DIGITALEUROPE

12 APRIL 2021

Critical entities: ensuring coherence of non-cyber and cyber resilience

Executive summary

The changing nature of the threat landscape requires better protection and more investment in the EU's resilience capacities to secure our critical infrastructure. DIGITALEUROPE welcomes the Commission's effort to strengthen the resilience of critical entities across the EU by developing and updating relevant legislation.

The proposal for a Directive on the resilience of critical entities (RCE Directive)[1] expands both the scope and depth of the 2008 European Critical Infrastructure (ECI) Directive.[2]

The following elements should be addressed during the legislative process:

- Requirements regarding physical non-cyber protection under the proposed RCE Directive should be more clearly separated from requirements regarding cyber protection under the revised Directive on Security of Network and Information Systems (NIS2);[3]
- The RCE Directive should not introduce additional requirements or obligations on digital infrastructure, which is already covered exhaustively under the NIS2;
- Clearer and more transparent supervision practices should be introduced; and
- Better harmonisation can be achieved between the RCE proposal, the NIS2 and the proposed Regulation on digital operational resilience for the

[1] COM(2020) 829 final.

[2] Council Directive 2008/114/EC.

[3] COM(2020) 823 final.

DIGITALEUROPE
Rue de la Science, 14A, B-1040 Brussels
T.+32 (0) 2 609 53 10 / www.digitaleurope.org / @DIGITALEUROPE
EU Transparency Register: 64270747023-20

financial sector (DORA),[4] including in terms of regulatory cooperation, implementation timelines and reporting thresholds.

[4] COM(2020) 595 final.

Table of contents

Scope

The RCE Directive is launched in parallel with the NIS2 review. As recognised in the proposal,[5] it is necessary to achieve a coherent approach between the two instruments. Overlaps should be avoided between the requirements regarding physical non-cyber protection under the proposed RCE Directive and requirements regarding cyber protection under the NIS2.

This distinction should be further clarified in the definition of 'resilience' in the RCE Directive.[6] It is unclear whether the current definition points specifically only to physical (non-cyber) aspects of resilience or not. Such unclarity may result in national authorities imposing overlapping rules that ultimately affect the overall resilience of the proposed system, causing counterproductive uncertainty and complexity for market players.

Specifying the scope

The RCE Directive states that Member States must, within three years from adoption, establish a list of essential services 'in the sectors referred to in the Annex.'[7] This provision does not 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. As the Directive is focused on critical entities, using terms such as essential services can also add to unnecessary confusion. DIGITALEUROPE therefore recommends further clarification of these provisions.

Legal regime for digital infrastructure

DIGITALEUROPE understands that the RCE Directive aims to exempt digital infrastructure as well as banking and financial market infrastructure from the reporting and material obligations foreseen in Chapters III-IV.[8]

However, the RCE Directive itself remains vague and there is no clear description of what the identification as 'equivalent to critical entities' implies.[9] It must be ensured that the RCE Directive does not introduce resilience requirements or additional reporting obligations on digital infrastructure, which is already covered exhaustively under the NIS2.

---

[5] See Recital 8, COM(2020) 829 final.

[6] See Art. 2(2), ibid.

[7] See Art. 4(1), ibid.

[8] See Art. 7 and Recital 14, ibid.

[9] See Art. 7, ibid.

Supervision and enforcement

Supervision practices should be clear and transparent.

Under the proposal, national authorities are granted generic powers and means to conduct on-site inspections.[10] Moreover, 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.[11] 'Advisory missions' for compliance monitoring of entities of particular 'European significance' are also granted generic access to 'all information, systems and facilities relating to the provision of … essential services.'[12]

The final text should specify clearer procedural safeguards, including which categories of information can be accessed by the authorities and the proposed 'advisory missions' to ensure the Directive provides legal certainty for entities.

Harmonisation with other existing legislation

DIGITALEUROPE welcomes the proposal's intention to harmonise the RCE requirements with existing and future EU legislation such as the NIS2 and the proposed DORA Regulation.

