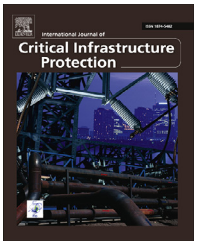
Available online at www.sciencedirect.com

ScienceDirect

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



Legally critical: Defining critical infrastructure in an interconnected world

Jakub Harašta

Faculty of Law, Masaryk University, Veveří 70, 611 80 Brno, Czech Republic

ARTICLE INFO

Article history:
Received 27 June 2016
Revised 29 August 2017
Accepted 31 May 2018
Available online xxx

Keywords:
Critical Infrastructure Protection
Legal Framework
Cyber Security
Interdependence
Critical Information Infrastructure

ABSTRACT

Cyber security becomes omnipresent within the society, stakeholders are taking actions necessary to reassure general public and to enhance the level of protection. One of the ways seems to be to incorporate cyber into existing frameworks for critical infrastructure protection. This text demonstrates how the introduction of cyber strains existing frameworks and demonstrates certain misconceptions on the case study of the legal change in the Czech Republic. Introducing cyber leads to selective choice of specific type of interdependency, while it ignores other significant types. The paper observes large discrepancy between the macro-level definitions and micro-level procedures and concludes that changes in the existing legal framework present a securitization exercise without significant added value.

1. Introduction

Cyber security becomes omnipresent within the present society, governments take actions necessary to reassure the public, enhance the level of protection of important public systems, and stimulate private businesses to do the same. The *Cyber Pearl Harbor* narrative [69], although disputed [49] or labeled as a hype [37], looms as a threat over the information society. States, non-state actors and criminal groups threaten to use our dependence on ICT to their advantage. In addition, terms such as *cyber war, information war, hybrid war or cyberterrorism* have become a significant part of vocabulary for military official and policy makers, and attracted significant attention from legal scholars [63,64].

Regardless of the factuality of the claims about the vulnerability of the information society, the perception of threats has changed – and so did the threats themselves. Our society depends on various ICT systems and their seemingly ever-growing sophistication and availability. With stronger reliance on Industrial Automation and Control Systems (IACS) for our critical infrastructure, cyber threats have become more acute in terms of their possible physical consequences. Cyber threats can manifest more frequently in their physical consequences and cause physical damage or casualties through cyber means. Attackers became able to turn off power grids and directly influence the physical reality through attacking the ICT layer of infrastructure, which we previously deemed impossible, or at least improbable to a large extent. Yet, we have witnessed the use of these methods, leading to physical consequences through code in a controlled environment [3], and we are encountering them in an operational environment as part of our new reality [27,38,55,71,72].

We have witnessed a sharp increase in attention towards critical infrastructure protection in the context of cyber threats during the last decade. The cyber security of critical infrastructure now receives wide international attention and is directly in the spotlight of the media. The cause probably lies in high-profile events operationalizing the cyber domain, such as the case of Estonia in 2007, which eventually lead to the establishment of the NATO Cooperative Cyber Defense Centre of Excellence in Tallinn and to a redefinition of the scope

E-mail address: jakub.harasta@law.muni.cz

https://doi.org/10.1016/j.ijcip.2018.05.007
1874-5482/© 2018 Elsevier B.V. All rights reserved.

of Art 5 of the Washington Treaty [31,39]. From more recent cases, it is possible to point out the case of Ukraine, where the prominence of cyber security rose during the War in Donbass and the related operations aimed at the Ukrainian critical infrastructure [27,29,72]. However, the idea of protecting often privately held but essential facilities became the focus of policy-makers and legislatures much earlier, as this paper will demonstrate.

First, the paper provides an overview of the legal and policy-based notion of criticality during the past two decades, as the concept still reflects some of this pedigree even today. It focuses predominantly on the U.S. and EU legal frameworks. The paper reviews the literature focused on the issues of interdependence of critical infrastructure. This topic has been largely covered by policy backed by empirical evidence, but has not been included in legal definitions, as their origin focuses on object-based protection. The paper then introduces and analyses the legislative effort to bring cyber interdependence into existing legal frameworks, using the example of the Czech Republic. The paper demonstrates how this development of legislation challenges the existing legally defined notion of criticality in critical infrastructure protection. Finally, the paper expands this development to argue for abandoning the isolationist object-based approach and creating sound legal frameworks for critical infrastructure protection. This paper addresses the perceived gap in literature by analyzing the legal notion of criticality in terms of the changed technological environment brought in by cyber.

Previous research has focused on interdependence from different perspectives. Kaska and Trinberg [33], and Moteff [48] focused mainly on policy analysis of the issue. Asselt et al. [2], and Lauta [36] included remarks on existing legal framework in their research, but mainly focused on risk analysis. Interdependence of critical infrastructure became pivotal topic for Rinaldi et al. [60], Zhang and Peeta [73], Dudenhoeffer et al. [13], Laugé et al. [35], and Pederson et al. [54]. Their works were mostly concerned with engineering or computer science, trying to achieve better modeling for purpose of critical infrastructure management and critical infrastructure protection.

