Int. Cybersecur. Law Rev. (2022) 3:163–180
https://doi.org/10.1365/s43439-022-00054-x

Cybersecurity of medical devices: new challenges arising from the AI Act and NIS 2 Directive proposals

Elisabetta Biasin · Erik Kamenjašević

Received: 17 March 2022 / Accepted: 23 April 2022 / Published online: 16 May 2022

Abstract Cyberattacks on the IT infrastructure of hospitals, electronic health records or medical devices that have taken place during the COVID-19 pandemic reaffirmed how crucial it is to ensure cybersecurity in the healthcare sector. Medical devices are regulated in the European Union (EU) through vertical product-specific legislation, such as the Medical Device Regulation (MDR), among others. The MDR foresees safety requirements implying cybersecurity obligations for medical device manufacturers. In 2021, the EU legislator put forward the Network and Information Security System Directive reform (NIS 2) and the Artificial Intelligence Act (AIA) proposal, containing additional cybersecurity requirements applicable to medical devices. This article analyses how the new reforms interact with the existing legislation from a cybersecurity perspective. The research finds that parallel provision of analogous cybersecurity requirements (especially on notification requirements) could lead to regulatory overlapping, fragmentation, and uneven levels of protection of individuals in the EU internal market. In the "Recommendations and conclusions", the article provides policy recommendations to the EU legislator to help mitigate these risks.

Keywords Security · Healthcare · Critical infrastructure · Artificial intelligence · Network and information system security

The authors equally contributed to the research and writing process of this manuscript.

Elisabetta Biasin (✉) · Erik Kamenjašević
KU Leuven Centre for IT & IP Law, Leuven, Belgium
E-Mail: elisabetta.biasin@kuleuven.be

Erik Kamenjašević
E-Mail: erik.kamenjasevic@kuleuven.be

1 Introduction

Cyberattacks on 'cyber-connected'[1] medical devices that have taken place during the COVID-19 pandemic reaffirmed the importance and urgency of ensuring cybersecurity in this sector.[2] According to a World Economic Forum study on healthcare cyberattacks, "the threat plagued the sector during the COVID-19 pandemic. The pandemic accelerated the growth of telemedicine and other digital health facilities. As technology develops and healthcare gets more digitalised, the potential risk of cyber incidents also increased" [22].

If successful, one such attack may have enormous and immediate life-threatening, material and/or economic consequences. For instance, if a cyberattack targets a patient's cyber-connected pacemaker, it may cause the device to stop working correctly and provoke severe health risks and/or death of that patient.[3] Moreover, such a cyberattack could also have indirect consequences, including but not limited to the diminishment of patients' trust in the security and safety of the healthcare system and fear or hesitancy towards using certain medical devices due to their potential vulnerability to falling victim to cyberattacks.[4]

In our previous paper[5], we analysed the European Union (EU) legal framework relevant for the cybersecurity of 'cyber-connected' medical devices[6]. This paper looks into two EU legislative proposals—the Network and Information Security System (NIS 2) Directive[7] and the Artificial Intelligence Act[8] proposals. In particular, our analysis here focuses on the new challenges their cybersecurity-related requirements applicable to the 'cyber-connected' medical devices pose to the existing EU legal framework[9].

[1] The term was coined by DeNardis [6]. "Cyber-connected medical devices include wireless cardiac appliances, insulin pumps, telemedicine diagnostic equipment, and other objects adjacent to or embedded directly in the flesh" (id.).

[2] See, for example, Cerulus [4]; Schwartz [33].

[3] See, for instance, the real life story about Dr Marie Moe in Dumitrascu [10].

[4] To further read about consequences of cyberattacks in the healthcare sector, see, for example, Rosager Ludvigsen and Nagaraja ([31] forthcoming).

[5] See [1].

[6] Next to these pieces of legislation, the EU Medical Devices Coordination Group (MDCG) issued non-binding Guidance on Cybersecurity of medical devices; see Medical Devices Coordination Group (2019). For a detailed explanation of applicable legislation concerning medical devices cybersecurity in the EU and an analysis of MDCG Guidance, see [1].

[7] Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 [7] (hereinafter NIS 2 Directive proposal).

[8] Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, COM/2021/206 final (hereinafter AI Act proposal) [27].

[9] For the complete overview of the EU legal framework dealing with the cybersecurity of medical devices, see [1].

2 Medical device cybersecurity in the context of *the NIS 2 Directive proposal*

The NIS Directive was approved in 2016 and has been directly applicable in EU Member States since 2018. The Directive sets common security requirements to ensure network and information security across the EU. The Directive is relevant to the healthcare sector. Healthcare providers are included in the scope of application of the Directive, and they are categorised as Operators of Essential Services (OES).[10] As such, they are subject to the Directive's requirements of adopting risk management processes and incident notification to ensure network and information systems security.

After its entry into force, the NIS Directive underwent a series of challenges in practice [23, p. 147].[11] The most crucial issue was its incoherent application due to the divergent Member State methodologies for identifying OES [17]. These different methodologies entailed the incoherent application of the NIS Directive across the EU and led to fragmentation in the EU internal market [2, p. 68].[12] Another fundamental challenge concerned the diverging security and incident notification requirements, left open by the Directive, applied differently from one Member State to another and causing fragmentation. Moreover, there was ineffective supervision, limited enforcement of the Directive and a lack of systematic information sharing among Member States. The EU legislator acknowledged this varying level of harmonisation as a problem to be solved and initiated the reform process of the NIS Directive with the NIS 2 Directive proposal.

The proposal introduces some significant changes. It removes the requirement on Member States to identify OES and Digital Service Providers (DSP) in their territories. This way, there would be no risks of having different methodologies across the Member States for their identification. In turn, the proposal replaces OES and DSP with new categories: 'essential' and 'important entities.' Essential and important entities are listed in Annexes I and II of the proposal. They are ordered per sector and sub-sector (for example, 'health' and 'manufacturing' sectors; 'manufacture of medical devices and in-vitro medical diagnostic medical devices' sub-sectors). Each sub-sector contains a list of 'types of entities.'

