ETNO POSITION PAPER

Review of the NIS Directive

@ETNOAssociation #ThinkDigital #ETNODigital WWW.ETNO.EU

Table of Contents

Introduction 2

Scope 3

Coherence Between Different Legislative Instruments 5

Harmonised Application 5

Awareness Building 6

Introduction

ETNO supports the European Commission's global approach to cybersecurity reaffirmed in the "Shaping Europe's Digital Future" communication and welcomes the upcoming revised European Cybersecurity Strategy, including a **review of the Directive on security of network and information systems (NIS Directive)**.

We believe that cybersecurity is of paramount importance, especially with the ongoing digitalisation of the entire society and economy that may be accelerated following the current COVID crisis. When designed, cybersecurity policy should take on board existing EU or international standards and good practices by the industry and acknowledge that there cannot be a one-size-fits-all set of cybersecurity measures. Cybersecurity challenges and measures vary considerably depending on the sector (e.g. critical infrastructures, government etc.), the type of users (consumers vs. enterprises), the types of data etc.

Several telecommunications operators and ETNO members are active across multiple countries in the European single market. Therefore, our industry calls for a legislative framework that provides for a **high common level of cybersecurity and legal certainty**. A fragmented set of European and national rules would inevitably lead to market distortions and differing security standards.

We would hereby like to point to gaps in the existing NIS Directive and in its implementation, and to recommend possible improvements from the perspective of the already highly regulated telecommunications industry.

The review of the NIS Directive should meet the following **key objectives**:

- Address all relevant actors, in particular by including **vendors of hardware and software** in the scope of the reviewed legislation to achieve a more robust, secure and resilient digital value chain;
- Ensure **coherence and consistency** between different legislative instruments to avoid complexity and redundancy in the application of security requirements, in particular with the provisions of the European Electronic Communications Code, the EU Cybersecurity Act and with new measures on critical infrastructure protection;
- Reduce fragmentation within the Single Market through legislation that provides for a **harmonised implementation** across Member States, and hence more legal certainty for pan-European operators;
- Expand public private cooperation to **raise awareness and build skills and competences** that are essential in an increasingly digitalised economy and society.

Scope

The **material scope** of the NIS Directive is a critical aspect that needs addressing in the upcoming review. On the one hand, the boundaries of the current scope are not clearly defined and have led to diverging approaches in national implementation; on the other hand, some key actors that have a major role in European networks and systems are not regulated by the Directive at present.

Telecommunications operators play a vital role in securing our networks and services. In addition, based on art. 40 and art. 41 of the **European Electronic Communications Code** (Directive EU 2018/1972, hereafter 'Code'), electronic communications service (ECS) providers are subject to strict obligations regarding minimum network and service security requirements and the reporting of security incidents to competent authorities as well as – in particular cases – to their customers.

Against this background, the recognition that a number of market players, notably **providers of electronic communication networks or services** (hereby Operators), are and should remain excluded from the scope of the NIS Directive because they already fall under existing obligations (as clearly stated in recital 7 of the Directive) should inform the upcoming review[1].

Unfortunately, the perimeter of the Directive has proven to be much more blurred than the letter of the law suggests. Member States have taken different approaches to implementing the Directive and identifying **operators of essential services (OES)**, which has led to diverging interpretations as to the services and actors that should be in scope.

Because Operators grant access to their networks and information systems and provide their services to OES, they have been caught in the scope of national implementing measures of the NIS Directive in some Member States, despite being already subject to similar requirements under sectoral law.

The review of the NIS Directive should provide for a **clear scope**, which must guarantee full certainty to both competent authorities and service providers about the perimeter of application of the revised rules and must avoid unwarranted double regulation.

At the same time, it is important that all actors of the digital value chain play their role in ensuring the security and resilience of networks equipment and services. In particular, **vendors (i.e., manufactures and suppliers) of hardware and software** have currently no legal responsibility regarding the security issues generated by their equipment as part of a network. Yet, these actors are fundamental to ensuring a secure and resilient digital infrastructure within the EU. Software will play an increasingly important role in our future digitalised society, and in telecommunications networks that are currently starting their virtualisation. Large quantities of hardware and software can contain design or implementation vulnerabilities in their code, which makes these products vulnerable to malware and hacking due to low-quality programming.

[1] Telecommunications operators are regulated as Digital Service Providers (DSPs) insofar as they offer their own or third-party cloud computing services to their customers or run digital infrastructure services like DNS and IXPs.

All Operators must comply with **operational and security validation procedures** for equipment from external suppliers. This validation would typically be based on tests and models stipulated by internationally recognised recommendations (e.g., ISO 27000, among others), and on their own experience (regulatory and internal security processes and policies resulting in operating procedures for the verification of appropriate security levels in the equipment).

