COMPUTER LAW & SECURITY REVIEW 41 (2021) 105502

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/CLSR

Computer Law & Security Review

Comment

The regulatory framework for the protection of critical infrastructures against cyberthreats: Identifying shortcomings and addressing future challenges: The case of the health sector in particular

*Dimitra Markopoulou**, *Vagelis Papakonstantinou*

Faculty of Law & Criminology, Vrije Universiteit Brussel (LSTS), Pleinlaan 2, 1050 Brussels, Belgium

A B S T R A C T

The concept of "Critical Infrastructures" is constantly evolving in order to reflect current concerns and to respond to new challenges, especially in terms of (cyber)security and resilience. Protection of critical infrastructures against numerous threats has therefore developed into a high priority at national and EU level. During the last two decades a new type of threat has prevailed in the Critical Infrastructure threat landscape, that of cyberattacks; Protection against them is the primary focus of this paper. In order to do so the analysis first aims to drop some light into the differences between Critical Infrastructures and Critical Information Infrastructures, terms that are often confused, and to indicate possible inadequacies in the applicable protection regulatory regime. Finally, the health sector has been chosen as a sector-specific case in an effort to demonstrate how protection of a Critical Infrastructure, challenged as it has been with a constantly increasing number of cyber incidents, could be sufficiently protected in the new digitalised era.

1. Introduction

The concept of "Critical Infrastructures" is constantly evolving in order to reflect current concerns and to respond to new challenges, especially in terms of security and resilience. At the same time, over the last decades, the number and variety of Critical Infrastructures have increased significantly, whereas their protection against numerous threats and the safeguarding of their uninterrupted operation has developed into a high priority at national and EU level. Disruption or destruction of their operation may be the result of natural disasters (earthquakes, floods), mechanical failures, poor design and human actions ranging from a simple theft or arson to a terrorist attack. Operators of Critical Infrastructures, both public and private entities, have, over the years, taken measures to protect their Critical Infrastructures against different types of attacks. The complexity of the attacks and the vulnerabilities of the infrastructures, however, indicate the need for constant alert from both operators and governments in order

* Corresponding author.
E-mail addresses: Dimitra.Markopoulou@vub.be (D. Markopoulou), Evangelos.Papakonstantinou@vub.be (V. Papakonstantinou).

https://doi.org/10.1016/j.clsr.2020.105502

to develop and implement updated policies for the protection of their Critical Infrastructures.[1]

The 9/11 terrorist attacks demonstrated the vulnerability of the USA's Critical Infrastructures to the threat posed by a terrorist attack of this magnitude. The catastrophic consequences that these attacks had in the operation of Critical Infrastructures and the provision of critical services resulted to the birth of Critical Infrastructure protection as a distinctive policy area in the US and provided significant motivation to all stakeholders worldwide to review their Critical Infrastructures Protection policies in order to strengthen the existing instruments. It was the 9/11 attacks that attributed a national security element to the definition of critical infrastructures, taking it a step forward from the traditional public sector approach. At European level, the first coordinated steps to this direction were made in 2004, following the terrorist attacks in Madrid, when the Commission published its Communication on Critical Infrastructure Protection in the fight against terrorism,[2] followed by the release in 2006 of the first European Programme for the Protection of Critical Infrastructure.[3]

During the last two decades a new type of threat has prevailed in the Critical Infrastructure threat landscape, that of cyberattacks. Recent years have seen a dramatic increase in the volume of cyber threats, as well as a diversity in both their nature and complexity. This new enemy brought to the surface the need to protect the Information and Communication Technologies (ICT) that constitute the backbone of Critical Infrastructures.[4] The term used, when referring to these underlying systems and technologies is "Critical Information Infrastructure". Either as direct targets of a cyber threat or as a vehicle used by the cyber offender in order to reach the final targets, namely the Critical Infrastructure itself, Information and Communication Technologies constitute a vulnerable target. Safeguarding the uninterrupted operation of these systems and technologies is crucial for the uninterrupted operation of the Critical Infrastructures they support. Therefore, their protection, their availability and resilience against any kind of threats, has been placed in the centre of national and EU interest.

The first part of this paper examines the differences between Critical Infrastructures and Critical Information Infrastructures. The two terms appear, in many cases, to be used interchangeably despite their conceptual and actual differences. The EU applicable regulatory framework for the protection of Critical Infrastructure and Critical Information Infrastructure will also be addressed in this analysis. Even though the current protection regime adopts an "against all-hazards approach", this paper focuses on the protection of the infrastructures against cyber threats and examines the effectiveness of the existing regulatory measures. Findings of the above analysis are subsequently exemplified in the second part of this paper while focusing on a specific field, that of the health sector. The health sector has been identified as one of the most important Critical Infrastructures, that has also been the target of a continuously increasing number of cyber incidents. Consequently, an assessment of its regulatory framework with an emphasis on security-related matters is expected to demonstrate in practice how specific measures and EU legislation on Critical Infrastructures apply in practice and help mitigate ever-increasing cyber threats.

2. The distinction between critical infrastructure (CI) and critical information infrastructure (CII): The role of industrial control systems (ICS)

2.1. *Defining critical infrastructures: What does "critical" mean?*

What do we mean by "Critical Infrastructures"? An official introduction to the term was made by the Commission in its Communication on Critical Infrastructure Protection in the fight against terrorism that was published in 2004 :[5] "*Critical infrastructures consist of those physical and information technology facilities, networks, services and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments in the Member States. Critical infrastructures extend across many sectors of the economy, including banking and finance, transport and distribution, energy, utilities, health, food supply and communications, as well as key government services*". Following the Commission's Communication, similar definitions on CIs may be found in different EU documents, all of which follow the same pattern. The definition that prevailed, however, and is used broadly until today, is the one included in the Council Directive 2008/114/EC[6]: "*critical infrastructure means an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions*".

A close look at the definitions provided above indicates that the characterisation of an infrastructure as "critical" is subjective and rests, to a large extent, to the Member State that suffers the consequences of a CI's failure. What therefore constitutes a CI in a Member State, may not be identified as such in another one, since not all sectors are relevant for all countries. Furthermore, based on the special char-

[1] See, for example, ENISA's CIIP Governance in the European Union Member States (Annex), January 2016 https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/ciip-governance-in-the-eu-annex

[2] See Communication from the Commission to the Council and the European Parliament - Critical Infrastructure Protection in the fight against terrorism, COM/2004/0702.

[3] See Communication from the Commission on a European Programme for Critical Infrastructure Protection, COM/2006/0786.

[4] On the emergence of cyberattacks see also Onyeji I. Bazilian M. & Bronk C., Cyber Security and Critical Energy Infrastructure, The Electricity Journal, Volume 27, Issue 2.

[5] See above footnote 2.