[10] Healthcare providers are considered OES inasmuch they are identified as such by the respective Member State. As OES, healthcare providers have to ensure a minimum level of security for their network and information systems and have to notify security incidents to competent authorities without undue delay. To reach that level, they must take appropriate and proportionate technical and organisational measures to manage the risk posed to the NIS security that they use in their operations. Security measures and modalities for communication of security incidents are defined at a national level by each Member State, which must adopt national strategies on network and information security.

[11] These were considered during the review by the European Commission. See European Commission [16, p. 2].

[12] This was particularly evident in the healthcare sector. To give an example, the mentioned report shows that Finland identified 10,897 OES for all NISD sectors due to the high number of OES identified for the healthcare sector. The number is very high if compared with other countries (e.g., Italy identified 533 OES for all NISD sectors) or the overall amount of OES—determined by all Member States (i.e., 4925) (see also SAFECARE [2]).

Compared to the NIS Directive, the NIS 2 Directive proposal broadens its scope of application with a significant impact on the healthcare sector. Healthcare providers[13] (which were already included in the NIS Directive as OES) remain in the scope of the legislation, and they are now considered 'essential entities' (Annex I). In addition to these, the NIS 2 Directive proposal adds new types of entities relevant to the healthcare sector. Under 'essential entities', the following are now included: EU reference laboratories[14], entities carrying out R&D activities of medicinal products[15], entities manufacturing basic pharmaceutical products and preparations[16] as well as manufacturers of medical devices considered critical during a public health emergency[17]. Concerning 'important entities', the proposal includes the 'entities manufacturing medical devices and in vitro diagnostic medical devices' (Annex II NIS 2 Directive proposal). The above-listed categories are not included in the NIS Directive, and therefore this expansion is a core change for the medical devices sector.

Similarly to the NIS Directive, the NIS 2 Directive proposal mandates the Member States to establish a set of security measures for the entities under its personal scope. Chapter IV of the proposal contains the obligations on cybersecurity and risk management and reporting. Article 18 of the proposal on cybersecurity risk management measures implies that essential and important entities shall "take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information system." As examples of measures, the article includes, amongst others, incident handling (prevention, detection and response to incidents) and measures to ensure supply chain security and vulnerability handling and disclosure. Article 20 of the proposal on reporting obligations introduces a two-step procedure to report significant security breaches, which could also be reported to the recipients of their services. Article 21 of the proposal concerns cybersecurity certification schemes. Enforcement and supervision of essential and important entities are delegated to competent authorities. Competent authorities shall supervise them and ensure their compliance with the security and incident notification requirements. An *ex-ante* supervisory regime is in place for essential entities and an *ex-post* one for important entities.

[13] For a definition of healthcare providers, see Article 3(g) of Directive 2011/24/EU [8] of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare [2011] OJ L201 (hereinafter Directive 2011/24).

[14] As referred to in Article 15 of Regulation on serious cross-border threats to health (see European Commission [18] Proposal for a regulation on serious cross-border threats to health and repealing Decision No 1082/2013/EU, COM (2020) 727).

[15] As referred to in Article 1(2) Directive 2001/83/EC of the European Parliament and of the Council of 6 November 2001 on the community code relating to medicinal products for human use (2001) OJ (L311).

[16] As referred to in section C division 21 of NACE Rev. 2, see European Commission, NACE Rev. 2 Statistical classification of economic activities in the European Community, 2018.

[17] See Article 20 of the European Commission's [18] Proposal for a Regulation of the European Parliament and of The Council on a reinforced role for the European Medicines Agency in crisis preparedness and management for medicinal products and medical devices COM (2020)725.

3 Medical device cybersecurity in the context of *the AI Act proposal*

The AI Act proposal introduces a number of provisions prohibiting certain AI systems and practices, proposes a risk-based mechanism for governing those AI systems that pose a high risk for individuals or society, stipulates fines for providers' non-compliance with the Act and establishes an EU body responsible for the harmonised application of the Act amongst Member States.[18]

Under Article 6 (1)(b) and Annex II (section 11) of the AI Act proposal, most medical devices would classify as high-risk AI systems. As stated by MedTech [27], the definition of AI and risk classification could mean that any medical device software could fall within the scope of the AI Act proposal and be considered a high-risk AI system since most medical device software needs conformity assessment by a notified body. Consequently, the following recitals and provisions of the AI Act proposal would be applicable to their providers when it comes to implementing cybersecurity requirements established by the AI Act proposal.

Recital 51 of the AI Act proposal acknowledges the role cybersecurity has in ensuring the resilience of AI systems against cyberattacks attempting to alter their use, behaviour and performance, or compromise their security properties. To ensure an appropriate level of cybersecurity of high-risk AI systems, providers need to take suitable measures.

Recital 43 of the proposal refers to the requirements that high-risk AI systems should respect in order to "effectively mitigate the risks for health, safety and fundamental rights, as applicable in the light of the intended purpose of the system, and no other less trade restrictive measures are reasonably available, thus avoiding unjustified restrictions to trade". One of these requirements is cybersecurity. In that regard, Recital 49 of the AI Act proposal states that high-risk AI systems need to perform consistently throughout their lifecycle and meet an appropriate level of cybersecurity in accordance with state of the art.

Article 13(1) of the proposal requires that high-risk AI systems are designed and developed in a way that ensures their transparent operation so the users can interpret the system's output and use it appropriately. In the instructions for use (Article 15(2-3) AI Act proposal), providers shall specify the level against which cybersecurity of the system has been tested and validated, which can be expected, as well as any known and foreseeable circumstances that may impact that level of cybersecurity. Article 15(4) of the proposal requires that the technical solutions aimed at ensuring the cybersecurity of high-risk AI systems are appropriate to the relevant circumstances and risks. To this end, high-risk AI systems certified according to the Cybersecurity Act (CSA)[19] shall be presumed to comply with the cybersecurity requirements set out in the proposal (AI Act proposal, Article 42).

[18] In this respect, see also Gartner [19] on '[w]hy the prohibition of certain persuasive technologies in the European proposal for an Artificial Intelligence Act is not a surprise'.