However, beyond the tests already done by Operators, there can be instances where it is impossible for an Operator to know whether a piece of equipment or service could present vulnerabilities during its **lifecycle**. In addition, critical updates to fix security issues are released according to vendors' priorities, sometimes leaving exposed products vulnerable to cyber threats for an unacceptable period of time.

Including hardware and software vendors within the scope of the NIS Directive would be helpful to tackle the vulnerability risk associated to the virtualisation of network functions and would ensure that **each actor bears their part of their responsibility** for a secure and resilient digital value chain, considering their important role in network and information security.

Typically, cybersecurity risks are addressed in contractual agreements with third-party vendors, which may include various security clauses regarding notification of breaches and cooperation, response time to vulnerabilities, demonstration of compliance, management of supply chain risk, etc. However, the high variety of contracts and of companies' bargaining power in negotiations does not ensure a fair and homogeneous distribution of responsibility for all critical services and networks. The introduction of **clear legal requirements for hardware and software vendors** would provide more legal certainty and a strong security baseline for individual contractual agreements.

As a result of these highlighted concerns, vendors of hardware and software should then be subject to minimum regulatory requirements, such as:

- Obligations to adopt **risk management practices**;
- Obligations to **disclose security incidents or vulnerabilities** to the relevant authorities and to their clients;
- Obligation to **remedy vulnerabilities** and to apply the "security-by-design" principle;
- Make regular **security updates available** for the period of the expected product lifecycle;
- Provide **information about vulnerabilities** to their clients, within a reasonable delay and according to the bulletin delivered to Computer Emergency and Response Team contact or equivalent;
- As the need may arise, align with the **security assurance levels** as defined in the EU's Cybersecurity Act.

Coherence Between Different Legislative Instruments

Within the EU and at international level, **enhanced coordination and a common approach** are needed to ensure a consistent and coherent application of security activities related to network and information security. At the international level, the UN processes on the implementation and applicability of norms for peace and stability in cyberspace are of particular relevance. Cybersecurity policy at the EU level can play an important role in creating awareness, spreading, and further strengthening such norms aimed at a more stable and peaceful ICT environment.

Operators are subject to **a number of sectoral regulations** and we would urge the European Commission to strive for better coordination (and effectiveness) at all levels in order to avoid overlaps with ongoing initiatives. Industry needs legal certainty and clarity. As a result, we call upon the European Commission to ensure that the future review of the NIS Directive remain consistent and coherent with **Article 40 of the Code** on the security of services and networks, which will replace Article 13a of the Framework Directive. Furthermore, the Commission should strive to ensure that any other initiative, for instance on critical infrastructures, remains fully consistent with the rules already in place for Operators and does not add complexity or create redundancy.

Finally, the **certification framework** introduced by the EU Cybersecurity Act should be used as an additional means to close the gaps of the NIS Directive, particularly with respect to the security of 5G networks.

Harmonised Application

Besides consistency of various legal obligations, it is crucial that the revised NIS text is **consistently implemented across Member States**. There are still today discrepancies in interpretation of whether an essential service falls within the scope of the Directive depending on the country. This means that some actors may be notified by their authorities as being OES in certain countries and not in others. The **scope of the notification** should be made clearer and identical in all Member States, and companies covered by such status should be duly notified by the competent authority. Whereas pan-European incidents are set to increase, expectations as to the obligations both on the part of notifying entities and of competent authorities should not diverge across States.

This also calls for the Commission to ensure **the highest level of harmonisation** when designing its amended rules. Consequently, decision makers should consider whether the revised NIS legal instrument should come in the form of a Directive including a set of binding and comprehensive provisions for national implementation, or even a Regulation providing for the highest possible level of EU harmonisation.

Awareness Building

Next to the necessary improvements to the current NIS Directive, **increasing private public cooperation, raising awareness, and building of skills and competences** within the EU will also continue to be very important going forward.

With the rapidly progressing digitalisation of the European and Global economy, the threat landscape for the digital environment is growing at an ever-faster pace. Today we are confronted with industrial espionage, organised crime, organised disinformation campaigns against democratic societies, and ultimately with cyberwar. Tackling all these risks and the potential damages are a growing burden for industry and society.

The successful uptake of services like Cloud, IoT, autonomous driving, eHealth, smart grid technology and other new applications depends on the **trust of users** in the security of an increasingly digitalised world. Furthermore, advancing cyber capabilities in the threat landscape have shown the potential for devastating **impact on societies**, ranging from potential impact on democratic institutions, to the health and safety of citizens, with attacks on civilian infrastructure, such as attacks on hospitals.

A more coherent European and global cybersecurity policy to protect digital services and networks has become essential for all industries and policy makers.

European Telecommunications
Network Operators' Association

info@etno.eu
+32 (0)2 219 3242
WWW.ETNO.EU

@ETNOAssociation

Subscribe to our weekly digital newsletter