[6] See Council Directive 2008/114/EC, of 8 December 2008, on the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection.

acteristics of each country, the list may need to be enriched with new sectors. While this divergence is justified, the freedom afforded to Member States entails a risk that ranges from overregulating sectors that do not need additional protection, with any inflexibility that this may cause, to underregulating others, where stricter security requirements would be critical for the continuity of their operation. The introduction therefore of some EU-wide standards and of a CI identification process that would be used as a guide by all Member States was deemed necessary.[7]

In this context the most frequently listed examples of CIs in EU documents, with some variations in terminology, encompass the sectors of banking and finance, government services, telecommunication and information and communication technologies, emergency and rescue services, energy and electricity, health services, transportation, logistics and distribution, and water supply. The list is, however, indicative. As regards the next step, namely the identification and designation by Member States of specific national CIs within their territories, guidelines are provided in order to achieve uniformity at EU level to the greatest extent possible. Therefore, each Member State must do so based on national predefined criteria, which however must be developed with minimum requirements in mind as these are included in official EU guidance. The Commission's Communication on a European Programme for Critical Infrastructure Protection, for instance, suggests the application of qualitative and quantitative effects of the disruption or destruction of a particular infrastructure as indicative for its characterisation as "Critical": The scope (meaning the extent of the geographic area which could be affected by its loss or unavailability) and severity in terms of public effect (eg. number of population affected), the economic effect (significance of economic loss and/or degradation of products or services), as well as, the environmental effect, political effects, psychological effects, or public health consequences.[8] The 2008 Directive on the identification of European Critical Infrastructures (ECIs)[9] also attempts to set some basic standards as regards identification and designation of ECIs through the adoption by all Member States of a common procedure.[10] However, the provisions of the Directive have a limited scope because they refer exclusively to ECIs, as these are defined in its text, thus leaving national infrastructures outside its scope. The NIS Directive,[11] on the other hand, has a broader application as it applies to all Operators of Essential Services; In practice, it describes the process Member States should follow for the identification of Operators of Essential Services[12] in an effort to introduce uniformity.[13]

2.2. *Defining critical information infrastructures*

There is no straightforward approach when it comes to defining a "Critical Information Infrastructure". From a legal perspective at least, the differences between the two terms are not obvious, and, until today, even though definitions of both terms can be found in official documents, there are few clear references regarding their relationship. On the contrary both terms are sometimes used interchangeably and when this is not the case, there is a considerable amount of overlap in their use.[14] According to Brunner and Suter "*The definition of exactly what should be subsumed under CI, and what should come under the heading of CII, is another question: Generally, the CII is that part of the global or national information infrastructure that is essentially necessary for the continuity of a country's critical infrastructure services. The CII, to a large degree, consists of, but is not fully congruent with, the information and telecommunications sector, and includes components such as telecommunications, computers/software, the internet, satellites, fibre-optics, etc. The term is also used for the totality of interconnected computers and networks and their critical information flows*".[15] Dunn, refers to CI and CII as follows: "*That the two concepts are closely interrelated is apparent from the current debate in protection necessities: the debate jumps from a discussion of protecting critical physical infrastructure to talk of protecting data and software residing on computer systems that operate these physical infrastructures. This indicates that the two cannot and should not be discussed as completely different concepts. Rather CIIP seems an essential part of CIP: While CIP comprises all critical sectors of a nation's infrastructure, CIIP is only a subset of a comprehensive protection effort, as it focuses in the critical information infrastructure*".[16]

Definitions of both terms can be found in different EU official documents. ENISA refers to Critical Information Infrastructure Protection in its 2016 report on the protection of CII.[17] [18] ENISA understands CII as part of a CI and more particu-

[7] See also Coroiu V, European Critical Infrastructures, European Journal of Public and National Security, Issue 6, (2 of 2015)/Volume II.

[8] See Communication from the Commission on a European Programme for Critical Infrastructure Protection, COM/2006/0786 final.

[9] See Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection

[10] A specific procedure is included in the Directive's Annex III.

[11] See 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.

[12] See article 5 of the NIS Directive and relevant analysis in Section 3.3 below.

[13] On the definition of CI see also Cedervall Lauta K., Regulating a Moving Nerve-On legally defining Critical Infrastructure, European Journal of Risk Regulation, 176 (2015)

[14] See Hyslop M., Critical Information Infrastructures, Resilience and Protection, Springer 2007.

[15] See Brunner E & Suter M, International CIIP Handbook 2008/2009: An Inventory of 25 National and 7 International Critical Information Infrastructure Protection Policies, CSS ETH Zurich.

[16] See Dunn Cavelty M, The socio-political dimensions of Critical Information Infrastructure Protection (CIIP), The International Journal of Critical Infrastructures 1 (2/3): 258-268, January 2005.

[17] See ENISA's report on Stocktaking, Analysis and Recommendations on the Protection of CIIs, January 2016, https://www.enisa.europa.eu/publications/stocktaking-analysis-and-recommendations-on-the-protection-of-ciis

[18] ENISA in particular states that "*CIIP can be seen as an essential part of the comprehensive efforts for CIP. While CIP covers the protection of a nation's infrastructure across various sectors, CIIP focusses on the protection of the underlying information infrastructure. CII is comprised of a physical component (networks, wires, satellites, computers etc.) and*

larly as the underlying information infrastructure. Another definition is introduced by the Commission's Green Paper.[19] [20] The OECD, on the other hand, in its 2008 Recommendation,[21] defines CII as "*those interconnected information systems and networks, the disruption or destruction of which would have a serious impact on the health, safety, security, or economic well-being of citizens, or on the effective functioning of government or the economy*". What may be concluded by these definitions is that CIs are complemented by CIIs, which are perceived as a sub-segment of CIs, in particular as the ICT systems that support their operation.

The realisation that ICT systems, services and networks form a vital part of the European economy and society placed the ICT sector's protection high on the European priorities' agenda early on. As early as 2005 the ICT sector was perceived as a CI, when the Commission published its Green Paper and the ICT was listed as one of the CI sectors that should fall under the European protection programme.[22] ICTs could either be perceived as CIs themselves, through provision of essential goods and services, or as the underpinning platform of other CIs. In either case their protection is of the essence. The need to give a priority to the ICT sector was also identified by the Commission's Directive on European Critical Infrastructures.[23] In its text it is stated that, in the event of considering of adding additional sectors under the Directive's scope during the review process, the ICT sector should be first in the list – however the Directive is still under review. The Commission needed however another four years (since the Green Paper) to move from these simple references to specific legislative measures that addressed CIs' protection separately.[24] This effort led eventually to the adoption of the NIS Directive and the implementation of a more consistent European approach on the protection of network and information systems.