The research as such has largely neglected analysis of legal frameworks in terms of definition of critical infrastructure. Therefore, this paper predominantly focuses on what is critical in terms of law, by employing desk-based analytical research, drawing inspiration partially from the existing research on how we establish what is critical outside the realm of law and how the law reflects on it.

2. Defining critical infrastructure

Cyber threats first received attention in the U.S. in 1996. At that time, the dependence on ICT systems and networks started to grow. The rate of growth and the overall dependence did not come close to what we experience today, but it already caused worries for policy-makers. The *President's Commission on Critical Infrastructure Protection* (PCCIP) was established in July, in order to report to President Clinton on any vulnerabilities in critical infrastructure with a primary focus on cyber threats [48]. PCCIP delivered its report in October 1997 [65] and noted there was no acute crisis in terms of cyber threats to the U.S. infrastructure. However, the PCCIP also pointed out that certain actions should be taken in order to prepare the U.S. for future development. Some dangers, stated the PCCIP, were inherent to the infrastructure. The main cause was the presence of uncontrolled interdependencies between critical infrastructure assets, arising from the fast technological development and affecting critical infrastructure both across sectors and within them.

This report was later followed by the Presidential Decision Directive No. 63, which set a national goal of protecting critical infrastructure from both physical and cyber threats. The situation then developed rather rapidly after 9/11 attacks, when the Patriot Act of 2001 introduced the legal definition of critical infrastructure. Critical infrastructure became defined by 42 USC 5195c(e) as *"systems and assets, whether physical of virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, of any combination of those matters."*

In this moment of extreme importance, the notion of criticality of critical infrastructure was given a legal definition for the first time. Although the accepted definition was seemingly all-encompassing and very broad in scope, it arose from policy discussions. Despite its vagueness, the definition gave us a general idea of the purpose of legislation on critical infrastructure protection, and captured the legal framework of critical infrastructure protection on a strategic level. The law aims to protect all assets critical for the nation, both stand-alone and closely interdependent or tightly coupled. The U.S. government then streamlined its activity to focus on critical infrastructure protection and its cyber security throughout both the remainder of Bush's administration and throughout Obama's administration [44,48].

Egan noted that the broad understanding of critical infrastructures is expanding and becoming very fluent with criticality of certain infrastructures periodically evolving and devolving [16]. Similarly, Pursiainen noted that earlier critical infrastructures were understood as stable and very specific – largely in terms of physical objects or very clearly delineated information and communication technology systems – while the post-9/11 era gave rise to a holistic conception [58]. The broad definition in the U.S. framework, arguably, rose from an anticipation of those tendencies in order to ensure its viability for a longer period. The general, vague definition can be accompanied by various lower-level legal rules or policy decisions that are more flexible and can more accurately reflect the current state of technology or the desires of the society. We can say that the definition is technology neutral (for explanation of term see pivotal works of Koops [34] and Reed [59]). The vagueness might be intentional – aimed to reflect the expected progress without need for extensive legislative changes.

The European Union (EU) accepted a similarly broad definition of critical infrastructure. The issue of security and protection of critical infrastructure received a significant amount of attention in the post-9/11 era. The notion of criticality started with the definition of an attack on critical infrastructure formulated by the Council of the European Union as *"causing extensive destruction of a Government or public facility, a transport system, an infrastructure facility, including an information system, a fixed platform located on the continental shelf, a* *public place or private property likely to endanger human life or result in major economic loss"* [23]. This definition established an essential distinction between income-generating and non-income-generating objects of protection [5], where the criticality is connected either with economic losses or casualties (see consequence-oriented definition of criticality in [57]). Later in 2004, after the attacks in Madrid, the European Commission released a communication [18] that reflected the challenges the modern security environment brought to critical infrastructure protection in a more knowledgeable manner. The communication explicitly noted not only a growing dependence of the society upon highly technological infrastructure, but also a growing interconnectedness of these infrastructures. Critical infrastructure was defined following the abovementioned distinction as *"those physical resources, services, and information technology facilities, networks and infrastructure assets, which, if disrupted or destroyed, would have a serious impact on the health safety, security or economic well-being of citizen or effective functioning of governments"* [18].