[19] See Article 56 of Regulation (EU) 2019/881 [30] 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), 2019 OJ (L 151).

Based on the current version of the text, the AI Act proposal and MDR apply simultaneously to medical devices. The main challenges for the manufacturers/providers of these devices are explained in the following section.

4 Achieving consistency within the EU cybersecurity regulatory framework: core challenges

4.1 Converging incident notification requirements between the MDR and the NIS 2 Directive proposal

The MDR and the NIS 2 Directive proposal foresee incident notification obligations. The MDR requires that manufacturers of medical devices report serious incidents to the relevant competent authorities (Article 87 MDR). The NIS 2 Directive proposal mandates Member States to require essential and important entities to notify, without undue delay, of any incident having a significant impact on the provision of their services (Article 20(1) NIS 2 Directive proposal) or cyber threats that could have potentially resulted in a significant incident (Article 20(2) NIS 2 Directive Proposal). These shall be notified to the competent authority or the national computer security incident response team (CSIRT).

The MDR's serious incidents are defined as "any incident that directly or indirectly led, might have led or might lead to any of the following: (a) the death of a patient, user or other person; (b) the temporary or permanent serious deterioration of a patient's, user's or other person's state of health, (c) a serious public health threat" (Article 4(65) MDR). The NIS 2 Directive proposal defines "any event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the related services offered by, or accessible via, network and information systems" (Article 4(5) NIS 2 Directive proposal).

Despite the different definitions, the two requirements may result in overlapping tasks, in practice, for medical device manufacturers. Let us imagine the following situation: A cyberattack affects a healthcare facility and its connected medical devices. The provision of its services could be impacted (which is a condition for incident notification). It could also lead to a temporary or permanent serious deterioration in a patient's state of health (which is a condition for serious incident reporting). Therefore, medical device manufacturers would have to comply with notification obligations stemming from both the MDR and the NIS 2 Directive proposal.

Overlapping in itself is not the problem. The issue lies in the interpretation of both requirements in the case of overlapping. According to the NIS 2 Directive proposal, when an incident notification requirement overlaps with another, sector-specific law should prevail if considered as *'at least equivalent'* (Article 2(6) NIS 2 Directive proposal). The shortcoming of this provision resides in its vagueness of 'at least equivalent'. The proposal does not elaborate on what 'equivalent' means, nor does it provide examples regarding medical devices. Moreover, it is not clear *to what* exactly equivalence refers.

It might be reasonable to conclude that, since MDR notification requirements are specific to the medical devices class of products, it would suffice to consider MDR

as a *lex specialis* and thus as 'at least equivalent'. On closer scrutiny, however, the MDR and the NIS 2 Directive proposal requirements show divergences.[20]

The first divergence concerns the *definitions* of incidents. In fact, not all serious incidents are also cybersecurity incidents. This is well exemplified in Annex II of the Medical Device Coordination Group (MDCG) Guidance [25], from which we report the following case:

> Warming therapy device for premature babies: an unauthorised user with physical access to the device guesses the weak password for the service account and exports therapy and patient data via the USB interface.[21]

According to the MDCG, this kind of security harm does not result in safety harm in terms of the MDR's serious incident notification. It is an event that could require incident notification but not serious incident reporting. In this case, the rules of the NIS 2 Directive proposal would cover circumstances that the MDR rules would not. Therefore, the medical device manufacturer would have to notify the incident about the unauthorised access to the NIS 2 Directive proposal competent authority and not the national relevant authority under the MDR (Table 1).

The second example of divergence concerns notification *timing*. The NIS 2 Directive proposal requires notification "without undue delay and in any event within 24 h after having become aware of the incident" (Article 20 NIS 2 Directive proposal), while the MDR mandates the notification from "immediately to no later than 15 days after becoming aware of the incident" (Article 87(3) MDR), 2 days in the event of a serious public health threat (Article 87(4) MDR) or 'immediately' in the event of death or unanticipated serious deterioration of a person's state of health (Article 87(5) MDR). In this respect, the two legal acts are not strictly equivalent.

The third element of divergence concerns the *recipients* of notification obligations, as these would be addressed to *different authorities*. Manufacturers shall notify the competent authority and/or the CSIRT under the NIS 2 Directive proposal, while the MDR would require the relevant competent authorities. Notification schemes for the NIS 2 Directive proposal vary across the Member States.[22] Could a notification to a national health authority as per the MDR be considered equivalent to a CSIRT as per the NIS 2 Directive proposal? In this case, too, it remains questionable whether the NIS 2 Directive proposal and the MDR could be considered equivalent.

In addition to this, it is worth noting that this decision on 'at least equivalence' could be left to a Member State since the NIS 2 Directive proposal requires a national act of implementation. As some authors (see, for example [9]) suggest, entrusting Member States with the burden of conducting such a balancing exercise between the EU sector-specific requirements and the NIS 2 Directive proposal's requirements

[20] See also the NIS Cooperation Group [29], exploring 'synergies' about notification requirements for sector-specific legislation and the NIS Directive.

[21] See MDCG Guidance [25], Annex II.

[22] Notification schemes may vary across Member States, as the EU Member States implement notification requirements differently. Incidents may be reported to one single national authority (the CSIRT), or they may be reported to sectoral authorities, or a mix of the former two options. See NIS Cooperation Group [29].