In practice, the argumentation regarding the differences or overlaps between the two terms should not be limited to a theoretical evaluation of their contents. A more precise and consistent reference to each in the relevant EU and Member State documentation could contribute to better identification by operators of CIs and/or CIIs respectively of the risks their infrastructures are up against. Ultimately, it would contribute to a more targeted implementation of protection measures depending on their recipients, based on whether these are the physical facility and asset or the information technology facility that supports it. This is exemplified in Part 4 of this analysis: The eHealth sector is an example of lack of uniformity, whereby lack of clarity is noted as early as regarding its own identification as a CII. Even in these cases where the eHealth sector has indeed been identified as a critical sector, still ongoing debates question whether it should be considered a CII itself or part of another CI, such as the broader health sector or, even, the ICT sector.[25]

2.3. *Integration of industrial control systems into critical infrastructures: Why are these systems so vulnerable?*

Most CIs nowadays such as energy, oil and gas, water, transportation systems, manufacturing facilities are controlled and monitored by Industrial Control Systems (ICS). ICS is a general term describing industrial automation systems responsible for data acquisition, visualization and control of industrial processes, often found in various industrial sectors and CIs. ENISA notes in a report released in 2015 that "*the ICS-SCADA environment is the fundamental component of European and national Critical Infrastructures*".[26] Over the last years a constantly increasing number of cyberattacks against these systems has been identified, which has highlighted the security of ICS as a high priority area among CIs' operators.[27] At the same time, their complexity and the high level of preparedness of the cyber offenders are additional parameters that raise concerns as regards their safety.[28]

There are basically two factors that have contributed to the targeting of ICS. The first is directly related to the indispensable contribution of ICSs to the operation of CIs and the severe consequences a successful attack could have. The bigger the damage the stronger the motivation for a cyberattack. The other refers to the vulnerabilities of the ICS, which, in many cases, make them a soft target. More specifically, ICS currently use open architectures and are often connected to external systems such as office systems. From being isolated systems running proprietary software and control protocols, thus having little resemblance to traditional information systems, they have begun to resemble the more traditional information systems. Increasingly, ICS use the same commercially available hardware and software components, which is translated to significantly less isolation from the outside world, introduc-

an immaterial component, which is the actual information transported by and through the physical components"

[19] See Green Paper on a European programme for critical infrastructure protection, COM/2005/0576 final, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52005DC0576&from=EN

[20] In the Green Paper Critical Information Infrastructure is defined as "*Information and Communication Technology systems (ICT) that are critical infrastructures for themselves or that are essential for the operation of critical infrastructures (telecommunications, computers/software, Internet, satellites, etc.)*. The same document defines Critical Information as "*specific facts about a critical infrastructure asset, vitally needed to plan and act effectively, so as to guarantee failure or cause unacceptable consequences for critical infrastructure installations*".

[21] See OECD Recommendation of the Council on the Protection of Critical information Infrastructures, C (2008) 35.

[22] See footnote 18.

[23] See footnote 5.

[24] See Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, on Critical Information Infrastructure Protection, COM/2009/149, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF

[25] See below 4.2.4.

[26] See ENISA's report on Analysis of ICS-SCADA Cyber Security Maturity Levels in Critical Sectors, December 2015, https://www.enisa.europa.eu/publications/maturity-levels

[27] According to Symantec in 2015, there were at least 135 public vulnerabilities reported, a significant increase considering that in 2014 only 35 ICS-related vulnerabilities were disclosed. Also, Kaspersky labs released Threat Landscape for H1 2018, according to the report the attacks increased by 41% percentage targeting ICS computers attacked when compared to H1 and H2 of 2017, https://gbhackers.com/ics-systems-attacks/

[28] The Aurora vulnerability and Stuxnet are examples of advanced and well-prepared attacks.

ing many of the same vulnerabilities that exist in current networked information systems.[29] As noted by ENISA "*Today ICS products are mostly based on standard embedded systems platforms, applied in various devices, such as routers or cable modems, and they often use commercial off-the shelf software. All this has resulted in reduction of costs, ease of use and enabled the remote control and monitoring from various locations. However, an important drawback derived from the connection to intranets and communication networks, is the increased vulnerability to computer network-based attacks*".[30]

Despite, however, the above realisations, ICS have not attracted the EU interest as far as regulatory initiatives are concerned, as this will be demonstrated in the relevant section that follows.

3. The protection policies for CIs and CIIs against cyberattacks. What is the protection regime for industrial control systems?

3.1. *Setting the regulatory landscape*

Critical Infrastructures and their protection have been in the centre of EU regulatory efforts since 2004. The severe consequences a possible disruption or manipulation of CIs may cause has motivated all involved stakeholders to contribute to their protection against cyberattacks by reducing their vulnerabilities and enhancing their resilience. The first official step to this direction was taken in June 2004, when the European Council asked the Commission to prepare an overall strategy to protect CIs. At that time, the main concern was the protection against terrorist attacks.[31] The Commission responded immediately by publishing a Communication to the Council and the European Parliament.[32] The official definition of CIs, as well as the framework for implementing a European Programme for Critical Infrastructure Protection were included in this document. The Communication was followed by a Green Paper that was adopted by the Commission in November 2005.[33] Main purpose of the Green Paper was to receive feedback concerning a possible European Programme on Critical Infrastructure Protection policy options by involving a broad number of stakeholders. The Green Paper introduced the notion of EU CIs, thus paving the way for the adoption of the main legislative EU instrument on this matter, the Directive on European Critical Infrastructures.[34]

An overall policy approach and the framework for Critical Infrastructure Protection activities in the EU was presented by the Commission in its EPCIP Communication issued in December 2006.[35] The European Programme for Critical Infrastructure Protection (EPCIP), while recognising the threat from terrorism as a priority, aimed to respond to all kind of threats, including criminal activities as well as natural disasters and other causes of accidents, using an "all-hazards" approach. Together with the Communication, the Commission presented a proposal for a Directive on the identification and designation of European Critical Infrastructures and a common approach to assess the need to improve their protection.[36] The Directive was officially published in December 2008 and it will be briefly presented in the section that follows.

Even after adoption of the Directive, however, protection of CIs and of CIIs remained in the centre of the Commission's interest. In 2009, the Commission adopted a Communication on Critical Information Infrastructure Protection setting out a plan (the CIIP Action Plan) to strengthen the security and resilience of vital Information and Communication Technology (ICT) infrastructures. The Communication focused on strengthening the security and resilience of CII, thus turning the interest to the information society.[37] [38] The emphasis on the security of CIIs was consistent with the debate launched at that time at the request of the Council and the European Parliament, to address the challenges for network and information security, a debate that, several years later, resulted in the NIS Directive.[39] In 2011 a new Communication was released by the Commission, which focused on the evaluation of the achievements and next steps of the CIIP Action Plan.[40] A new

[29] For vulnerabilities of Industrial Control Systems see also Alcare C. & Zeadally Sherali, in Critical Infrastructure Protection: requirements and challenges for the 21st century, International Journal for Critical Infrastructure Protection 8 (2015), 53-66.

[30] See ENISA's report on Protecting Industrial Control Systems, Recommendations for Europe and Member States, https://www.enisa.europa.eu/publications/protecting-industrial-control-systems.-recommendations-for-europe-and-member-states.

[31] See also Coman I., Cross-Border Cyber-Attacks and Critical Infrastructure Protection, International Journal of Information Security and Cybercrime, 6(2), 47 (2017)

[32] See Communication from the Commission to the Council and the European Parliament - Critical Infrastructure Protection in the fight against terrorism, COM/2004/0702 final, https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=celex:52004DC0702.