This strategic notion of criticality of critical infrastructure was not part of the legal framework yet, but the discussion was oriented towards outcomes similar to the one in the U.S. The EPCIP Green Paper [21] further delimited the term critical infrastructure to explicitly contain interdependent cyber and physical networks and objects which have a cultural and political significance, including mass events. Therefore, the definition broadened outside of physical installations (railroads, pipelines and power plants) to procedures – complex networks of socially and culturally determined values preceding and helping to operate heavy physical installations. These social- and culture-based procedures might be connected technologically, but the dissemination of these values will be largely mediated by technological means present in the information society. The EPCIP Green Paper brought the interdependence further into the strategic perception by differentiating between critical infrastructures and EU critical infrastructures [21]. The latter includes critical infrastructures which would affect several Member States of the EU through cross-border effects of rendered non-functionality.

These policy outcomes later transformed into a legislative process that brought the Directive 2008/114/EC [10] into life. The legislative distinction between critical infrastructure in general and EU critical infrastructure (critical infrastructure *sui generis*) respects the principle of subsidiarity of EU legislation. As such, the Directive did not prescribe any means of national critical infrastructure protection to the Member States. However, once national critical infrastructure became labeled as critical infrastructure *sui generis*, the Directive became applicable and set conditions aiming to prevent negative effects affecting neighboring EU Member States. EU critical infrastructure effectively consists of two sectors – energy and transport.

According to the Directive, 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"* [10]. EU critical infrastructure is then defined as *"critical infrastructure located in Member States the disruption or destruction of which would have a significant impact on at least two Member States. The significance of the impact shall be assessed in terms of cross-cutting criteria. This includes effects resulting from cross-sector dependencies on other types of infrastructure"* [10].

Similar to the U.S., the technology-proof thinking over the notion of criticality is apparent within the Directive. It is open-ended and largely aimed to contain any infrastructure, regardless of its form and shape, as long as its malfunction or loss negatively affects the nation (or several of them in case of EU critical infrastructure). These open-ended definitions provide us, at least in broad strokes, with a general idea of what governments understand as critical to their nations – or, to use the words of President Bush from National Strategy to Secure Cyberspace, what is essential to *"its economy, security, and way of life"* [67]. States are not perceived as comprised of its citizens, but rather as comprised of essential capacities provided to their citizens [14].

The broad and vague definitions described in the text above result from extensive discussions over policy and to a certain extent they reflect the possible technological progress and a holistic approach towards critical infrastructure protection. However, these general definitions require adequate and specific operative procedures [9]. When examining the Patriot Act of 2001 or the Directive 2008/114/EC, the definitions clearly aim at almost anything imaginable – system or asset, physical or virtual. These definitions base the notion of criticality on the function of infrastructure within the society, but as such, they provide for little guidance or legal ground for potential enforcement.

Law is inherently reductionist in its approach to reality. A multi-faceted and complex reality spans over endless possibilities, but it needs to be compartmentalized into a handful of boxes that arise from an existing legal framework. The broad legal definition of critical infrastructures would be too difficult to enforce and requires specific procedures that allow distinguishing infrastructure of any kind and critical infrastructure. Looking over the abovementioned broad definitions, the understanding of critical infrastructure is naturally negative. We perceive the criticality of infrastructure through the consequences of its absence – through subsequent loss or damage [5]. The same approach can be seen within the Directive – the identification of EU critical infrastructure follows the cross-cutting criteria of casualties, economic effects and public effects [10], which serve as operationalization of general broad definitions.

3. Accounting for the interdependence of critical infrastructure

Setting up criteria allows us to assess the negative impact in terms of numbers – hypothetical casualties can be counted, economic loss can be measured, hardship caused to inhabitants can be assessed. Even in the context of broad definitions, only these operative elements allow us to label any infrastructure "critical". Broad and all-encompassing definitions are suitable for policy or strategic legal thinking, but they need to be specified to facilitate administration and enforcement. However, the cross-cutting criteria we use for evaluation of harmful consequences do not allow us to

Please cite this article as: J. Harašta, Legally critical: Defining critical infrastructure in an interconnected world, International Journal of Critical Infrastructure Protection (2018), https://doi.org/10.1016/j.ijcip.2018.05.007

properly understand the interdependence between different critical infrastructures. Legal reduction of reality inherently leads us to an object-based protection – to label something as important and to administer it properly, we need to set up perimeters. Despite the general definitions seeking to ensure functionality (or more precisely seeking to avoid negative consequences caused by the loss of such function), operationalizing norms are focused on the protection of infrastructure supporting these functions.

The link between critical infrastructures is undisputed [44] and reflected in the broad definition of critical infrastructure. It contains both the cross-border dependencies and the dependence of critical infrastructures upon one another. This is, at least from the standpoint of policy and law, one of the least explored areas of vulnerabilities. Law and policy accounted for interdependence only superficially in setting up definitions. Attempts to understand it more in depth to allow for setting up lower-level norms providing more illustrative guidelines are very scarce [33].