Table 1 Comparative table: the NIS 2 Directive proposal (incident) and the MDR (serious incident)

	NIS 2 Directive proposal	MDR
Product	Medical devices	Medical devices
Regulated entities	*Important and essential entities*	*Manufacturers*
Definition	*'Incident'*: any event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the related services offered by, or accessible via, network and information systems. '*Cyber threat*': any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons	'*Serous incident*': any incident that directly or indirectly led, might have led or might lead to any of the following: (a) the death of a patient, user or other person; (b) the temporary or permanent serious deterioration of a patient's, user's or other person's state of health, (c) a serious public health threat
Event/ conditions	*Potential or occurred* The event shall have a significant impact on the provision of services (having the potential to cause substantial operational disruption or financial losses for the entity concerned; or has affected or has the potential to affect other natural or legal persons by causing considerable material or non-material losses)	*Potential or occurred* Reporting obligations also if aware—yet unsure—of potentially reportable incident
Timing	Without undue delay and *in any event within 24 h* after having become aware of the incident'	*Immediately to no later than 15 days* after becoming aware of the incident; 2 days in the event of a serious public health threat; or 'immediately', in the event of death or unanticipated serious deterioration of a person's state of health
Authorities	*CSIRT* or national *competent authority*	Relevant *competent authority*

MDR Medical Device Regulation, *NIS* Network and Information Security System, *CSIRT* computer security incident response team

may not be a fair solution when other EU sector-specific legislation is directly and uniformly applicable (such as the MDR) (*id.*). Furthermore, leaving it to Member States to decide on a matter of *lex specialis* and *lex generalis* could lead to their different interpretation and application, thus ultimately leading to fragmentation issues.[23]

To mitigate this, the final text should add a specific reference to the medical device legislation when notification requirements are at stake. Alternatively, the NIS 2 Directive—or any further guidance issued by the European Commission—should explicitly specify whether medical device legislation is considered as 'at least equivalent'.

[23] There could be in principle conflict of (EU/national) laws about the issue of incident notification *lex generalis–lex specialis*. The analysis of this aspect falls outside the scope of this paper; however, it could be a possible avenue for further research.

The choice of considering MDR as a *lex specialis* might be a rather pragmatic one. As the above considerations showed, the NIS 2 Directive proposal and the MDR notification requirements are not strictly 'equivalent'.

As a first hypothesis, let us consider the MDR as *a lex specialis.* This could bring more simplification for manufacturers, but some safety harms (as explained *supra*), would be left unaddressed. As a second hypothesis, let us not consider the MDR as a *lex specialis.* On the one hand, this could imply more guarantee in terms of safety and cybersecurity for users, at the cost of, on the other hand, overlapping and possibly adding more compliance burdens on manufacturers.

If the legislator aims to give prominence to simplification, then the first hypothesis would be more fitting for the purpose. In such a case, the legislator should assess and establish coordination mechanisms between notified authorities to guarantee the safeguards of the legal act, which will not be considered *lex specialis.* If the legislator aims to give more relevance to patients' safety and rights protection, then the parallel application is the most suitable regulatory approach to that objective. A wider range of safety and security harms would be addressed (as explained *supra*) for patients. As a possible 'third-way' hypothesis—to balance the above-mentioned objectives—the legislator could consider the MDR as a *lex specialis* for specific circumstances only (by clarifying for which ones the MDR is considered as a *lex specialis*). In that case, further research would be needed to support the legislator in ascertaining the taxonomy of cases leading to overlapping between the NIS 2 Directive proposal and the MDR and the feasibility of this approach itself.

4.2 Converging cybersecurity requirements in the MDR and the AI Act proposal

The AI Act proposal contains comparatively general provisions on cybersecurity[24], while the MDR enlists a more detailed set of requirements.[25] Questions about convergence between the AI Act proposal and the MDR may arise regarding incident notification requirements. From the perspective of cybersecurity—and as exemplified *infra*—an incident could occur following the MDR[26] and the AI Act proposal.

The MDR defines a serious incident as "any incident that directly or indirectly led, might have led or might lead to (...) the death of the patient user or other person, the temporary or permanent serious deterioration of a patient's, user's or other person's state of health, a serious public threat" (Article 87 MDR). The AI Act proposal, conversely, defines serious incidents as "any incident that directly or indirectly led, might have led, or might lead to (...) (a) the death of a person or serious damage to a person's health, to property or the environment, (b) a serious and irreversible disruption of the management and operation of critical infrastructure" (Article 3(44) AI Act proposal).

[24] As analysed supra, see Sect. 3.

[25] For a more detailed list of requirements and relevant analysis, see also [1].

[26] For a broader elaboration, see the MDCG [25] Guidance.

To show how an incident under the AI Act proposal could, in principle, be a cybersecurity incident, we could again cite a case from the MDCG Guidance [25]:[27]

> Anaesthesia device: An unauthorised user with physical access to the device guesses the weak password for the service account and manipulates the configuration settings. As a safety harm result, the anaesthesia supplies a wrong anaesthetic concentration (MDCG Guidance [25], Annex II).

The proposed case could lead to the following consequences: A wrong anaesthetic concentration could directly or indirectly lead to the 'deterioration of a patient's health' (MDR condition) or also a 'serious damage' to it (AI Act proposal condition). Therefore, the AI Act proposal and the MDR both have provisions for incident notification from the cybersecurity perspective.

With regard to this, however, one may wonder how the AI Act proposal and MDR requirements could interact. Should they apply in parallel, or does one prevail over the other? The explanatory memorandum of the AI Act proposal gives some notes on its possible interplay with the New Legislative Framework (NLF) legislation, which also encompasses medical devices.[28] The proposal specifies that, since NLF legislation aims at ensuring the overall safety of the final product, it may also contain specific requirements regarding the safe integration of an AI system into the final product. The explanatory memorandum follows and clarifies that the "proposal will be integrated into the existing sectoral safety legislation to ensure consistency" and that "the requirements for AI systems set out in the proposal will be checked as part of the existing conformity assessment procedures under the relevant NLF legislation" (AI Act, Explanatory Memorandum).

These specifications seem to lack concreteness. Therefore, interpretative efforts are necessary to further understand the possible interplay of the two acts (Table 2).

As a first hypothesis, one could consider the medical devices law as a *lex specialis* to the AI Act proposal. This hypothesis would be based on the above remarks on the integration of requirements into NLF legislation in the explanatory memorandum.[29] However, considering MDR requirements as *lex specialis* may not be entirely correct. In fact, the general requirements provided in the AI Act proposal set different safeguards if compared with those provided by the MDR. In the *definition* of an incident, the AI Act proposal includes 'the serious damage to property or the environment', which is not an element present in the MDR.[30]

Furthermore, from the perspective of the *conditions for the notification,* the AI Act proposal requires the notification of serious incidents when they constitute a 'breach

[27] In this case, the example is taken from MDCG [25] and MDCG [26], see Annex IV— Classification examples for medical device software.