[33] See Green Paper on a European programme for critical infrastructure protection, COM/2005/0576 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52005DC0576.

[34] See Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32008L0114.

[35] See Communication from the Commission on a European Programme for Critical Infrastructure Protection, COM/2006/0786 final, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52006DC0786).

[36] See Proposal for a Directive of the Council on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection, COM/2006/0787, https://eur-lex.europa.eu/legal-content/BG/TXT/?uri=CELEX:52006PC0787.

[37] See Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, on Critical Information Infrastructure Protection, COM/2009/149, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF.

[38] See also Satola D. & Luddy W.J., The potential for an international legal approach to Critical Information Infrastructure protection, Jurimetris 47, no 3, (2007)

[39] 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, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

[40] See Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Informa-

approach on the EPCIP plan, was incorporated in the Commission's Staff Working Document, that was adopted in 2013 to take account of increasing cross-border interdependencies.[41] [42]

3.2. *The 2008 directive on European critical infrastructures*

The 2008 Directive is a key pillar of the Commission's EPCIP programme. The Directive constitutes a first step in an effort to identify and designate ECIs and to assess the need to improve their protection. One critical point that needs to be made before examining the Directive's specific provisions concerns its scope. The Directive adopts a sector-specific approach, limiting its implementation to the energy and transport sectors only leaving thus outside its scope several policy sectors such as the health sector or the drinking water supply and distribution sector or the financial sector. This limitation is acknowledged in its text, where it is specifically mentioned that, by the time of its review, subsequent sectors may be identified, with a priority to be given to the ICT sector.[43] Given that both the Green Paper and the Proposal for the Directive include in their Annexes a list of eleven different CI sectors, it is interesting to note that the regulator decided against a more extensive list. A possible explanation could be that these two sectors were selected on a trial basis and that the list would be expanded together with the Directive's review which was due for the year 2012.[44] However, even though the process of reviewing commenced in 2012, it has not been completed until today.

Another issue that needs special attention is that the Directive focuses specifically on European Critical Infrastructures, namely infrastructures that are critical from a European perspective, *i.e.* where their disruption or destruction would have a significant impact on at least two Member States. In other words, not all CIs fall under the Directive's scope but rather a limited category that fits its definition.[45] While it is indeed true that the Directive was perceived in the context of the European Programme for Critical Infrastructure Protection, thus aiming protection at EU level, nevertheless it is also true that it ended up being a regulatory instrument of a very limited scope, that eventually left national CIs unregulated at EU level until such a late time as in 2016, when the NIS Directive came into force.[46]

As far as the specific provisions of the Directive are concerned, the Directive requires each Member State to identify the CIs that may be designated as European Critical Infrastructures within its territory. The identification procedure is described in Annex II of the Directive. Once an ECI is identified, the Member State needs to communicate it to any other Member State which may be affected by its disruption in order to reach an agreement regarding its designation. The process may be initiated by a Member State which believes that is significantly affected by a potential European Critical Infrastructure but has not been identified as such by the Member State on whose territory the same is located. As a next step, the Directive requires a specific set of actions to be taken by the CI's owner/operators in order to develop an Operator Security Plan. Minimum requirements for such a plan are incorporated in Annex III of the Directive. Provisions for establishment of a Security Liaison officer are included in the Directive: The Security Liaison officer is to function as the point of contact for security related issues between the owner/operator of the CI and the relevant national authority.[47]

Despite therefore its innovative character the Directive introduces a generic approach regarding protection of CIs. Its efficiency is examined in the Commission Staff Working Document published in June 2012.[48] The document presented a strong perception by Member States that implementation of the Directive did not result in sufficiently clear and tangible improvements to ECIs security levels. Basic fact supporting this view was that few European Critical Infrastructures had been identified and very few Operator Security Plans had been produced until then. Despite though however the existence of contradicting opinions on the actual improvement of security, Member States reached a near consensus on the added value of side-effects of the Directive, such as increased awareness and cooperation. Furthermore, it was supported that the very existence of a legal instrument nurtured policies on the protection of national CIs.

Same conclusions were adopted in the Commission's evaluation roadmap on the Directive that was released in March 2018.[49] among others, it was observed that, even though the Directive was quickly transposed in the national laws of Member States, its application remained limited. Furthermore, wide discrepancies in the application of the Directive among Member States were pointed out: For instance, at the time of publication of the evaluation the vast majority of CIs were designated by two Member States only (approximately 60% of the total number of designations), and primarily in the energy sector. As of August 2018, the Member States had designated ninety-three European Critical Infrastructures; Of these,

tion Infrastructure Protection 'Achievements and next steps: towards global cyber-security, COM/2011, 163 https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0163:FIN:EN:PDF

[41] See Commission Staff Working Document on a new approach to the European Programme for Critical Infrastructure Protection Making European Critical Infrastructures more secure, SWD/2013, 318, https://ec.europa.eu/energy/sites/ener/files/documents/20130828_epcip_commission_staff_working_document.pdf

[42] See also Pursiainen C., The Challenges for European Critical Infrastructure Protection, Journal of European Integration, 31:6, 721-739

[43] See article 3 par.3 of the 2008 Directive

[44] See article 11 of the 2008 Directive

[45] See also van Asselt M, Vos E. & Wildhaber I. in "Some Reflection on EU Governance of Critical Infrastructures Risks", European Journal of Risk regulation (EJRR), 6(2), 185-190

[46] See footnote 10.

[47] See also Lazari A & Simoncini M., Critical Infrastructure Protection beyond compliance. An analysis of National Variations in the implementation of Directive 114/08/EC, Global Jurist 267 (2016)

[48] See Commission's Staff Working Document on the review for the European Programme for Critical Infrastructure Protection, SWD/2012, 190, https://ec.europa.eu/home-affairs/sites/homeaffairs/files/pdf/policies/crisis_and_terrorism/epcip_swd_2012_190_final.pdf

[49] See evaluation roadmap, Evaluation of the 2008 European Critical Infrastructure Protection Directive

eighty-eight were in the energy sector and five in the transport sector.

On July 2019 the Commission published its latest evaluation of the Directive.[50] Among the conclusions presented were that the Directive appears to have partial relevance in view of recent technological, economic, social, policy/political and environmental developments and the challenges they entail. Also, the limited sectoral scope of the Directive means that it does not fully account for growing cross-sectoral interdependencies. As regards its effectiveness, the evaluation concluded that the Directive has been partially effective in achieving its stated objectives, namely the establishment of a common ECI identification and designation procedure. It remains therefore to be seen, once the process of reviewing the Directive will have been concluded, how these challenges will be addressed in the updated document.[51]

3.3. *The NIS directive and the role of Enisa in protecting critical infrastructures against cyberthreats*

When it comes to cyber resilience and protection of CIs against cyberthreats, in particular of the network and information systems that support their operation, the NIS Directive should be taken into consideration. The NIS Directive does not make any explicit reference to CIs, it makes use however the term "Essential Services" which should be considered equivalent. Operators of Essential Services, as recipients of the Directive's requirements, include all public or private entities that provide a service which is essential for the maintenance of critical societal and/or economic activities.[52] The type of entities that fall under the definition of the NIS Directive for Operators of Essential Services, more or less, coincides with the indicative list of Critical Infrastructure sectors included in the relative European documents on Critical Infrastructure Protection. A thorough analysis of the NIS Directive's scope and provisions lays beyond the purpose of this document; Here it is enough to be noted that the NIS Directive, which was adopted in 2016 and entered into force in May 2018, currently is the main EU cybersecurity legal instrument addressed to Member States in order for them to warrant high levels of protection for network and information systems supporting, among others, the operation of CIs and the provision of critical/essential services.

