Bitkom position on the proposal for a Directive on the Resilience of Critical Entities

April 2021

Preliminary Remarks

Rooted in the identified need to counter threats from terrorism and while focusing exclusively on the transport and energy sector, the Council Directive 2008/114/EC, better known as the European Critical Infrastructure (ECI) Directive: "*establishes a procedure for the identification and designation of European critical infrastructures, and a common approach to the assessment of the need to improve the protection of such infrastructures in order to contribute to the protection of people*". Besides the ECI-Directive, the Directive 2016/1148 concerning measures for implementing an equivalent and commonly high level of security in network and information systems across the Union (hereafter referred to as the NIS-Directive) has shaped the European understanding of critical infrastructure protection. Bitkom shares the Commission's 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.

On 16 December 2020, the European Commission launched the EU's new Cybersecurity Strategy for the Digital Decade, seeking to bolster Europe's cyber resilience and step up the EU's leadership in cybersecurity regulation. As part of this major overhaul, the Com-Commission released two proposals, a renewed NIS-Directive to better address cyber-related risks and the new Critical Entities Resilience Directive (hereafter referred to as CER-Directive) to account for non-cyber-related risks such as natural hazards, hybrid threats, terrorism, insider incidents, public health emergencies or accidents. The later replaces the ECI-Directive, as the EU seeks to enhance the resilience of critical entities against physical threats. The proposed CER-Directive expands both the scope and depth of the ECI-Directive. The new scope includes the sectors energy, transport, banking, financial market infrastructures, health, drinking water, waste water, digital infrastructure, public administration and space.

Bitkom agrees that the existing framework for protecting critical infrastructures is inadequate in the light of increasing interdependencies and evolving risks. The changing nature of the threat landscape requires both better protection and more investment in resilience capacities to secure our critical infrastructure. We see the imperative need for a future-proofed protection framework and therefore welcome the Commission's initiative. Bitkom recognizes the European Commission's aim to simultaneously address cyber and non-cyber threats by combining the NIS2-Directive with the new CER-Directive. Besides our detailed and already submitted position on the NIS2-Directive, we appreciate the opportunity to also provide feedback on the CER-Directive.

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

Sebastian Artz
Information Security & Security Policy
s.artz@bitkom.org

Albrechtstraße 10
10117 Berlin
Germany

President
Achim Berg

CEO
Dr. Bernhard Rohleder

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.

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. Cybercriminals, governmental organizations or terrorists use the same procedures and affect ultimately the same objectives to which we are committed (business continuity, readiness for response / resilience, better prevention). What is needed is a European harmonization of the included sectors as well as of the requirements (general and sectoral). This remains difficult to convey to a regional and sectoral structure of authority.

That's why Bitkom strongly calls for consistency and alignment of the new CER-Directive with other regimes and legislative developments. Maintaining or even introducing new cross-country fragmentation must be avoided at any cost. At European level, the renewed NIS-Directive, the EECC, the proposed DORA regulation as well as the Cybersecurity Act must go hand in hand with the new CER-Directive. This requires consistent and clear definitions, coherent across the entire regulatory landscape as well as an unambiguous sectoral scope. Only if these conditions are met we will succeed in truly harmonising the European and national level in the field of cybersecurity and critical infrastructure protection.

The CER Directive must strike the right regulatory balance and avoid overburdening critical entities with new obligations. In some points, the current proposal is too far-reaching. Most notably, the (new) cross-border risk assessment and additional reporting obligations are a mammoth task in themselves.

With respect to the required alignment of the NIS- and CER-Directive, entities being classified as essential under the NIS2-Directive should be classified as critical under the CER-Directive. The European Commission and Member States should provide critical and essential entities with one single point of contact where these entities are supposed to register, and where they can notify both cyber incidents and incidents according to Article 13 (1) of the CER Directive. Either Member States should identify what constitutes both critical and essential in their country (CER-logic), or the EU should do so for all Member States (NIS2-logic). Anything but a common understanding, seamless cooperation and close coordination would be completely counterproductive and undermine the overall objective of increasing the resilience of critical infrastructures across Europe.

Content

Article 2: Definitions

Article 2 (2) defines resilience as: "*the ability to prevent, resist, mitigate, absorb, accommodate to and recover from an incident that disrupts or has the potential to disrupt the operations of a critical entity*". This definition requires further clarification as it does not distinguish between the cyber and the physical non-cyber dimension of resilience. The CER-Directive must exclusively target the later; the former is already comprehensively covered by the NIS2-Directive.

Article 3: Strategy for reinforcing the resilience of critical entities

It is to be welcomed that each Member State must adopt a strategy for reinforcing the resilience of critical entities. However, Member States must consult critical entities before developing such a strategy.

Article 4: Risk assessment by Member States

Article 4 (1) states that Member States must, within 3 years from adoption, establish a list of essential services "*in the sectors referred to in the Annex*". The provision does not explicitly explain if Member States have a right to *pick* categories of services listed in the Annex or if they are obliged to identify entities within *each* category. Considering the fact that the Directive is focused on Critical Entities, using the term essential services leads to unnecessary confusion as the NIS2-Direcitve introduces the category of essential entities.

Article 5: Identification of critical entities

Considering the almost identical sectoral scope of the CER- and NIS2-Directive, it does not seem reasonable why critical entities shall be identified by each Member State individually while essential entities are identified uniformly throughout Europe. Bitkom recommends a closer alignment of the proposed scope of the CER- and NIS2-Directive in terms of critical and essential entities. A coherent terminology and scope is of great importance.

