Proceedings of the 1st European Cluster for Securing Critical Infrastructures (ECSCI) Virtual Workshop

*

Healthcare critical infrastructures protection and cybersecurity in the EU: regulatory challenges and opportunities

Author: Elisabetta Biasin (KU Leuven Centre for IT & IP Law)¹

*

Abstract: 2020 marks a crucial year for the EU agenda on critical infrastructure protection and cybersecurity, as EU policy-makers which will have to re-consider key pieces of legislation on the matter. By applying a particular focus on healthcare, this contribution aims at providing key perspectives on the upcoming regulatory challenges, based on the research carried out in the SAFECARE project.

Critical Infrastructures; Healthcare; Cybersecurity; Medical Devices

1. Introduction

Healthcare critical infrastructures are essential services for the security and well-being of individuals. The protection thereof should ensure their continuous functioning in order to impede disruptions and serious consequences for society from which it depends. Such a kind of protection is currently regulated at the EU and national level – and in the upcoming months, these rules may be revised by EU regulators. This workshop paper outlines the main regulatory challenges that concern the regulation of healthcare critical infrastructures, leveraging upon the research carried throughout the SAFECARE project. To do so, this paper gives a brief contextualisation of the matter (§2); it outlines the relevant frameworks (§3); and regulatory challenges concerning the European Critical Infrastructures Directive (ECI Directive)² (§4); the Network and Information System Directive (NIS Directive)³(§5). In light of such brief analysis, conclusive remarks (§6) will provide key takeaways on the regulatory challenges and opportunities that EU policy-makers should consider for the healthcare critical infrastructures and their cybersecurity.

2. Context

Ensuring the protection of healthcare infrastructures is becoming a great disquiet for organisations and professionals worldwide. Physical attacks are a common source of insecurity for healthcare facilities. Attacks may deprive people of urgently needed care, endanger healthcare providers and undermine health systems.⁴ These concerns embrace cybersecurity, too. The last few years have seen an increasing rate of IT security incidents and data breaches for many healthcare ecosystems. Disrupting attacks to healthcare facilities, such as Wannacry and NotPetya underlined the necessity of keeping the level of those infrastructures adequate to security risks. This concern did not diminish after the COVID19 outbreak, which, on the contrary, led to an increase of cyber-attacks in healthcare.⁵ At the same time, physical threats remained a critical factor to monitor in hospitals as the shortage of medical products caused thefts and security incidents in a wide range of cases.⁶

3. Setting the framework

Modern society is characterised by a strong interdependency between processes, resources and the correct functioning of infrastructural systems, whose interruption, damage or unavailability may cause economic damages for the society, and may

¹ Correspondence email: Elisabetta.biasin@kuleuven.be. Contributors: Erik Kamenjasevic (KU Leuven Centre for IT & IP Law), Pierre Notermans. Funding acknowledgement: this research has received funding from the European Union's H2020 research and innovation programme under grant agreement no. 787002.

² Council Directive 2008/11/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection [2008] OJ L345/75 (ECI Directive).

³ Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union [2016] OJ L194/1 (NIS Directive).

⁴ WHO 'Stopping attacks on health care' (WHO) <<https://www.who.int/activities/stopping-attacks-on-health-care>> accessed 30 September 2020.

⁵ INTERPOL 'Cybercriminals targeting critical healthcare institutions with ransomware' (INTERPOL, 4 April 2020) <<https://www.interpol.int/en/News-and-Events/News/2020/Cybercriminals-targeting-critical-healthcare-institutions-with-ransomware>> accessed 30 September 2020.

⁶ J Philpot 'Security Incidents in Healthcare Infrastructure during COVID-19 Crisis' (SAFECARE, 25 September 2020) <<https://www.safecare-project.eu/?p=588>> accessed 30 September 2020.

imply domino effects also in the provision of services and social development.⁷ That is why critical infrastructures must be protected.

The protection of critical infrastructures in Europe requires the consideration of two distinct yet intertwining frameworks: first, the Critical Infrastructures Protection (CIP) framework and second, the Critical Information Infrastructures Protection (CIIP) – most commonly referred to as ‘cybersecurity’.⁸ CIP is a matter of national regulation due to the EU subsidiarity principle.⁹ At the EU level, the protection of critical infrastructures is regulated under the European Critical Infrastructure Directive (ECI Directive), whose implementation is embraced under the European Programme for CIP (EPCIP) and the CI Warning Network. Cybersecurity is a field that in recent years received growing attention by the EU legislator within the framework of the European Commission’s 2013 Digital Single Market Strategy. Such impulse led to the adoption of the first piece of legislation on cybersecurity, the NIS Directive, which was followed by other hard and soft laws, including the Cybersecurity Act¹⁰.