ENISA, from its part, has recognised the significant impact cyberattacks may have on CIIs and related services. ENISA shares the opinion that identification of a CII is the first step in the process to secure and protect the availability of critical assets. In this context, it has published several reports on the identification of CIIs and their protection ;[53] [54] In addition, ENISA has developed a series of guidelines in order to assist Member States to implement the NIS Directive, including a tool that maps security measures for Operators of Essential Services to international standards,[55] as well as, a report on mapping of Operators of Essential Services' security requirements for specific sectors, including the health sector that will be thoroughly presented below.[56] ENISA's role in supporting the NIS Directive's implementation and in contributing to increasing cybersecurity capabilities at Union level was further reinforced by the Cybersecurity Act.[57] Among the objectives of the new Regulation, which came into force on 27th June 2019, is the strengthening of ENISA's role by granting to it a permanent mandate and the development and implementation of Union policy on cybersecurity certification of ICT products, ICT services and ICT processes.

3.4. *Protection of industrial control systems*

As seen above, CIs and CIIs have been extensively addressed at EU level and different policy areas have been developed to this effect. ICS' protection, however, is not addressed explicitly in any of the EU's relevant official documentation. Given the critical role of ICS in the uninterrupted operation of many European and national CIs, the lack of specific measures that could contribute to their protection is considered a significant omission.[58]

ENISA, having identified this regulatory gap, published in 2011 a study on protecting ICS.[59] The study aims to identify threats, risks and challenges in the area of ICS protection, as well as, to recognize national, European and international initiatives on ICS security. The first challenge identified in the report is the lack of specific initiatives on ICS security in combination with the lack of a European reference with regard to se-

[50] See Commission's Staff Working Document Evaluation of Council Directive 2008/114, SWD/2019/310, https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20190723_swd-2019-308-commission-staff-working-document_en.pdf

[51] See also Lazari A., European Critical Infrastructure Protection, Springer International Publishing, 2014.

[52] See Article 4(4) of the NIS Directive.

[53] See ENISA's report on Stocktaking, Analysis and Recommendations on the protection of CIIs, January 2016, https://www.enisa.europa.eu/publications/stocktaking-analysis-and-recommendations-on-the-protection-of-ciis

[54] See ENISA's report on methodologies for the identification of Critical Information Infrastructure assets and services, February 2015, https://www.enisa.europa.eu/publications/methodologies-for-the-identification-of-ciis

[55] See https://www.enisa.europa.eu/news/enisa-news/enisa-launches-oes-tool-to-map-security-measures

[56] See ENISA's report on mapping of OES Security Requirements to Specific Sectors, January 2018, https://www.enisa.europa.eu/publications/mapping-of-oes-security-requirements-to-specific-sectors

[57] See 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 (Cybersecurity Act)

[58] See also Piggin R., Are industrial control systems ready for the cloud?, International Journal of Critical Infrastructure Protection, 9 (2015), 38-40

[59] See ENISA's report on Protecting Industrial Control Systems, Recommendations for Europe and Member States, https://www.enisa.europa.eu/publications/protecting-industrial-control-systems.-recommendations-for-europe-and-member-states

curity standards and guidelines. The report goes on to recommend actions that need to be undertaken in order to achieve the required level of ICS protection, such as reviewing the concept of ICS and their role when embedded into CIs, reviewing the threats that could affect these systems from a multitude of perspectives, describing the main differences between ICS and regular IT systems, listing the challenges to ICS security, summarising the current policy context under which the protection of ICS should be framed at EU level and in the US, and analysing the different technical solutions that are currently applied for protecting ICS.

4. Making the healthcare sector more resilient against cyber incidents: Emerging vulnerabilities and the applicable regulatory framework for its protection

4.1. *Hospitals under attack: Setting the (cyber) threat landscape*

Over the last years the healthcare sector has been challenged with a constantly increasing number of cybersecurity incidents. Ransomware, medjacking,[60] phishing (through targeting email addresses of physicians), medical devices tampering, denial of service,[61] and, even, cyberespionage are some examples of malicious actions targeting healthcare organisations and their ICT systems. These threats, if successful, may have disastrous consequences not only to the provision of healthcare services but also to the broader social and financial welfare. The Wannacry ransomware, for instance, devastated the UK NHS in 2017, hit international shipper Fedex and infected more than 300.000 computers in 150 countries. In the SingHealth attack, Singapore's worst cyberattack, hackers infiltrated the data bases of SingHealth, the largest group of healthcare institutions in the country, that eventually led to the theft of personal data of 1,5 million patients. The cyberattack against Anthem Insurance in 2015 had also serious consequences: As a result of this data breach, 79 million personal records were affected, including names, birthdays, medical IDs, and social security numbers.[62]

There are specific vulnerabilities and particularities of the healthcare industry that make it more attractive to cyber offenders and at the same time constitute it a *soft* target. First and foremost, the personal data that hospitals and healthcare organisations store in their systems consist mainly of heath data. Given the monetary value and the high sensitivity of medical data, many cyber offenders are motivated by financial gain, whereas others seek to obtain intellectual property or consumer information. Data theft therefore is one of the main cyberthreats health institutions are facing. According to research findings, healthcare data security incidents ranked second for the health services industry in 2016.[63] Another factor that contributes to the increase in the occurrence of cyber incidents targeting the health sector refers to the technological advancements. The health sector is becoming increasingly connected, whereas the integration of ICT systems in the health services and infrastructures has increased significantly over the last decades. In this rapidly advancing technological environment, traditional hospitals move to a smart hospital environment, thus introducing new capabilities in patient healthcare.[64] Furthermore, modern healthcare is dominated by an extensive network of connected medical devices, the use of which has changed the ICT landscape in the healthcare industry worldwide. ENISA mentions in its Guidelines for Cybersecurity in Hospitals that medical technology companies currently manufacture more than 500,000 different types of medical devices, such as wearables, implantable and stationary medical devices. The Internet of Medical Things market in Europe alone is expected to grow from 11 billion in 2017 to 40 billion in 2022, while the European medical technology market was estimated at roughly 115 billion in 2017.[65]