However, this simplifying stance of selective ignorance towards the proper understanding of certain interdependent aspects is not applicable to engineering. The interdependency of critical infrastructures has received and continues to receive significant attention through both theoretical and empirical research. It has also led to the development of methodologies for describing and understanding the interdependence between critical infrastructures.

Rinaldi created one of the prominent methodologies in 2001 [60]. In a joint study with other researchers, he proposed a general framework for describing interdependence between infrastructures. According to this framework, various and highly diverse factors requiring consideration affect the function of critical infrastructures – some of these are, to a certain extent, also dynamic, which further complicates the description and understanding of the interdependencies between critical infrastructures. In order to ease and clarify the discussion, Rinaldi proposed six descriptive dimensions: the type of interdependency, the state of operation, the infrastructure characteristics, the type of failure, the coupling and response behavior and the environment. The types of interdependency most important for this analysis can be easily transferred from engineering into policy and legal discussion. According to Rinaldi, these contain distinguishable types of physical interdependence, cyber interdependence, geographic interdependence and logical interdependence.

These types describe interdependencies through a basic ontological distinction between their connections. Interdependence is based on a physical connection when a critical infrastructure directly or indirectly depends on a material output from another critical infrastructure [60] – e.g. in order to generate electricity, power plants need fuel (coal, fission materials). A cyber connection ensues in an interdependence when a critical infrastructure depends, again directly or indirectly, on information output from the other [60] – e.g. in order to operate a power plant properly, one needs to monitor and manage various operations within the system to regulate fuel supply, cooling or air conditioning. A geographic connection between critical infrastructures constitutes interdependence when two or more infrastructures share spatial proximity [60]. Despite a perceived similarity between the physical and geographic connection, these do not directly imply one another, although, at the same time, they are not mutually exclusive [50]. Geographic proximity can co-exist with both the physical and the cyber connection and all of these can therefore constitute different interdependencies – e.g. utilities being laid underground together (such as a heat supply and a water supply) or with other infrastructural elements (optical fiber cables). Finally, logical proximity serves as a sort of residual category [54], as it gives rise to interdependence without physical, cyber or geographical connections. It is often symbolized by a human decision regarding the policy and other regulatory frameworks [60] – it involves e.g. mergers [44] or pro-competition measures aiming to dissolve existing monopolies.

Despite the prominence of Rinaldi's methodology, it is not the only existing framework. Other methodologies, although they arise from a different background, reach to a certain extent a similar conclusion by encompassing the interdependence caused by the cyber connection. Zimmerman introduced the term functional interconnectedness and explicitly stated its particular relevance in face of the rapid evolution of information technologies [74]. Dudenhoeffer and his colleagues used the term informational interdependence and described it as dependence between critical infrastructures through the flow of information [13]. Functional interdependence then appeared once more with a more general meaning in the work of Zhang and Peeta – their functional interdependence contains any dependence of a critical infrastructure asset upon the input from another critical infrastructure asset [73]. All of these three notions can be understood as an equivalent to the cyber connection described in Rinaldi [51].

Regardless of the chosen methodology, either the interdependency through cyber connection receives special attention or its existence is generally acknowledged. The specific nature of cyber security can be seen as arising from these methodologies, because cyber is understood mainly as a medium through which communication occurs. Of course, this communication has different qualities [41]. Industrial Automation and Control Systems (IACS) systems are serving as a means for direct control, while other systems, such as a publicly accessible broadband infrastructure, are acting as information transport media. The broadband is inherently tied to information society, but it can hardly be said that it has the exact same role and function as IACS systems. In this regard IACS systems serve as a sort of qualified cyber systems and as such they currently receive significant attention.

However, the loss of function of an IACS system as such cannot *stricto sensu* cause a loss of human life and/or an economic loss in terms of criticality assessment. Any effect on reality that a malfunction of an IACS system can possibly have is indirect. It is caused by the fact that a system has lost its quality and is not able to control the related machinery properly (a pipeline valve, a power plant generator). This loss of quality can then cause physical damage and results in a countable negative impact for the purpose of cross-cutting criteria – the loss of a human life and/or economic loss [64]. An IACS system does not provide the society with electricity and it is not critical for the society on its own. Of course, it allows operators to control the critical infrastructure asset more efficiently or comfortably. But IACS systems still do not have a direct effect on reality as such – their effect is merely a second order of consequence of effects in the cyber domain [25]. And although the law has quite a strong tradition in ignoring conceptual differences established within other fields or even stemming directly from existing ontological differences, this omission is never entirely without consequences as there are plenty of examples in literature: for application of inherently tangible concept of property on ‘information’ see [70]; for sui generis database rights, see [6]; for copyright see [11]; for discussion on data as objects under international humanitarian law see [12,42]; and for data protection regime of human tissue and biobanks see [7] and [40].

