scope of the current NIS Directive by adding new sectors based on their criticality to the economy and society, and by introducing a clear size cap – meaning that **all medium and large companies in selected sectors will be included in its scope**.

The proposal eliminates the distinction between operators of essential services and digital service providers and replaces it with a distinction between **essential entities** and **important entities**. The full list of "essential entities" and "important entities" are included in Annex I and II of the Directive.

The **scope** of the **new directive** covers many new sectors: energy, transport, banking, financial market infrastructures, health, water supply and distribution and various layers of digital infrastructure, public administration, and space. By expanding the scope of the directive, the Commission aims to **increase preparedness at national and Union level** to prevent, detect, respond to and mitigate cyber threats and be prepared to act in crisis.

Furthermore, it will **enhance cyber resilience of all key economic sectors** and reduce fragmentation of the internal market by **increasing the level of harmonisation of requirements** applied to entities in those sectors.

IV/ Three Interlinked Regulations

Another fundamental question that needs to be answered is the policy-coordination with the **Regulation on Digital Operational Resilience for Financial Sectors (DORA)** and the **Critical Entities Resilience (CER)**. The period for feedback of all three regulations will end on **11 February 2021.**

Where potential conflicts of law may arise between the three regulations, the **NIS 2** which sets a broad harmonization framework, will take precedence over the others *(***Article 2.6**).

- The **DORA Regulation** provides clarity on the application of NIS in the **financial sector**, and **harmonizing regulations** among the Member States. This necessity stems from the increasing dependence of the financial sector on Information and Communication Technology (ICT), raising new challenges in terms of operational resilience.
- The **CER Directive** establishes close synergies with the proposed NIS 2 Directive to cover the offline world. Competent authorities designated under, both, the NIS 2 Directive and the CER Directive take **complementary measures and exchange information** as necessary regarding cyber and non-cyber resilience.

V/ Expected Results

The revised NIS Directive and Critical Infrastructure Directive, taken together with the proposal for a regulation on digital operation resilience in the financial sector constitute a considerable 'upgrade' to the European cybersecurity framework.

Consequently, this will likely **increase** the overall **trust in the digital economy**, having a positive effect on growth and investments. Moreover, the higher level of harmonization may result in a **reduction of regulatory costs** for those companies complying with divergent national laws.

In sum, the proposals detail a legislative framework that entails a significant upgrade for cybersecurity particularly in areas related to the supervision and enforcement. Those sectors previously considered outside the scope of the NIS and cybersecurity in general, now find themselves inside the scope, due to their integral role to the broader economy and proliferation of digital technologies broadening the surface for attack by malicious actors.

However, obligations on companies, especially those identified as essential and important entities have also increased considerably, and will likely require investment in terms of personnel and resources to comply with the legislation and requirements set within each member state.

The proposals will now move to the **Council** and the **European Parliament** for further debate. The European Commission maintains a role to shepherd the proposals through the legislative process. In addition, the Commission has signalled another regulation to enshrine a **'cybersecurity by design'** into products will be announced in the course of 2021.

Companies looking to express their views on any and all of these upcoming initiatives should have their views heard by policymakers. With a team specialised in the EU cybersecurity strategy, Lighthouse Europe is ideally situated to assist businesses and industry groups with an interest in these policy discussions and can assist with a better understanding of the legislative process, analysis of the policy debates, and assessment of the market-participants.