In addition, so-called "eHealth" is another digital development which has, during the past few years, developed into an important segment of the provision of health services overall. eHealth denotes the use of ICT in support of health and health-related services. The term is widely used to describe the interaction between patients and health-service providers ranging from patients' online access to basic data on their treatment to national schemes, like ePrescription services or cross border eHealth information sharing. Similarly, so-called "Mobile health" (mHealth) is a rapidly developing component of E-Health that covers "*medical and public health practice supported by mobile devices, such as mobile phones, patient monitoring devices, personal digital assistants, and other wireless devices*".[66] It particularly includes the use of mobile communication devices for health and well-being services and information purposes, as well as, mobile health applications. Over 97,000 mHealth apps are currently available across multiple platforms on the global market; Of these, 70% target consumers and fitness while 30% target health professionals.[67] [68]

[60] The difference between cryptojacking and medjacking is basically the kind of hardware involved. In the firstcase we are talking about general purpose IT infrastructure and in the second we are referring to IT-basedmedical equipment

[61] Denial of Service is a very common cyberattack that can take down servers at a healthcare organisation, especially because they are usually reluctant to use public cloud infrastructure, so the capacity of servers is limited. The impact can be high, depending on the type of systems affected

[62] See also Cashwell G., Cyber-Vulnerabilities & Public Health Emergency Response, Journal of Health Care and Policy, 21(1), 29-58.

[63] Symantec's 2017 Internet Security Threat Report (ISTR) found that reported breach incidents increased by 22 percent last year, rising to 328 from 269 in 2015

[64] "A smart hospital is a hospital that relies on optimised and automated processes built on an ICT environment of interconnected assets, particularly based on Internet of things (IoT), to improve existing patient care procedures and introduce new capabilities".

[65] See ENISA's Procurement guidelines for cybersecurity in hospitals, Good practices for the security of Healthcare services February 2020, https://www.enisa.europa.eu/publications/good-practices-for-the-security-of-healthcare-services

[66] See Commission's Green paper on mobile Health ("mHealth)", COM/2014/219, https://ec.europa.eu/transparency/regdoc/rep/1/2014/EN/1-2014-219-EN-F1-1.Pdf

[67] See https://research2guidance.com/wp-content/uploads/2015/08/Mobile-Health-Market-Report-2013-2017-Preview.pdf

[68] See also Niezen M., Unobtrusiveness in mHealth Design and Use: A Systematic Literature Study, in Adams S., Purtova N &

Digital transformation of healthcare and the use of electronic means to acquire, transfer or store healthcare related information and to provide services used by health professionals and patients/consumers has improved the provision of health services and is anticipated to increase the well-being of millions of citizens. At the same time the increased pace of digitalisation opens up "opportunities" for cyberattacks and consequently new challenges for cybersecurity. The adoption of a comprehensive and consistent EU regulatory framework that will address these new challenges and will introduce EU-wide standards for the provision of health services is therefore necessary. The EU has been intensively working to this effect since 2004, as elaborated in the section that follows.

4.2. *The regulatory framework to address (cyber)security requirements in the health sector*

The following analysis focuses on the main regulatory instruments applicable to the health sector, with a particular emphasis on those addressing (cyber)security issues in the provision of health services and the operation of health infrastructures. The regulatory framework presented here consists of both regulation of a horizontal scope which applies to the broader health sector, as well as, sector-specific legislation. *As regards the first category, healthcare is, without exception, listed as a CI in all relevant EU official documentation. Consequently, the regulatory framework on the protection of CIs, as elaborated in the first part of this analysis, finds full application on the health sector as well. At the same time, the provision of healthcare services is continuously dependent upon an ICT environment. Increased ICT deployment inevitably leads to greater ICT dependency and, in turn, to greater need for information security. Protection of the underlying information infrastructure of the health sector falls under the protection regime for CII, as this will be explained below where the perception of eHealth as a CII is being considered.. Accordingly,* healthcare providers have been identified as Operators of Essential Services, in the context of the NIS Directive, while eHealth has been characterised as a CII by most Member States. In addition to the general framework for the protection of CIs, the NIS Directive is the main regulatory instrument available to hospitals and healthcare organisations in order to minimise the security risks posed to their network and information systems. The General Data Protection Regulation[69] is also applicable (see the analysis that follows): Processing of health data is extensively addressed in its text, which introduces security requirements and specific obligations applicable to healthcare organisations, as data controllers.

At the same time the EU has been working on sector-specific legislation. In this context, two Regulations have been recently adopted by the Commission to strengthen the European regulatory framework for medical devices and *in vitro* diagnostic medical devices. Reference in this analysis to these Regulations is considered necessary for two reasons: First, they constitute an inseparable part of the EU regulatory framework on the health sector; Second, the increased dependency of their subject-matter (medical devices) on ICT and their exposure to cyber threats makes the discussion on their protection against cyberattacks relevant. Furthermore, a short presentation of the initiatives adopted at EU level on eHealth has been included in this paper. Even though there is no specific security parameter of the applicable framework in eHealth (including mHealth), this was considered necessary for picture completeness purposes, especially taking into account the ongoing discussion on the identification of eHealth as a CII, as this will be elaborated below.

4.2.1. *Health sector security requirements in the NIS directive*

As see above under 3.3. the NIS Directive constitutes, at the time being, the main legislative EU cybersecurity legal instrument at Member States' disposal in order to warrant a high level of protection for network and information systems that support, among others, the operation of CIs and the provision of critical/essential services. As regards the health sector, in particular, healthcare providers are listed among the entities identified in the NIS Directive's Annex as Operators of Essential Services.[70] As a result, hospitals and healthcare settings must implement the NIS Directive's security and notification requirements. In particular, they need to take appropriate and proportional technical and organisations measures to manage the risks posed to the security of network and information systems that they use in their operations and to prevent and minimise the impact of incidents affecting the security of such systems. The obligation to notify the competent authority of incidents having a significant impact on the continuity of the essential services they provide complements the set of obligations set under the NIS Directive for all entities operating within the health sector.

ENISA, in the same context as above, assisting Member States and organisations to implement the NIS Directive, has published a number of reports and guidelines for the health sector: Having recognised the significance of digital health networks as CII, it has developed actions focusing on the security challenges and risks faced by the health sector in Member States.[71] ENISA has also launched an "eHealth Security Experts Group" with the aim to create an active community to share information and exchange knowledge on this field.

4.2.2. *Health sector security requirements in the general data protection regulation*

The General Data Protection Regulation (GDPR) is particularly relevant in the health sector because essentially all or most of health data or medical records are "personal data" in the context of its provisions.[72] While a comprehensive analysis

Leenes R (Editors), Under Observation: The Interplay Between eHealth and Surveillance, Springer, 2017.

[69] See 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) .

[70] This is explicitly included in the types of entities that fall under the definition of operator of essential services. As further specified hospitals and healthcare settings and healthcare providers as defined in point (g) of Article 3 of Directive 2011/24/EU of the European Parliament and of the Council

[71] See Security and resilience in eHealth Infrastructures and Services, December 2015 and cybersecurity and resilience for Smart Hospitals, November 2016

[72] See article 4.1. of the GDPR

of health-related personal data processing under the GDPR lies beyond the purposes of this analysis, here it is only noted that hospitals and healthcare providers should, when processing patients' data, comply with the processing principles and other obligations provided in the GDPR. In essence, they must, as data controllers, take all appropriate technical and organisational measures to ensure and be able to demonstrate that the requirements of this Regulation are met, including the security of the processing.