4. *Regulatory challenges and opportunities for the CIP in healthcare: the ECI Directive*

As research carried out in SAFECARE showed, the CIP framework envisages two opportunities and challenges upfront. The first one concerns the applicability of the ECI Directive for the healthcare sector. As widely known, the ECI Directive applies only to the energy and transport sector. In the past, this choice appeared already not fully aligned with EPCIP guidance documents which outlined the necessity to protect also other sectors concerning the critical infrastructures.¹¹ This inconsistency was highlighted as well by some authors, which explained that the result of the ECI Directive should have been regarded as a temporary result, a compromise that has been reached at EU level in order to reach as fast as possible a common strategy among the Member States for the protection of critical infrastructures.¹² The ECI Directive itself indicated that it ‘should be reviewed with a view to assessing its impact and the need to include other sectors within its scope, among other things, the information and communication technology (‘ICT’) sector’¹³. Following this path, in 2019 the European Commission (in its working document on the ECI Directive evaluation) went further and noticed that ‘the limited sectoral scope of the Directive means that it does not fully account for growing cross-sectoral interdependencies.’¹⁴ This eventuality represents a crucial challenge and thus, opportunity for the ECI Directive revision. In this regard, possible scenarios for the ECI Directive would imply expanding its scope either maintaining a sector-specific approach or adopting a cross-sectoral one. Both scenarios would represent a positive opportunity for ECI protection in the EU. If this might prove right, caution should be paid, however, in order not to result in overlapping with the NISD.¹⁵

The second challenge, inherently linked to the previous one concerns the consideration at a national level of healthcare within the critical infrastructures sectors. Member States adopted different approaches in their national CIP strategies – from sectors, to cross-sectors to critical processes. This has impacted healthcare, too. As the research in SAFECARE showed, the Member States across Europe have adopted different approaches towards healthcare CIP, and some Member States do not consider healthcare as a critical sector. The study of the CIP framework for the SAFECARE pilot cases (France: Assistance Publique-Hôpitaux de Marseille (AP-HM); the Netherlands: Academisch Medisch Centrum (AMC); and Italy: Azienda Sanitaria Locale Torino 5 (ASLTO5)) underlined this evidence. By way of example, the SAFECARE D3.9 report outlined that, while France included healthcare in its twelve sectors for critical infrastructures, the same did not appear for the Netherlands, which recently reformed its CIP framework changing from a ‘sector approach’ to a ‘process approach’. These views are further corroborated

⁷ See SM Rinaldi, JP Peerenboom, and TK Kelly, ‘Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies’ [2001] IEEE Control Systems Magazine 11.

⁸ For a wider illustration and analysis on the concepts of Critical Infrastructures (CI) and Critical Information Infrastructure (CII) see: E. Biasin, D. Bresic, P. Notermans, E. Kamenjasevic, SAFECARE Deliverable: D3.9 Analysis of ethics, privacy, and confidentiality constraints (2019), <https://www.safecare-project.eu/?p=465>, 42-50.

⁹ Link subsidiarity principle.

¹⁰ Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 [2019] OJ L 151/15 (Cybersecurity Act).

¹¹ Commission Staff Working Document on the ex post evaluation of the ‘Prevention, Preparedness and Consequence Management of Terrorism and other Security related risks’ 2007-2013 Programme (CIPS). Accompanying the document Report from the European Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions ex post evaluation for the period 2007 to 2013 of actions financed by the ‘Prevention and fight against crime’ programme (ISEC) and the ‘Prevention, Preparedness and Consequence Management of Terrorism and other Security related risks’ programme (CIPS) SWD(2018) 331 final Annex 8.

¹² Luisa Franchina, ‘Le infrastrutture critiche nazionali ed Europee’ [2012] Quaderno n. 3 I quaderni del Network AIAS 1, 15.

¹³ ECI Directive, recital 5.

¹⁴ Commission, ‘Evaluation of Council Directive 2008/114 on the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection’ SWD(2019) 308 final (Commission Evaluation Report), 20.

¹⁵ Risks were already pointed out in a study commissioned by the EC in 2018. For a broader analysis, see: EY, RAND, *Evaluation study of Council Directive 2008/114 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection*, 25.

by previous EU projects in the field of healthcare critical infrastructures,¹⁶ who found that Member States' protection level for healthcare CI remains uneven. The review of the ECI Directive could play a role in ensuring a convergent approach by Member States for CIP.