Article 7: Entities equivalent to critical entities under this chapter

Article 7, in conjunction with recital 14, aims to exempt digital infrastructures as well as banking and financial market infrastructure from the reporting and material obligations foreseen in Chapter III and IV of the CER-Directive. While the explanation in recital 14 is unambiguous, the wording in Article 7 itself remains vague and there is no clear description of what the identification as "entity equivalent to critical entity" implies. The final wording must ensure that no resilience requirements or reporting obligations on digital infrastructures are introduced, as they are indeed covered exhaustively under the NIS2-Directive.

Article 8: Competent authorities and single point of contact

There is an urgent need to have a clearly defined reporting process. So far, our members face highly inefficient, redundant and non-transparent reporting structures across sectors, requiring entities to inform different (public) institutions about the very same incident while having to comply with distinct processes and timelines. Nobody wants to report too much, but too little is punishable. This makes it even more confusing for companies to report the required information to the responsible entity before the respective deadline. With the newly proposed expansion of the scope of the NIS and with additional legislative proposals being discussed simultaneously, it is now more important than ever to ensure a high level of consistency amongst all other legislations. This refers in particular to legislation such as the General Data Protection Regulation (GDPR), Payment Services in the internal market Directive (PSD2) and the EECC all have related reporting requirements, which vary with regards to entities reporting timeframes, level of information/detail and potential non-compliance penalties. The newly proposed CER-Directive should not introduce even more complexity to the reporting landscape. This would lead to unnecessary bureaucracy and duplication of effort, because each authority has different requirements and regulations for reporting. Therefore, a single point of contact should be established not only to exercise a liaison function to ensure cross-border cooperation and cooperation with the Critical Entities Resilience Group but also to simplify and harmonise reporting channels (one-stop-shop principle).

Article 10: Risk assessment by critical entities

Strong risk management frameworks play a core part in mitigating physical and cyber treats. It must be ensured that the risk assessment remains with the respective critical entity and is not subject to control by national authorities. The EU should explicitly refer to European and internationally recognized standards (e.g. ISO 22301). Furthermore, a holistic assessment – across borders and sectors – is not possible within six months. In this sense, the planned period for the assessment must be extended to one year.

Article 11: Resilience measures of critical entities

When the European Commission adopts delegated or implementing acts under Article 11, it must ensure coherence between already existing national requirements and the requirements to be adopted by the EU Commission. In Germany, for example, the national legislator is in the process of introducing new measures. These are laid down in the IT Security Law 2.0 and, for the telecommunications sector, additionally in § 109 of the Telecommunications Act (§164 new) and the corresponding security catalogue. This increases the probability that the delegated acts or implementing acts of the European Commission will deviate from the German regulatory framework in the future and that German companies will be confronted with contradictory requirements. This must be avoided at any cost. Bitkom sees the risk of further fragmentation if European and national institutions both start adopting more and more delegated or implementing acts without passing through the necessary feedback loops including the private sector.

Article 12: Background checks

Background checks are to be welcomed, but authorities must conduct them in a timely reasonable manner and without overly bureaucratic obstacles.

Article 13: Incident notification

In a globalized economy, it is difficult to track every piece of data. Information sharing and publication of security incidents may enhance security, but it is crucial that only essential information is distributed (Article 13, 3). In the same vein, the responsibility to assess the number of users affected or their respective geographical location should be limited (Article 13, 2).

Article 14: Critical entities of particular European significance

Under no circumstances a Critical Entity of European Significance should be subject to double-reporting obligations. Fortunately, the proposal accounts for this need. Granting the advisory mission access to relevant documents and sites cannot run counter to the smooth operation of the entity's services. In addition, sensitive information as well as business secrets must be treated confidentially at all time.

Article 18: Implementation and enforcement

Article 18 (1) foresees that national authorities obtain the possibility to conduct monitoring, supervision, and "*shall have the powers and means to conduct on-site inspections of the premises that the critical entity uses to provide its essential services*". In addition and according to Article 14 and 15, entities of particular 'European Significance' are subject to specific oversight, where Member State authorities report to the European Commission and the Critical Entities Resilience Group on their compliance with requirements. Member States should also ensure that special advisory groups for compliance monitoring have access to "*information, systems and facilities relating to the provision of its essential services*" (Article 15(6)).

The introduction of fines is justified. However, and instead of referring to the annual turnover, the maximum level of administrative fines should not exceed a maximum of two million EUR. In general, the Commission would be well advised not to forego the potential of incentivizing essential and important entities. Such approach is currently missing in the proposal.

Bitkom represents more than 2,700 companies of the digital economy, including 2,000 direct members. Through IT- and communication services alone, our members generate a domestic annual turnover of 190 billion Euros, including 50 billion Euros in exports. The members of Bitkom employ more than 2 million people in Germany. Among these members are 1,000 small and medium-sized businesses, over 500 startups and almost all global players. They offer a wide range of software technologies, IT-services, and telecommunications or internet services, produce hardware and consumer electronics, operate in the digital media sector or are in other ways affiliated with the digital economy. 80 percent of the members' headquarters are located in Germany with an additional 8 percent both in the EU and the USA, as well as 4 percent in other regions of the world. Bitkom promotes the digital transformation of the German economy, as well as of German society at large, enabling citizens to benefit from digitalisation. A strong European digital policy and a fully integrated digital single market are at the heart of Bitkom's concerns, as well as establishing Germany as a key driver of digital change in Europe and globally.