In brief, as regards health data in particular, the GDPR aims to strike the right balance between the protection of individuals in relation to the processing of their personal data, which are by nature particularly sensitive, and the social welfare, in particular in the context of the management of health or social care services and systems. In this context, hospitals are excluded from the general rule of Article 9 of the GDPR, which prohibits any processing of special categories of data, on the grounds that processing of such data is carried out for certain health-related purposes by persons subject to a legal obligation of professional secrecy.[73] At the same time, however, the processing of special categories of personal data entails high risks for the data subjects. On these grounds, the GDPR provides a set of additional obligations to controllers that are engaged, among others, in processing on a large scale of special categories of data pursuant to Article 9, such as hospitals and healthcare providers. These organisations must therefore designate a Data Protection Officer,[74] carry out a data protection impact assessment[75] and notify a personal data breach likely to result in a risk to the rights and freedoms of individuals.[76] Security of processing is another obligation that burdens both the controller and the processor of personal data. According to Article 32 of the Regulation, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, such as pseudonymisation, encryption, ability to ensure confidentiality and to restore the availability etc.

The rapid development of eHealth, including mHealth, creates new challenges in terms of safeguarding the lawfulness of processing of the personal data collected through health apps and platforms and through the provision of digitalised health services as a whole. Exchange of personal data through the eHealth Digital Service Infrastructure for Cross-Border eHealth Information Services has been addressed in the Commission's Implementing Decision. In particular, it has been clarified that, as regards such processing, the Commission shall be regarded as data processor for patients' personal data, whereas the Member States shall be regarded as controllers.[77]

4.2.3. *The medical devices regulations*

It is undisputable that medical devices have dominated the health sector and that their use for the provision of health services is constantly increasing. Therefore, implementing regulatory schemes for medical devices is deemed necessary for the protection of public health and patient's safety. At the same time medical devices have developed a significant dependence on ICT systems for their operation, which makes them even more vulnerable to security risks, thus turning their safety into a priority for all involved stakeholders.[78] Medical device cybersecurity is a growing concern in light of the increasing number of cybersecurity incidents and data breaches. The new regulatory framework for medical devices aims to address these concerns by laying down a set of rules concerning the placing on the market, making available on the market or putting into service of medical devices for human use and accessories for such devices in the EU. The two new Regulations on medical devices and on *in vitro* diagnostic medical devices, Regulation 745/2017 (MDR) and Regulation 746/2017 (IVDR) entered into force in May 2017. The new Regulations will replace the existing regulatory framework for medical devices that consists of Directives 90/385/EEC and 93/42/EC. The MDR has a transition period of three years and will fully apply from 26 May 2020. The IVDR has a transition period of five years and will fully apply from 26 May 2022.[79]

As regards security issues in particular, the Regulations introduce specific provisions related to IT security for all medical devices. These security requirements are included in Annex I of the Regulations and deal with both pre-market and post market aspects. In particular, the Regulations make explicit reference to devices that "*incorporate electronic programmable systems and software that are devices themselves*". For these medical devices, manufacturers need to comply with specific design requirements in order to ensure repeatability, reliability and performance in line with their intended use.[80] Furthermore, whenever software is incorporated into medical devices it must be developed and manufactured in accordance with the state of the art, taking into account the principles of development life cycle, risk management, information security, verification and validation.[81] Another obligation imposed upon manufactures is to set out minimum requirements concerning hardware, IT networks and IT security measures, including protection against unauthorised access, necessary to run the software as intended.[82] As regards post-market measures, manufacturers need to implement a post-market surveillance system proportionate to the risk and appropriate to the type of device.[83] A notification obligation is

[73] See article 9 par. 2 (h)
[74] See article 37 of the GDPR
[75] See article 35 of the GDPR.
[76] See article 33 of the GDPR.
[77] See article 7 of Commission Implementing Decision 2019/1765 of 22 October 2019 providing the rules for the establishment, the management and the functioning of the network of national authorities responsible for eHealth, and repealing Implementing Decision 2011/890/EU .

[78] See Williams P. & Woodward A., Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem, Medical Devices: Evidence & Research, 20 July 2015.
[79] It is noted that safety aspects addressed by Directive 2014/30/EU of the European Parliament and of the Council are an integral part of the general safety and performance requirements laid down in this Regulation for devices. Consequently, this Regulation should be considered a lex specialis in relation to that Directive.
[80] See article 17.1 of Annex I of the MDR and article 16.1 of Annex I of the IVDR
[81] See article 17.2 of Annex I of the MDR and article 16.2 of Annex I of the IVDR
[82] See article 17.4 of Annex I of the MDR and article 16.4 of Annex I of the IVDR
[83] See article 83 of the MDR and article 78 of the IVDR

also provided under the new Regulations, according to which manufactures have to report any serious incidents involving devices made available on the EU market.[84] [85]

4.2.4. *E-health as a critical information infrastructure*

eHealth[86] has been in the centre of the EU agenda since 2004, when the first eHealth action plan was adopted.[87] Since then, the Commission and the Member States have been developing initiatives aimed at incorporating eHealth into their healthcare systems. Global statistics published by the WHO show that 58% of the Member States have an eHealth strategy, 55% of them have introduced legislation to protect electronic patient data and 87% of the same group of countries report having one or more national initiatives under development on mHealth. Improving cross border exchange of health data in particular and achieving interoperability of national eHealth systems have been treated as a priority at European level. Both initiatives are mainly supported by Directive 2011/24.[88] To attain its objectives the Directive established the eHealth network; The rules for the establishment, the management and the functioning of the eHealth Network were further clarified by the Commission's Implementing Decision 2019/1765.[89] In 2012 the Commission published the eHealth Action Plan 2012–2020[90] in an effort to remove the barriers to deployment of eHealth that continued to exist until that point.

The latest developments in the eHealth field include the Commission's Communication on the transformation of digital health and care, which was released in April 2018.[91] One of the initiatives presented in the Communication was the development by the Commission of the eHealth Digital Service Infrastructure for the facilitation of the interoperability of European eHealth systems and the exchange of patients' health data. Currently two electronic cross-border health services are operational, e-prescription, which allows citizens in Europe to retrieve their medication in a pharmacy located in another European country, and patient summary, which provides information on important health-related aspects of each individual.[92] The first cross-border exchanges started in 2019. By 2021, both services will gradually be implemented in 22 EU countries. In the longer term, the Commission is working towards a European electronic health record exchange format accessible to all EU citizens. The plan is that a full Health Record will become available across the EU.