[28] Section 1.2, Explanatory Memorandum of Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, COM/2021/206 final [27].

[29] See *supra.*

[30] As a side aspect, the AI Act proposal requires notification of malfunctioning, a term that is left undefined in the proposal.

Table 2 Comparative table: the AI Act proposal (incident) and the MDR (serious incident)

	AI Act proposal	MDR
Product	High-risk AI systems	Medical devices
Regulated entities	*Providers of high-risk AI systems*: A natural or legal person, public authority, agency or other body that develops an AI system or that has an AI system developed with a view to placing it on the market or putting it into service under its own name or trademark, whether for payment or free of charge	*Manufacturers of medical devices*: means a natural or legal person who manufactures or fully refurbishes a device or has a device designed, manufactured or fully refurbished, and markets that device under its name or trademark
Definition	'*Incident*': any incident that directly or indirectly led, might have led, or might lead to (a) the death of a person or serious damage to a person's health, to property or the environment, (b) a serious and irreversible disruption of the management and operation of critical infrastructure '*Malfunctioning*' (undefined)	'*Serious incident*': any incident that directly or indirectly led, might have led or might lead to any of the following: (a) the death of a patient, user or other person; (b) the temporary or permanent serious deterioration of a patient's, user's or other person's state of health, (c) a serious public health threat
Event/ conditions	*Potential or occurred* Shall constitute a breach of obligations under Union law intended to protect fundamental rights	*Potential or occurred* Reporting obligations also if aware—yet unsure—of potentially reportable incident
Timing	*Immediately* after the provider has established a causal link between the AI system and the incident or malfunctioning or the reasonable likelihood of such a link, and, in any event, *not later than 15 days* after the providers becomes aware of the serious incident or of the malfunctioning	*Immediately to no later than 15 days* after becoming aware of the incident; 2 days in the event of a serious public health threat; or 'immediately', in the event of death or unanticipated serious deterioration of a person's state of health
Authorities	Relevant market *authority*	Relevant competent *authority*

AI Artificial Intelligenc, *MDR* Medical Device Regulation

of obligations under Union law intended to protect fundamental rights'. While the MDR is about ensuring the health and safety of individuals and thus their dignity and patient's rights—it nevertheless does not rely upon the risks posed to the *individual's fundamental rights* as a condition for reporting serious incidents. This means that one could notify an incident that is relevant from the cybersecurity point of view by following the AI Act proposal (since, for example, it has effects on the environment or since it poses risks to fundamental rights, such as the right to non-discrimination) and not of the MDR.

Most importantly, *regulated entities* subject to notification obligations are not the same. According to the MDR, *manufacturers* shall be subject to the incident reporting requirement. In the MDR, manufacturers are defined as a "natural or legal person who manufactures or fully refurbishes a device or has a device designed, manufactured or fully refurbished, and markets that device under its name or trademark" (Article 2(30) MDR). For the AI Act proposal, *high-risk AI system providers* must notify serious incidents. These providers are defined as the "natural or legal person, public authority, agency or other body that *develops* an AI system, or that

has an AI system developed *with a view to* placing it on the market or putting it into service under its own name or trademark, whether for payment or free of charge" (emphasis added). In contrast to the MDR, the AI Act proposal encompasses the category of *developers*—while the MDR does not. The MDR puts the focus on the entity that *places* the product on the market.[31] Additionally, the AI Act proposal says *with a view* to placing on the market, wording which suggests that there is a prior stage to what is considered 'placing on the market'.

In conclusion, coming back to the argument *lex specialis versus lex generalis,* it may be more evident now why considering MDR requirements as *lex specialis* may not be a fully suitable solution. The AI Act proposal and the MDR have differences in their incident notification, and a parallel application would be the solution that would guarantee the highest degree of safeguards for individuals. For reasons of simplification, the legislator may decide to have just one piece of legislation applicable for incident notification. Most probably, it will be the MDR.[32] In this case, further analysis could assess how the differences illustrated above could be overridden by future regulatory interventions.[33]

4.3 Incoherent use of the term cybersecurity

The meaning and evolving use of the term 'cybersecurity' is a recurrent issue in EU legislation, and the problem remains in the NIS 2 Directive proposal.[34] As explained *infra*, this issue is gaining importance due to a conceptualisation shift at the policymaking level—from the protection of network and information systems to the individual—which is not yet mirrored appropriately in the NIS 2 Directive proposal.[35]

Until recently, cybersecurity had a broader and vaguer understanding amongst EU stakeholders and policymakers, and there was no standard definition of cybersecurity in EU binding legislation. This issue was repeatedly pointed out by the European Network and Information Security Agency (ENISA) [13]. For instance,

[31] In the medical device industry terminology, outsourced developers of manufacturers are defined as 'virtual manufacturers'. These are different from the category of manufacturers that remain the responsible entities for most of MDR compliance. For a detailed analysis, see MHRA [28].

[32] See *above,* with regard to the references in the AI Act proposal on NLF.

[33] As a side note, it is worth observing that convergence between the two legal acts shall be tackled with caution and due attention to timing. Specific requirements provided by one specific legal act could apply in concurrence with the general requirements (not wholly or yet operationalised into sector-specific legal provisions) of another. If these integration aspects are not addressed in a timely manner, the lack of coordinated frameworks could lead, in practice, to regulatory uncertainty.

[34] Legal studies on EU cybersecurity law have underlined the conceptualisation issue about cybersecurity. Kasper & Antonov, for instance, highlighted that cybersecurity as a core concept lacks clarity. In their view, such a lack could raise questions about coherence and consistency of already adopted and newly proposed legislative acts in the field of cybersecurity. For a critical overview of cybersecurity conceptualisation and regulation in the EU see Kasper and Antonov [21]; González Fuster and Jasmontaite [20].