Regulatory challenges and opportunities for CIIP in healthcare: the NIS Directive

The NIS Directive is relevant for SAFECARE as the users of the technology to be developed will be healthcare providers. According to the NIS Directive, healthcare providers may be identified by at a national level as 'Operators of Essential Services', which have to ensure the security of their networks and information systems.¹⁷ Throughout the project, we have analysed the key aspects of the NIS Directive and its implementation in Europe. In light of these, several challenges could be enlisted.¹⁸ This section reports some of these. A first challenge relates to the implementation of the NIS Directive. The NIS Directive is an EU regulatory instrument that – likewise the ECI Directive – needs an implementative act by the Member States. Namely, NIS Directive's objective is to provide minimum harmonisation for the protection of network and information systems with a margin for the Member States to develop further requirements on a national level.¹⁹ After being approved in 2016, the NIS Directive had to be transposed across the Member States before May 2018. However, the NIS Directive was not timely implemented in all MS before the May 2018 deadline. This brought adverse effects for many stakeholders willing to put in place the necessary measures foreseen by the EU law and national law.²⁰ Another challenge resides in national-level methodologies chosen by the Member States for the identification OES. Member States adopted different methodologies which led to the incoherent application of the NIS Directive within the Union.²¹ As the EC puts it, such kind of scenario may have possible consequences for the whole internal market and the effective handling of cyber-dependencies.²² Finally, having regard to sector-specific legislation, it is worth to recall new challenges posed by medical devices cybersecurity regulation in the EU.²³ Risks of duplication with medical devices legal requirements on serious incidents²⁴ and GDPR²⁵ data breach requirements may arise. In this regard, it should be observed that simplification and cooperation mechanisms amongst competent authorities should be strengthened, to diminish burdens for healthcare organisations, as well as manufacturers.

5. Conclusions

Purpose of this contribution was to outline healthcare CIP regulatory challenges for policy-makers for the year 2020. The results achieved through research carried out for the SAFECARE project showed a wide array of challenges and opportunities. Concerning CIP: in the revision of ECI Directive, EU policy-makers should consider whether to include healthcare in the scope of the Directive; or, if a cross-sector approach is chosen, risks of overlapping with the NIS Directive should be avoided. Concerning cybersecurity: the effectiveness of implementation and coordination efforts at a national level needs to be monitored closely, to avoid risks of diverging application of the NIS Directive, (as it would bring thus detrimental effects to the EU internal market). Finally, as regards healthcare-specific legislation (notably, medical device law): more substantial alignment is needed with new cybersecurity pieces of regulation – such as the NIS Directive, and the others.²⁶

¹⁶ THREATS, 'An Analysis of Critical Infrastructure Protection Measures Implemented within the European Union: Identifying which European Member States includes the Health Sector as part of Critical National Infrastructure and which facets of Health Infrastructure are considered Critical' [2014] Report No: DR/1/001 <<http://www.threatsproject.eu/WP1%20D1%20final.pdf>>.

¹⁷ For the definition of OES, see NIS Directive, art 4(4).

¹⁸ For a more detailed debrief see also SAFECARE deliverables and publications. See E Biasin et al, SAFECARE D3.9 Analysis of ethics, privacy, and confidentiality constraints (SAFECARE, 2018) <<https://www.safecare-project.eu/?p=465>> accessed 30 September 2020. See also E Maia et al, 'Security Challenges for the Critical Infrastructures of the Healthcare Sector' in J Soldatos et al (eds), *Cyber-Physical Threat Intelligence for Critical Infrastructures Security: A Guide to Integrated Cyber-Physical Protection of Modern Critical Infrastructures* (Now Publishers 2020) 142–165.

¹⁹ NIS Directive, art 1.

²⁰ See *ibid*, 148.

²¹ See Commission, 'Report from the Commission to the European Parliament and the Council assessing the consistency of the approaches taken by Member States in the identification of operators of essential services in accordance with Article 23(1) of Directive 2016/1148/EU on security of network and information systems' COM(2019) 546 final, 22.

²² *ibid*. Also, see Maia et al (n 17), 27 fn 8.

²³ For a broader overview, see also: E Biasin, E Kamenjašević 'Cybersecurity Of Medical Devices. Regulatory challenges in the EU' [*forthcoming*, 2020]; E Biasin 'Medical devices cybersecurity a growing concern?' (*CITiP Blog*, September 2019) <<https://www.law.kuleuven.be/citip/blog/medical-devices-cybersecurity-a-growing-concern/>> accessed 30 September 2020.

²⁴ Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC [2017] OJ L 117/1 (MDR), art 87.

²⁵ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4 May 2016, art 33.

²⁶ For broader remarks on regulatory overlaps for medical devices and the CSA, see E Biasin, Kamenjašević (n 23).