Vague definitions lead us to the holistic approach that grants IACS systems the notion of criticality, because of their role in a specific function required by the society (such as energy distribution). On the other hand, lower-level norms lead us to object-based protection that requires specific infrastructure serving as a representation for the desired function itself. This claim becomes more apparent when we introduce the need for cyber security into the Czech legal framework of critical infrastructure protection.

4. The Czech Republic: legal framework for critical (information) infrastructure

As concluded above, both the U.S. and the EU have a broad definition of critical infrastructures, but the notion of criticality still has to be assessed by procedure provided by lower-level norms. EU introduced crosscutting criteria which allows us to measure the negative impact of the malfunction or destruction of respective infrastructure. This involves quantifying casualties and economic losses. However, introducing cyber security directly into the legal framework through the specific category of critical information infrastructure following this rationale results in discrepancies and tensions between broad, strategic-level definitions, and operative, lower-level norms.

The Czech Republic started taking its cyber security seriously around 2012. However, at the same time, it reached the decision to introduce what can be labeled as complex cyber security legislation. Due to special attention paid to the principles of regulatory minimization and proportionality the Cyber Security Act of 2014 [52] focuses largely on critical infrastructure protection. It amends the general critical infrastructure legislation and introduces the critical information infrastructure as a cyber component of critical infrastructure assets.

As mentioned above, in order for an infrastructure to be labeled as critical the Directive 2008/114/EC requires it fulfills one of the cross-cutting criteria of casualties, economic or public effects. The Czech transposition of this Directive consists of an amendment to the Crisis Act of 2000 [53] and the Government Regulation on Critical Infrastructures of 2010 [28].

The cross-cutting criteria set in the latter label infrastructure as critical once its estimated negative effect reaches more than 250 casualties or more than 2500 injured with a subsequent hospitalization longer than 24 h (human loss), the economic impact of the loss larger than 0.5% GDP (economic loss), or a large-scale limitation of necessary services or goods effectively affecting the everyday life of more than 125,000 people (public effect) [28,45]. However, these cross-cutting criteria are only the first step in identifying the critical infrastructure asset. The Czech legislation adds sectoral criteria that allow us to establish the criticality of infrastructure based on its perceived function. The sectoral criteria are established for 9 sectors – energy, water management, food industry and agriculture, health services, transport, communication and information systems, financial market and currency, and emergency services and public administration. Cyber security as such was missing from the existing legislation until the Cyber Security Act of 2014 came into effect on 1st January 2015.

The Cyber Security Act of 2014 was a result of the National Cyber Security Strategy 2012–2015, that set two main objectives: the creation of legal framework of institutionalized cyber security and the establishment of the National Cyber Security Centre. Since both objectives were effectively achieved during 2014 and 2015, the new National Cyber Security Strategy 2015–2020 mainly aims to deepen the cyber security commitment and further the development of a secure environment in the Czech Republic. Cyber security has found its way to various policy documents [46,47] and has become an essential part of the Czech security discourse.

The Act aimed to approach cyber security in a complex manner. Besides creating an institutional framework for incident information sharing and establishing national and governmental CERT teams, it also affected other legal instruments. As mentioned above, one of these legal instruments was the Government Regulation on Critical Infrastructures of 2010. The legislative solution of choice was to introduce a new subsector into the existing sector of communication and information systems with new sectoral criteria to reflect on cyber security. The criticality of information infrastructure is newly based on the fact that an information and communication system has a significant or full effect on the functioning of a critical infrastructure asset. Therefore, if the function of a critical infrastructure asset depends on an IACS system, the system itself is by this second order of criticality considered to be a critical information infrastructure asset. This notion of criticality directly correlates with the abovementioned interdependence caused by cyber connection. The relevant information and communication systems are not seen as critical on their own; their criticality is based on their direct control of or influence over another critical infrastructure asset which partially corresponds with the definition of critical infrastructure proposed in [21].

Therefore, with regard to all of the above, the identification of critical information infrastructure assets newly comprises of the three following steps:

1. Identification of critical sectors/services – the sectors are prescribed by the Government Regulation.
2. Identification of Critical Infrastructure assets within each critical sector – this involves an evaluation of whether the cross-cutting and sectoral-criteria are fulfilled.
3. Identification of Critical Information assets within each Critical Infrastructure asset – this involves an evaluation of whether a certain information and communication system affects any critical infrastructure asset or not.

This shift in legislation has occurred very recently, so it is quite difficult to assess its consequences. We still have to wait to fully conclude what kind of effect it has on critical infrastructure protection. However, the adjacent legislative changes on the operative level of critical infrastructure protection have raised certain questions about the existing legal framework and its role. The notion of criticality based on the assessment of cross-cutting criteria and sectoral criteria has a tendency towards object-based protection, because it perceives critical infrastructure assets as stand-alone representations of complex functions. It simply has to, since it is based on a reductionist legal approach, which has to facilitate administration and enforcement of broad definitions.