As regards mHealth in particular, the Commission published a Green Paper on mobile Health in 2014.[93] The Green Paper was announced in the eHealth Action Plan 2012–2020[94] and its objective was to launch a broad stakeholder consultation on existing barriers and issues related to mHealth. A wide range of stakeholders (industry, national and regional authorities, health professionals, research community, non-governmental organisations, patient associations etc.) responded to the consultation and provided their input on several issues relating to the uptake of mHealth in the EU, such as data protection, big data, applicable legal framework, patient safety, liability and others.[95] The Green Paper was accompanied by the Commission's Staff Working document to raise app developers' awareness of EU rules on data protection, medical devices and consumer directives.[96]

There is no doubt that eHealth has attracted significant legislative attention as regards both its definition and regulation. However, there is no official reference to eHealth as a CII. Even though ENISA has acknowledged the significance of eHealth[97] not only as a major contributor to the societal and financial welfare but, more specifically, as a CII, most Member States have not developed a specific methodology or legislation for the identification of critical eHealth infrastructures. In many cases eHealth is identified as part of a critical sector such as Heath care and/or ICT. Therefore, the approach that has been adopted until today by the majority of Member States is that of identifying and protecting eHealth infrastructures in the con-

[84] See article 87 of the MDR and article 82 of the IVDR

[85] See also https://ec.europa.eu/docsroom/documents/38941

[86] eHealth is the use of ICT in health products, services and processes combined with organisational change in healthcare systems and new skills, in order to improve health of citizens, efficiency and productivity in healthcare delivery, and the economic and social value of health. eHealth covers the interaction between patients and health-service providers, institution-to-institution transmission of data, or peer-to-peer communication between patients and/or health professionals (see https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012DC0736&from=EN).

[87] See Communication from the Commisision tro the Council, the European Parliament, the European Economi and Social Committee and the Comitte of the Regions e-health-making healthcare better for European coitizens: An action plan for a European –Health Area, COM (2004), 356 https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2004:0356:FIN:EN:PDF

[88] Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32011L0024

[89] See Commission Implementing Decision 2019/1765 of 22 October 2019 providing the rules for the establishment, the management and the functioning of the network of national authorities responsible for eHealth, and repealing Implementing Decision 2011/890/EU, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019D1765.

[90] See Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on eHealth Action Plan 2012-2020 - Innovative healthcare for the 21st century, COM/2012/0736.

[91] See Communication from the Commission to the European Parliament , the Council, the European Economic and Social Committee and the Committee of the Regions on enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society, COM/2018/233 finalhttps://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A233%3AFIN

[92] The digital Patient Summary is meant to provide doctors with essential information in their own language concerning the patient, when the patient comes from another EU country and there may be a linguistic barrier.

[93] See footnote 50.

[94] See footnote 73.

[95] For the summary report on the Public Consultation on the Green Paper on Mobile Health see https://ec.europa.eu/digital-single-market/en/news/summary-report-public-consultation-green-paper-mobile-health

[96] See Commission Staff Working Document on the existing EU legal framework applicable to lifestyle and wellbeing apps accompanying the document Green Paper, COM (2014) 219.

[97] See https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/health

text of the general regulation and strategy for CIIP. ENISA in its report on Security and Resilience in eHealth,[98] in an effort to treat eHealth as an CII, lists a number of assets that, based on feedback received by interviewees, are considered as critical. The list includes, among others, Health Information systems, Laboratory Information Systems, Patient Health Record services, Authentications server etc. The report places emphasis upon two systems that were considered critical by all interviewees, namely the Electronic Health Record System (EHR) and the e-Prescription system. The discussion on the identification of eHealth as an independent CII may still be found at an early stage, however it is foreseeable that the constantly increasing use of eHealth services and their contribution to the operation of the healthcare sector overall, combined with the security challenges emerging in eHealth, will accelerate this process.

5. Conclusion

Critical Infrastructures constitute the backbone of our societal and economic well-being. Improving their resilience against different kind of attacks has therefore become a priority for the authorities around the globe. The list of risks and threats that CIs encounter has expanded over the last decades to include anything from traditional risks such as natural disasters and human errors to emerging and unpredictable threats, such as cyberattacks. At the same time the constantly growing dependence of CIs on ICT for their operation has placed the protection of CIIS firmly into the EU and national agendas. This high dependence on CIIs, their cross-border connectivity and interdependencies with other infrastructures in combination with the sophistication and the volume of cyberthreats targeting them have developed into a challenging task for both operators of these infrastructures and legislators. As regards the legislative effort undertaken to this effect, it is undisputable that Europe has placed substantial resources into implementing an EU-wide regulatory framework for the protection of CIs and the underlying network and information systems that support them, with the NIS Directive being at the spearhead of this effort.

There is of course still plenty to be done in terms of promoting cooperation at EU and international level, enhancing preparedness for better response to the constantly emerging new threats and adapting to the new challenges that the continuous integration of digital technologies in CIs brings along. As regards the current regulatory approach, it is expected that the upcoming review of the Directive on the Protection of European Critical Infrastructures, will acknowledge the shortcomings of the first draft and will adequately address the new developments and emerging challenges in the field. As the Directive is, at the moment, the main legislative instrument for the protection of CIs at EU level, it is expected that the revised document will live up to these expectations. When it comes to protection of network and information systems that support CIs, the NIS Directive assumes the role of the applicable mechanism for protection against cyberattacks. Given that the NIS Directive came into force in 2018, it remains to be seen how the Member States and the Operators of Essential Services will make use of its provisions in practice. Both the Commission and ENISA are expected to contribute to this effort by further clarifying the security and notification requirements provided in the NIS Directive and by assisting all involved parties in implementing them. Last but not least, protection of CIs seems incomplete without a regulatory framework for the protection of Industrial Control Systems. Even though ENISA identified this regulatory gap since 2011, this issue remains pending.

The health sector in particular offers an example of how digitalisation opens up new transformative opportunities. While the quality of services and therefore the safety and well-being of patients have been drastically improved as a result of the extensive use of ICT in the provision of health services, from medical devices and smart hospitals to eHealth and mHealth, at the same time the sector has been extremely vulnerable to cyberattacks. Taking into consideration what is at stake, from human lives due to a device malfunction to violation of privacy as a result of a personal data loss or theft, safeguarding the protection of this CI has been treated as a high priority by all involved parties. In this context, a number of regulatory instruments have been introduced that consist of legislation of a horizontal scope together with sector specific measures. Nevertheless, lack of clarity and uniformity in terminology risk creating misunderstanding and, therefore, warranting a decreased level of protection.

Digitalisation has transformed the lives of individuals and the organisation and functioning of the society, as a whole. Living in the digital era promises a more qualitive and comfortable life to the majority of the word population. At the same time, however, digitalisation comes with a price. Protecting our CIs and other assets against threats that did not exist before has been turned into a speed and endurance race that demands alertness, flexibility, preparedness and substantial effort by all the parties involved.

Declaration of Competing Interest

This research has been funded under the European Commission's H2020 project SPHINX – A Universal Cyber Security Toolkit for Health-Care Industry, Grant Agreement 826183.

[98] See ENISA's report on Security and Resilience in eHealth Infrastructures and Services, https://www.enisa.europa.eu/publications/security-and-resilience-in-ehealth-infrastructures-and-services