Position Paper – European Critical Infrastructure Directive

Bitkom views concerning the Inception Impact Assessment

6 of August 2020

Introduction

As the voice of the German digital economy, Bitkom highly appreciates the opportunity to provide feedback on the European Commission's consultation on the possible review of the existing European Critical Infrastructure Directive (hereafter referred to as the ECI Directive). Rooted in the identified need to counter threats from terrorism and while focusing exclusively on the transport and energy sector, the ECI Directive sets out a procedure for identifying European Critical Infrastructures and aims to improve their protection and resilience.

Bitkom shares the Commissions view that the quality of life throughout the European Union and the security of its citizens as well as the correct functioning of the internal market essentially depend on reliably functioning critical infrastructures. We also agree that the existing framework for protection and resilience of critical infrastructures is inadequate in the light of increasing interdependencies and evolving risks and that a single focus on physical protection does not ensure a reliable functioning of critical infrastructures.

Our position is guided by the urgent need to create a more coherent and harmonized common level playing field. We are convinced that common and harmonized legislation at EU level is the most effective way to improve protection and promote resilience of critical infrastructures. To this end, and considering the parallel consultation process of ECI and NIS Directive, we strongly encourage the Commission to make smooth and streamlined communication the key priority. Anything but seamless cooperation and close coordination between the different directorates would be completely counter-productive and undermine the overall objective of increasing the resilience of critical infrastructures across Europe.

Bitkom is of the position that policy **'option 3'**, namely *new requirements for European critical infrastructures*, would be the best approach to ensure the security of our critical infrastructures in the future. The recent evaluation[1] of the ECI Directive revealed several shortcomings and inconsistencies that we consider as best addressed by targeted legal amendments.

[1] SWD(2019) 308 (link).

Bitkom
Bundesverband
Informationswirtschaft,
Telekommunikation
und neue Medien e.V.
(Federal Association
for Information Technology,
Telecommunications and
New Media)

Sebastian Artz
IT Security
s.artz@bitkom.org

Albrechtstraße 10
10117 Berlin
Germany

President
Achim Berg

CEO
Dr. Bernhard Rohleder

European Critical Infrastructures

In accordance with the third policy option envisioned in the inception impact assessment, we call for a clarification and streamlining of cross-legislative definitions and requirements to further facilitate the implementation in all Member States. Any future legislation under the ECI should aim at improving consistency in terms of:

- streamlined requirements for operators;
- better intertwining with sectoral legislation;
- accounting for interdependencies between European critical infrastructures.

At the same time, we see the need to clarify the distinction between critical infrastructures and European Critical Infrastructures. For doing so, we recommend to also view critical infrastructure legislation through the prism of subsidiarity. Admitting that nationally located critical infrastructures are usually best regulated at national level is likely to help narrowing the scope of European Critical Infrastructures and, thereby, significantly improve their protection and resilience following a (European) risk-based approach.

Nevertheless, we are rather reserved when it comes to the proposal of expanding the scope of European Critical Infrastructures beyond energy and transport as other sectors, such as banking, health or telecommunication, are already covered by tailored regulations including respective security obligations. As the Commissions background report correctly concludes: *"Several complementarities and overlaps with other pieces of European sectoral legislation/policy documents in the energy, transport and ICT sectors exist"*. The NIS Directive further complements the regulatory picture. If the Commission, notwithstanding our reservations, should opt for an enlarged sectoral scope under the ECI, we clearly highlight the importance that any expansion must be guided by scientific reasoning and should not be the outcome of mere political interests.

Regulatory Overlaps

The biggest foe of security is complexity. The same holds true for legislation and respective reviews. It remains tricky to fully embrace the intention of reviewing the ECI- and the NIS-Directive simultaneously under the supervision of two distinct directorates without providing guidance or expectation management concerning the future interplay. While the ECI Directive is rooted in the identified need to counter threats from terrorism and focuses exclusively on the transport and energy sector, the NIS Directive aims to increase the levels of cybersecurity across the Union, in particular on the level of national cybersecurity capabilities and the capacity to mitigate growing security threats to network and information systems.

Although we are well aware of the fact that cyber-related issues are not yet fully congruent with all (physical) threat vectors to critical infrastructures, the division into IT and physical security is becoming increasingly blurred. This development is likely to continue in the years to come. Subdivisions based on the motivation of the attackers are irrelevant in most cases. It makes no difference whether an attack on critical infrastructure is launched by an economically oriented cybercriminal, a governmental organization or a terrorist. They use the same procedures and affect ultimately the same objectives. From our perspective, the NIS Directive represents a more inclusive horizontal approach and, therefore, is the more sophisticated instrument to counterbalance cybersecurity risks, including terrorism, which has become a hybrid digital threat by now. Against this backdrop, and in order to avoid any kind of double legislation, we call for a more integrative and combined approach merging the overlapping points of both directives within the NIS Directive.

In the same vein, we clearly warn against any inclusion or regulation of cyber-related threat elements under the ECI Directive as the cyber-sphere is best addressed by the NIS Directive. Considering the circumstance that the initial impact assessment of the ECI Directive also touches upon cyber-attacks, drones, 5G and AI, we highlight the urgent need to avoid imposing new forms of double legislation and excessive administrative burdens. Any updated ECI Directive would rather profit the most when referencing to the reviewed NIS Directive in a coherent fashion. At this point we would like to draw the Directorates General attention to our Bitkom position paper concerning the Roadmap of the NIS-Review (available after the 13th of August on our Bitkom website).