[35] This article does not aim to offer new conceptual solutions for the term 'cybersecurity' in the EU, as this would require more space and further specifications that would be beyond the scope of the paper. The literature on cybersecurity conceptualisation is copious. Amongst the many, see Kasper & Antonov [21], for the relevance to the EU policy framework.

ENISA noted that cybersecurity, being a relatively young term, had a diverse range of understanding and would deserve an appropriate understanding to be used in the context of the intended use of the stakeholders and policymakers (*id.,* p. 9). To ENISA, cybersecurity was a contextual-dependent 'enveloping term', for which it was not possible to make a definition over the extent of the things cybersecurity covers (*id.*, p. 7). Instead, the Agency recommended that Member States find a commonly agreed working definition of cybersecurity that is precise enough to support the definition of common goals across the EU [12, p. 12].

The EU policy documentation started to use cybersecurity only recently [20, p. 103]. The most relevant point, indeed the 'tipping point', of EU documentation referring to cybersecurity is the 2013 EU Cybersecurity Strategy [14]. The document contained a cybersecurity definition in a footnote (*id.*, p. 3). It referred to this as "the safeguards and actions that can be used to protect the cyber domain, (...) from those threats that are associated with or that may harm its interdependent networks and information of information infrastructure" (*id.*). Cybersecurity would help preserve "the availability and integrity of the network and infrastructure and the confidentiality of the information contained therein" (*id.*). As González Fuster and Jasmontaite [20] note, EU institutions appeared reluctant in the past to use the term 'cybersecurity'. For instance, the NIS Directive (often referred to as the first EU-wide cybersecurity legislative act [15]) contained only one minor reference to cybersecurity.[36] Instead, it formally referred to the 'security of network and information systems' (defined in Article 4(1)(2) as "the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems").

With the CSA, cybersecurity was defined at the EU level in a legally binding document for the first time "as a set of activities to protect network and information systems, the users of such systems, and other persons affected by cyber threats" (Article 4 CSA)[37]. Interestingly, the new definition of cybersecurity adds a new layer of protection for individuals. The CSA definition of cybersecurity includes the protection not only of network and information systems but also 'users' and 'persons' that might be affected by threats.

The core aspect of the NIS Directive is that it was formerly focused on the protection of network and information systems' security, having regard to the 'data' and 'services' offered by those systems.[38] Now, even the title of the new proposal—"on

[36] Recital 34, Directive (EU) 2016/1148 [7] 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 (L 194).

[37] Whereas cyber threats are "any potential circumstance, event, or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons" (Article 2(8) CSA). Such a definition seems to be in continuity with the 2013 Cybersecurity Strategy definition, as it refers to the 'set of activities' to protect network and information systems.

[38] Article 4(1)(2) Directive (EU) 2016/1148 [7] 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 (L 194): "the ability (...) to resist (...) any action that compromises the availability,

measures for a high common level of cybersecurity across the Union"—suggests that it is no longer an issue of network information system security but of cybersecurity.

Notwithstanding this change in the title, the CSA and the new references to cybersecurity, the NIS 2 Directive proposal mirrors the above-mentioned terminological issues. As the European Data Protection Supervisor (EDPS) observed in its Opinion on the Cybersecurity Strategy and the NIS 2 Directive, the proposal demonstrates a lack of coherence in using the 'cybersecurity' and 'network and information systems security' terms.

The definition of 'national strategy on cybersecurity' in Article 4 of the NIS 2 Directive proposal may reflect this problem. The national strategy on cybersecurity is defined as "a coherent framework of a Member State providing strategic objectives and priorities on the *security of network and information systems* in that Member State" (emphasis added). However, this reference appears to be in contradiction with the CSA definition of cybersecurity since it refers to network and information systems when referring to national strategies on cybersecurity. Moreover, such a definition leaves aside the *individual protection* perspective referred to above. Consequently, such a provision seems to show that the two terms, in some instances, are used interchangeably [11, p. 12].[39]

This terminological issue in the proposal is important from doctrinal and conceptualisation perspectives. It is crucial as this change is there to affirm that cybersecurity is no longer meant as a network and information system issue, but is about the individual sphere. This is why, from a conceptual perspective, the final text of the NIS 2 Directive proposal must offer increased awareness of the different meanings between 'cybersecurity' and 'network information system security'.

The term 'cybersecurity', meaning 'a set of activities to protect network and information systems', should be used as a general rule to overcome this challenge. In contrast, 'security of network and information systems' should be used only when the context requires it, mainly technical. The use of more coherent wording in the NIS 2 Directive proposal (and any following acts relevant for cybersecurity) and preference for 'cybersecurity' as a general rule would pave the way for increased individuals' protection when affected by cyber threats and attacks.

4.4 Incoherent use of the term critical infrastructures

Another terminological issue concerns 'critical infrastructures'. As Markopolou and Konstantinos [24, p. 1] have illustrated, 'critical infrastructure' is an evolving concept reflecting the current concerns for responding to new challenges in terms of security and resilience envisaged by Member States. In the literature, critical infrastructures are usually defined as essential services to ensure the security and well-being of citizens [32]. They are considered 'critical' when their disruption could have an

authenticity, integrity or confidentiality of (...) data or the related services offered by, or accessible via, those network and information systems".

[39] There, the EDPS exemplifies Article 4(4) of the Proposal: 'national strategy on cybersecurity' means a "coherent framework of a Member State providing strategic objectives and priorities on the security of network and information systems in that Member State". See EDPS [11].

impact on the functioning of society in terms of economy, security and people's well-being [3].

Critical infrastructure protection is a matter of national legislation as a substantiation of EU sovereignty and subsidiarity principles. Although EU acts define 'European critical infrastructures' (Directive 2008/11/EC[40]), the definition and identification of critical infrastructure and their respective sectors are left at the Member State level and thus are not harmonised.[41] As some studies reported [34], the status of harmonisation concerning the physical protection of critical infrastructure across the EU is disparate, including the healthcare sector (*id.*; [3, p. 49]). However, such a lack of harmonisation at a national level may bring unexpected risks for the future application of the AI Act in healthcare.