However, the Czech legal framework, valid since 1st January 2015, respects the dependence of critical information infrastructure assets on the critical infrastructure assets they supervise or control. But at the same time it does not tackle other types of interdependencies established by the abovementioned engineering methodologies. It selectively introduces a legislative solution of specific interdependence to further a policy goal. This legislative solution presents a missed opportunity to abandon the legislative origin tending to object-based protection and to bring the legal framework to terms with the interdependence of critical infrastructure.

Similar approach is present within current European legislative effort to harmonize the approach towards cyber security. Directive 2016/1148 [24] is not focused on critical infrastructures *per se*. However, there is a strong overlap between the scope of Directive 2016/1148 and the scope of Directive 2008/114/EC. As mentioned above, EU critical infrastructure established by Directive 2008/114/EC consists of two sectors – energy and transport. These two are present within the upcoming Directive 2016/1148 as well, but are also accompanied by other sectors that are not considered to be EU critical infrastructure sectors, but are often present within member states' scopes of critical infrastructure protection – namely banking, financial market infrastructures, health sector, drinking water supply and distribution and digital infrastructure [24]. Directive 2016/1148 introduced the new definition of operator of essential services in Art. 5(2), which is a public or private entity providing a service essential for the maintenance of critical societal and/or economic activities within abovementioned sectors. Similarly to existing Czech legislation, Directive 2016/1148 introduces tight coupling between physical and cyber. If the provision of essential services depends on network and information systems and an incident would have significant disruptive effects on the provision of that service, it falls under the scope of Directive 2016/1148 (more precisely under respective national legislation implementing the Directive). Therefore, the Directive 2016/1148 also selectively introduces a legislative solution of specific interdependence to further a policy goal.

5. Objects, processes, and law

When we look back to the definitions of critical infrastructure that appear in the U.S. and the EU legislation, the basic idea seems to be to ensure the definitions are as broad as possible. However, when it comes to the specific means that allows us to label an infrastructure as critical, the broad definition is narrowed down and prefers traditional physical infrastructures. Object-based protection stems from the Cold War attitude of protecting physical machinery. Despite the rapid emergence of cyber security in recent years, the general public still struggles with grasping what cyber security really means. Focusing on objects with firmly set perimeters is cognitively easy. It is also very kind to us in terms of law-in-books, as it allows us to set clear conditions within lower-level norms.

Thus, it can be said that the Czech amendment has tightly bound critical information assets together with their related critical infrastructure assets. Basically, it has stuck to an object-based protection that is closer to the stand-alone perception critical infrastructure has within its legal framework. Thus, the difference is that the object of protection now possesses both a physical part and a virtual part. Unfortunately, the appearance of the interdependence within the legal framework, although leading to a law that is less oblivious to the multi-faceted reality, has also led to a rise in institutional fragmentation [4]. The physical and virtual parts of the same object of protection are affected by different bodies. Security of the critical information infrastructure falls under jurisdiction of the National Security Authority (NSA CZ), while the physical part falls under jurisdiction of a different public body, depending on the sector to which the respective critical infrastructure belongs. For example in the case of a critical infrastructure asset from the energy sector, the physical part is being overseen by the Ministry of Industry and Commerce, while the linked critical information infrastructure asset is the responsibility of the NSA CZ. This dual-responsibility creates additional pressure, while at the same time, with cyber being the main interconnecting driver [41], critical infrastructure becomes more complex and interdependent than ever. This can lead to an increased vulnerability of critical infrastructure in the future.

An alternative solution to the rise of cyber within the legal framework of critical infrastructure protection would be to start over – meaning that the Czech legislative solution is burdened by its pedigree. It presents a typical conflict between trying to solve a legal challenge, but being bound by pre-existing limitations imposed by a former legal regime [8]. To start over would mean acknowledging that critical infrastructure protection is a wicked problem (see [61] for the term). Asselt et al. [2] stated that *"it is important to underline that CI risks are, unlike 'simple risks', complex and inherently ambiguous and may be highly uncertain"*. The issue is too complex because of high interdependency of critical infrastructure [68], which is further advanced by cyber security issues [43]. Trying to search for a solution by setting a legal framework inherently leads to the use of an authoritative strategy [62] for managing complex problems – which requires authority. Roberts [62] identified authoritative strategy, competitive strategy and collaborative strategy for solving wicked problems. The administrative reductionist solution aims to solve the problem by introducing a simple checkbox involving an assessment of cross-cutting and sectoral criteria. This allows us to tame the problem and escape its complexity [62]. The Czech legislative solution is viable, but it still creates objects by tightly coupling two critical infrastructure assets together and does not solve the complexity.