It is important to promote increased coordination among supervisory bodies under these legislative proposals. Notably, the RCE Directive sets out a Critical Entities Resilience Group that will cooperate with the NIS Cooperation Group. We note that the proposal envisages an annual cadence of meetings between the two groups, which may be insufficient to achieve meaningful progress in this direction.[13] We would also recommend that the DORA supervisory authorities be also included.

Since critical infrastructure is largely owned and managed by private entities, DIGITALEUROPE recommends more structural involvement of industry in these coordination efforts, for both better alignment and as resource for industry-specific knowledge.

Lastly, aligned timetables for the entry into force of the RCE Directive, the NIS2 and DORA would benefit the overall implementation process.

[10] See Art. 18(1), ibid.

[11] See Art. 15, ibid.

[12] See Art. 15(6), ibid.

[13] See Art. 16, ibid.

Reporting thresholds

The RCE Directive, comparable to the NIS2 proposal, calls for notifications of incidents having 'the potential to significantly disrupt operations.'[14]

In most cases, such demands will lead to overinforming by the entity to the national authority, with massive amounts of data and information burdening their internal incident handling processes.

Sharing general cyber threats or near misses is not useful and would create unnecessary burden for organisations that would need to process and try to operationalise the information shared. By contrast, periodic updates or threat analysis reports from relevant entities, complemented by dialogue to provide context, are more relevant and useful.

FOR MORE INFORMATION, PLEASE CONTACT:

Alberto Di Felice

Director for Infrastructure, Privacy and Security

alberto.difelice@digitaleurope.org / +32 471 99 34 25

Martin Bell

Privacy and Security Policy Manager

martin.bell@digitaleurope.org / +32 492 58 12 80

[14] See Art. 13, ibid.

About DIGITALEUROPE

DIGITALEUROPE represents the digital technology industry in Europe. Our members include some of the world's largest IT, telecoms and consumer electronics companies and national associations from every part of Europe. DIGITALEUROPE wants European businesses and citizens to benefit fully from digital technologies and for Europe to grow, attract and sustain the world's best digital technology companies. DIGITALEUROPE ensures industry participation in the development and implementation of EU policies.

DIGITALEUROPE Membership

Corporate Members

Accenture, Airbus, Amazon, AMD, Apple, Arçelik, Autodesk, Bayer, Bidao, Bosch, Bose, Bristol-Myers Squibb, Brother, Canon, Cisco, DATEV, Dell, Dropbox, Eli Lilly and Company, Epson, Ericsson, Facebook, Fujitsu, GlaxoSmithKline, Google, Graphcore, Hewlett Packard Enterprise, Hitachi, HP Inc., HSBC, Huawei, Intel, Johnson & Johnson, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, Mastercard, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe Inc., NEC, NetApp, Nokia, Nvidia Ltd., Oki, OPPO, Oracle, Palo Alto Networks, Panasonic Europe, Philips, Pioneer, Qualcomm, Red Hat, Ricoh, Roche, Rockwell Automation, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Siemens Healthineers, Sony, Swatch Group, Technicolor, Texas Instruments, Toshiba, TP Vision, UnitedHealth Group, Visa, VMware, Workday, Xerox.

National Trade Associations

Austria: IOÖ
Belarus: INFOPARK
Belgium: AGORIA
Croatia: Croatian Chamber of Economy
Cyprus: CITEA
Denmark: DI Digital, IT BRANCHEN, Dansk Erhverv
Estonia: ITL
Finland: TIF
France: AFNUM, SECIMAVI, Syntec Numérique, TECH IN France
Germany: BITKOM, ZVEI
Greece: SEPE
Hungary: IVSZ
Ireland: Technology Ireland
Italy: Anitec-Assinform
Lithuania: INFOBALT
Luxembourg: APSI
Netherlands: NLdigital, FIAR
Norway: Abelia
Poland: KIGEIT, PIIT, ZIPSEE
Portugal: AGEFE
Romania: ANIS
Slovakia: ITAS
Slovenia: ICT Association of Slovenia at CCIS
Spain: AMETIC
Sweden: Teknikföretagen, IT&Telekomföretagen
Switzerland: SWICO
Turkey: Digital Turkey Platform, ECID
United Kingdom: techUK