The AI Act proposal refers to 'critical infrastructures' twice, in Recital 34 and Article 3(44)(b). Recital 34 suggests that for "the management and operation of critical infrastructures", it would be appropriate to classify "the AI systems intended to be used as safety components in the management and operation of road traffic and the supply of water, gas, heating and electricity" as high-risk systems (Recital 34 AI Act proposal). Article 2(44) AI Act proposal mentions critical infrastructures in the definition of serious incidents.[42] The possible regulatory challenges in this provision rely on referring broadly to 'critical infrastructures'. In fact, given that the identification of critical infrastructure is delegated to the Member States, and given that the Member States have different approaches in considering critical infrastructures (and healthcare as a critical infrastructure notably) in their legal systems, fragmentation risks may arise.

For instance, if a serious incident occurs to a high-risk AI system used as a safety component for healthcare critical infrastructure, there could be different consequences depending on the Member State in which the incident occurs. For example, if a Member State considers a healthcare service provider (i.e., a hospital) as a critical infrastructure, the provider of an AI system should notify the serious incident according to the AI Act proposal. On the contrary, if a Member State does not consider a hospital as critical infrastructure, the AI Act notification requirements would not apply. Consequently, the situation could result in a different level of protection for the affected individuals across the Member States. Individuals in a Member State not considering healthcare as a critical infrastructure could have a lower level of protection than individuals in a Member State considering healthcare as a critical

[40] The ECI Directive provides a definition of European Critical Infrastructure, see Article 2(1)(a) Council Directive 2008/114/EC [5] of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection OJ L 345: "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 thereof would have a significant impact in a Member State as a result of the failure to maintain those functions". It is worth noting that The ECI Directive has been be the subject of an evaluation process and review (see [3]).

[41] The current trends followed by Member States include the definition of critical infrastructure based on defence strategies, national emergency management and long-term national traditions. For an overview of critical infrastructure protection legislation—stemming from but not limited to the ECI Directive—in the healthcare sector see [3].

[42] See also *supra.*

infrastructure. Ultimately, such irregular application across the Member States could decrease protection against risks posed by AI systems to individuals' fundamental rights and safety across the EU, not to mention fragmentation risks in the internal market.

5 Recommendations and conclusions

Ensuring a high common level of cybersecurity across the European Union has become a key objective for the EU, testified to by the increasing number of cybersecurity-related legislation and requirements.

In this paper, we have presented how the introduction of new cybersecurity-related provisions may quickly bring new challenges, such as fragmentation risks (for critical infrastructures), regulatory uncertainty (concerning the MDR and AI Act proposal requirements) and overlapping (of the incident notification requirements) across the EU. We also noted that, in some cases, the use of broad concepts—even though considered by some advantageous [13, 24]—may also cause fragmentation and might lead to an uneven level of protection of individuals across Member States (i.e., 'cybersecurity' and 'critical infrastructures').

Following our analysis, the EU legislator should consider the subsequent recommendations to mitigate the risks mentioned above posed to the expanding regulatory framework concerning the cybersecurity of 'cyber-connected' medical devices.

First, clarify the meaning of '*at least equivalent*' in the NIS 2 Directive proposal's recitals. The legislator should explicitly indicate whether the MDR applies or prevails (as outlined *supra*) concerning incident notification. Specific examplifications of what constitutes serious medical device incidents *vis-à-vis* incident notification under the NIS Directive proposal should be assessed and explained via *ad hoc* guidance. These measures may help mitigate overlapping risks and foster a homogeneous interpretation of the future NIS 2 Directive requirements by Member States.

Second, expand explanatory remarks and recitals of the AI Act proposal in parts concerning the interaction between the AI Act and NLF, especially medical device safety requirements focusing on cybersecurity. Address convergence issues for serious incident notification explicitly in the text or future guidance. This could anticipate some regulatory uncertainty for medical device manufacturers in the future.

Third, adopt more coherent wording as regards 'cybersecurity' and 'network information system security' in the NIS 2 Directive proposal. As the EDPS already suggested, 'cybersecurity' should be used in general contexts, while 'network and information system security' should be referred to only in specific contexts (e.g., a purely technical one, without having regard to impacts also on users of systems and other persons). This would help strengthen the terminological coherence of cybersecurity in the new Directive, which should also prove beneficial for the forthcoming legislative pieces.

Fourth, limit to the extent possible the diverging interpretation of the term 'critical infrastructure' in the AI Act proposal to avoid the uneven application of the future Regulation at the Member State level. Further clarification and/or a reference to the healthcare sector for serious incidents in the AI Act could help reduce fragmentation

risks and thus promote an equal level of protection for individuals' fundamental rights in the EU.

Acknowledgements The authors would like to thank Dr. Patricia Vargas Leon, Prof. Dr. Scott Shackelford and Prof. Susan Landau for their remarks as discussant during the 2022 Tufts Student Symposium on Cybersecurity Policy. Special thanks also go to Dr. Griet Verhenneman for her comments on the manuscript's early draft, as well as to the anonymous reviewers. All errors are our own.