To overcome these limitations, we need to be able to reassess the concepts behind the existing legal framework for critical infrastructure protections. Instead of object-based protection, process-based protection should be introduced. It would allow us to focus on certain processes that are critical within the society by introducing the combination of physical assets, virtual assets and a complex interdependency evaluation. Instead of object-based protection, which is binary and essentially treats all protected infrastructure assets as indispensable, process-based protection would allow us to introduce a certain degree of resiliency. Instead of drawing borders and setting up perimeters, we would be able to focus on finding a solution to keep processes intact. Since cyber security is fixed to an inherently highly dynamic virtual environment, setting up a perfect defense, which is something we generally tend to aim for within object-based protection, is futile. Process-based protection would allow us to evaluate weak points and increase their redundancy to ensure a higher level of protection for critical infrastructure.

Emphasizing resilience within legal frameworks would undoubtedly abolish the reductionist approach to critical infrastructure protection we are currently witnessing, which stems from rise of newly emerging regulations and institutions [36]. However, a complex assessment of interdependence would eventually involve advanced calculations, which would turn the whole discussion even less understandable to the general public than it is now with its rather technical but simplistic legal framework. Lower-level norms of critical infrastructure protection would reflect the strategic level with its broad definitions more clearly. Applying complex models and simulations to the legal framework would involve significant legal bureaucracy and procedures within operative levels. It would also cast our ability to label infrastructure as critical into obscurity subjected to minimal transparency.

Another closely related issue would be introducing resilience into the legal framework. Involving resilience in critical infrastructure protection would mean admitting that a failure is possible [56], which is something we simply have to accept. Experts are aware of this because they tend to understand the dynamics of the cyber environment. However, it is something we are not really used to hearing about within the current critical infrastructure protection. The current legal environment with its binary perception of criticality and its object-based protection is soothing for the public due to its abovementioned cognitive simplicity. As explained by Dunn [15], process-based protection focuses on *"services, flows, their role and function for society, and especially core values that are delivered by infrastructures."* As such, it is far more abstract.

Given the conceptual problems we encounter while introducing cyber security with its inherent interconnectivity into the legal framework of critical infrastructure protection, we need to ask what the purpose of the existing framework really is. Its reductionist legal approach with a preference for simple administration is currently being challenged – object-based protection is easy to communicate and understand, but it is an over-simplification . On the other hand, a complex approach allowing us to understand what is going on would lead to obscurity for the general public – process-based protection would not soothe the public and would hand critical infrastructure protection over to complex engineering and mathematics. Moreover, since wicked problems have no stopping rule and no ultimate solution a complete understanding of process-based protection is impossible and its results would change rapidly in time, creating an environment without a legal certainty.

Transposing critical infrastructure protection to a legal discourse is immensely difficult and necessarily simplistic. Therefore, we have to search for a measure of conceptual simplicity that we introduce into the law. Every legal regulation has to have a purpose [32] that will justify the existence of the legislation and the shape it has received from the legislators. The perception of critical infrastructure legislation stems from its strategic level – these broad and all-encompassing definitions closely resemble policy documents. These definitions are so broad that lower-level norms have to be simplistic and oblivious to interdependence, as we see in the current framework. Another option is an engineering-driven approach with complex calculations and an admitted constant struggle for a solution. Both of these solutions are extreme in their nature and I assume that the real purpose of this legislation must lie somewhere else.

If we state that the purpose of the legislation is to protect critical infrastructure effectively and efficiently, the current Czech legal development suggests that our statement might be wrong and misguided. The law on its operative level does not sufficiently reflect the broad definition on a strategic level. Cross-cutting and sectoral criteria allow us to approach certain interdependencies selectively, but not to cover them exhaustively. To state one example, the cyber realm is prone to various interdependencies by its nature, also through interoperability, which we think of as beneficial. In order to facilitate interoperability and mutual communication between various systems, the whole infrastructure could eventually evolve into a technology monoculture, which is prone to common cause failure or cascade failure [26]. This interdependence is completely unaccounted for in the framework. Therefore, many systems directly connected to critical information infrastructure will just slide below the notion of criticality. Moreover, these issues span far beyond the Czech law – since this development occurred within the existing EU legal framework, we can draw some conclusion about its effect as well.