References

1. Biasin E, Kamenjašević E (2022) Cybersecurity of medical devices: regulatory challenges in the European Union. In Cohen I, Minssen T, Price II W, Robertson C, Shachar C (eds.) The future of medical device regulation: innovation and protection. Cambridge, Cambridge University Press, pp 51–62. https://doi.org/10.1017/9781108975452.005
2. Biasin E, Siapka (2020) A SAFECARE D3.10. Implementation of ethics, privacy and confidentiality. https://www.safecare-project.eu. Accessed 15 Mar 2022
3. Biasin E, Bresic D, Notermans P, Kamenjašević E SAFECARE D3.9 (2019) Analysis of ethics, privacy and confidentiality constraints. https://www.safecare-project.eu/?p=465. Accessed 15 Mar 2022
4. Cerulus L (2020) Hackers use fake WHO emails to exploit coronavirus fears. https://www.politico.eu/article/hackers-use-fake-who-emails-to-exploit-coronavirus-fears-for-gain/?fbclid=IwAR379JroScZEggppneFxEQqMpYfKP9M0Rg90k1lB-xziGkIH_3Byy1NtKjE. Accessed 8 Feb 2022
5. 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, O.J. (L 345/75) (ECI Directive)
6. DeNardis L (2020) The internet in everything. Freedom and security in a world with no off switch. Yale University Press, https://doi.org/10.2307/j.ctvt1sgc0
7. Directive (EU) 2016/1148of 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 O.J. (L 194)
8. Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC, 2014 O.J. (L 153)
9. Ducuing C (2021) Understanding the rule of prevalence in the NIS directive: C-ITS as a case study. Comput Law Secur Rev 40:1–12. https://doi.org/10.1016/j.clsr.2020.105514
10. Dumitrascu A (2020) A man-in-the-middle of my heart attack. https://ec.europa.eu/futurium/en/connect-university/man-middle-my-heart-attack-0.html. Accessed 8 Feb 2022
11. EDPS (2021on) Opinion 5/2021 on the cybersecurity strategy and the NIS 2.0 directive. https://edps.europa.eu/data-protection/our-work/publications/opinions/edps-opinion-cybersecurity-strategy-and-nis-20_en. Accessed 8 Feb 2022
12. ENISA (2012) National cyber security strategies—setting the course for national efforts to strengthen security in cyberspace. https://www.enisa.europa.eu/publications/cyber-security-strategies-paper. Accessed 8 Feb 2022
13. ENISA (2016) Definition of cybersecurity—gaps and overlaps in standardisation. https://www.enisa.europa.eu/publications/definition-of-cybersecurity. Accessed 8 Feb 2022
14. European Commission (2013) Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Cybersecurity strategy of the European Union: an open, safe and secure cyberspace, JOIN(2013) 1 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52013JC0001. Accessed 8 Feb 2022
15. European Commission (2017) Joint Communication to the European Parliament and the Council. Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU JOIN(2017) 450 Final. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52017JC0450. Accessed 8 Feb 2022
16. European Commission (2019) 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 Available via https://digital-strategy.ec.europa.eu/en/library/report-assessing-consistency-approaches-identification-operators-essential-services Accessed 8 Feb 2022

17. European Commission (2020) Combined evaluation roadmap/inception impact assessment revision of the NIS directive. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=PI_COM:Ares(2020)3320999&from=EN. Accessed 8 Feb 2022
18. European Commission's (2020) Proposal for a Regulation of the European Parliament and of The Council on a reinforced role for the European Medicines Agency in crisis preparedness and management for medicinal products and medical devices COM(2020)725. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020PC0727. Accessed 8 Feb 2022
19. Gartner M (2021) Why the prohibition of certain persuasive technologies in the European proposal for an artificial intelligence act is not a surprise. https://www.law.kuleuven.be/citip/blog/why-the-prohibition-of-certain-persuasive-technologies-in-the-european-proposal-for-an-artificial-intelligence-act-is-not-a-surprise/. Accessed 2 Feb 2022
20. González Fuster G, Jasmontaite L (2020) Cybersecurity regulation in the European Union: the digital, the critical and fundamental rights. In: Christen M, al (eds) The ethics of cybersecurity. Springer, Cham, pp 97–115. https://doi.org/10.1007/978-3-030-29053-5_5
21. Kasper A, Antonov A (2019) Towards Conceptualising EU Cybersecurity Law, Discussion Paper [C253 2019]. Center for European Integration Studies Rheinische Friedrich-Wilhelms Universität, Bonn
22. Lekshmi SA (2022) Growing concern on healthcare cyberattacks & need for cybersecurity. PsyArXiv. https://doi.org/10.31234/osf.io/7m4qf
23. Maia E et al (2020) Security Challenges for the Critical Infrastructures of the Healthcare Sector. In: Soldatos J et al (ed) Cyber-Physical Threat Intelligence for Critical Infrastructures Security: A Guide to Integrated Cyber-Physical Protection of Modern Critical Infrastructures. Now Publishers, Boston-Delft, pp 142–165. https://doi.org/10.1561/9781680836875
24. Markopoulou D, Papakonstantinou V (2021) 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. Comput Law Secur Rev 41:1–12. https://doi.org/10.1016/j.clsr.2020.105502
25. MDCG (2019a) Guidance on cybersecurity of medical devices. https://ec.europa.eu/docsroom/documents/41863. Accessed 8 Feb 2022
26. MDCG (2019b) Guidance on Qualification and Classification of Software in Regulation (EU) 2017/745 – MDR and Regulation (EU) 2017/746 – IVDR https://ec.europa.eu/docsroom/documents/37581. Accessed: 8 Feb 2022
27. MedTech (2021) MedTech Europe response to the open public consultation on the Proposal for an Artificial Intelligence Act (COM/2021/206). https://www.medtecheurope.org/news-and-events/news/medtech-europe-response-to-the-open-public-consultation-on-the-proposal-for-an-artificial-intelligence-act-com-2021-206/. Accessed 8 Feb 2022
28. Medicines & Healthcare products Regulatory Agency (2019) Virtual manufacturing of medical devices—Version 2.0. https://www.gov.uk/government/publications/medical-devices-virtual-manufacturing-replaces-own-brand-labelling/virtual-manufacturing-of-medical-devices. Accessed 8 Feb 2022
29. NIS Cooperation Group (2018) Reference document on Incident Notification for Operators of Essential Services—CG Publication 02/2018. https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53644. Accessed 8 Feb 2022
30. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), 2019 O.J. (L 151)
31. Rosager Ludvigsen K, Nagaraja S Dissecting liabilities in adversarial surgical robot failures: a national (Danish) and EU law perspective. https://arxiv.org/abs/2008.07381. Accessed 8 Feb 2022 (forthcoming)
32. Rinaldi SM et al (2000) Identifying, Understanding, and Analysing Critical Infrastructure Interdependencies. IEEE Control Syst Mag 4(6):11–25
33. Schwartz M (2020) COVID-19 complication: ransomware keeps hitting healthcare. https://www.bankinfosecurity.com/covid-19-complication-ransomware-keeps-hitting-hospitals-a-13941. Accessed 8 Feb 2022
34. THREATS (2014) 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