6. Conclusion

The problem as such is not the broad legal definition of criticality, but the large discrepancy between broad strategic-level definition and accompanying lower-level norms. These lower-level norms cannot reflect the sheer scope of the strategic-level definition. That being said, I believe the legal framework of critical infrastructure to be a continued securitization of the issue [1,30]. The broad definition of critical infrastructure as present within legal framework of EU [10,24] and, as demonstrated on the case of the Czech Republic [28,52,53], in its member states, furthers the securitization of the issue by labeling it as influential enough to move into the realm of law and to achieve institutionalization within its framework. Since the strategic level with its broad definitions has a purpose, simplistic lower-level norms are justified to a certain extent, because they allow for administration in the issue. Therefore, a legal framework of critical infrastructure protection does not present a significant legal value that needs to be maintained – it merely mirrors the lax or active role this issue plays within policy discussions. Since the existing strategies and policy documents often mention protection of critical infrastructure as one of its goals [17,19,20,22,66,67], legal framework is required to exist. It also eventually allows policy makers to fully apply a hands-off approach and hand the problem over to administrators (lawyers). Critical infrastructure protection and the precise position of the border between critical and non-critical is a sensitive topic, and passing it on to lawyers leads to an assignment of responsibility away from political decisions (which is the realm of critical infrastructure protection), as Lauta [36] and Asselt [2] have already warned.

Acknowledgment

I would like to gratefully acknowledge the generous support of the Minerva Center for the Rule of Law under Extreme Conditions at the Faculty of Law and Department of Geography and Environmental Studies, University of Haifa, Israel and of the Israeli Ministry of Science, Technology and Space. I am also very thankful to Pavel Loutocký for research assistance and to Matěj Myška for reading earlier drafts of this paper, and the anonymous reviewers and journal editors for their valuable comments and suggestions.

REFERENCES

[1] C. Aradau, Security that matters: Critical infrastructure and objects of protection, *Security Dialogue* vol. 415, pp. 491–514, 2010.
[2] M. van Asselt, E. Vos and I. Wildhaber, Some reflections on EU governance of critical infrastructure risks, *European Journal of Risk Regulation* vol. 62, pp. 185–190, 2015.
[3] S. Applegate, The dawn of kinetic cyber, in *5th International Conference on Cyber Conflict* K. Podins, J. Stinissen and M. Markus Eds., NATO CCD CoE Publications, Tallinn, Estonia, pp. 163–177, 2013.
[4] M. de Bruijne and M. van Eeten, Systems that should have failed: Critical infrastructure protection in an institutionally fragmented environment, *Journal of Contingencies and Crisis Management* vol. 151, pp. 18–29, 2007.
[5] P. Burgess, Social values and material threat: The European programme for critical infrastructure protection, *International Journal of Critical Infrastructures* vol. 33-4, pp. 471–487, 2007.
[6] L. Bygrave, Information concepts in law: Generic dreams and definitional daylight, *Oxford Journal of Legal Studies* vol. 351, pp. 91–120, 2015.
[7] L. Bygrave, The body as data? Biobank regulation via the 'Back Door' of data protection law, *Law, Innovation and Technology* vol. 21, pp. 1–25, 2010.
[8] B. Cherry, Institutional governance for essential industries under complexity: Providing resilience within the rule of law, *CommLaw Conspectus: Journal of Communications Law and Policy* vol. 171, pp. 1–32, 2008.
[9] D. Clemente, Cyber Security and Global Interdependence: What is Critical?, Royal Institute of International Affairs, London, United Kingdom, www.chathamhouse.org/sites/files/chathamhouse/public/Research/International%20Security/0213pr_cyber.pdf, 2013.
[10] Council of the European Union, Council Directive 2008/114/EC, on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, Brussels, Belgium, 2008.
[11] C. Craig, Technological neutrality: Preserving the purposes of copyright law, in *The Copyright Pentalogy: How the Supreme Court of Canada Shook the Foundations of Canadian Copyright Law* M. Geist Ed., University of Ottawa Press, Ottawa, Canada, pp. 271–305, 2013.
[12] H. Dinniss, The nature of objects: Targeting networks and the challenge of defining cyber military objectives, *Israeli Law Review* vol. 481, pp. 39–54, 2015.
[13] D. Dudenhoeffer, M. Permann and M. Manic, CIMS: A framework for infrastructure modeling and analysis, *Proceedings of the 2006 Winter Simulation Conference* pp. 478–485, 2006.
[14] M. Dunn and K. Kristensen, Introduction: Securing 'the Homeland': Critical infrastructure, risk and (In)Security, in *Securing 'the Homeland': Critical Infrastructure, Risk and (In)Security,* M. Dunn and K. Kristensen Eds., Routledge, London, United Kingdom, pp. 1–14, 2008.
[15] M. Dunn, Understanding critical information infrastructures: An elusive quest, in *International CIIP Handbook, Vol. II. Analyzing Issues, Challenges, and Prospects* M. Dunn and V. Mauer Eds., Swiss Federal Institute of Technology, Zurich, Switzerland, pp. 27–53, 2006.
[16] M. Egan, Anticipating future vulnerability: Defining characteristics of increasingly critical infrastructure-like systems, *Journal of Contingencies and Crisis Management* vol. 151, pp. 4–17, 2007.
[17] European Commission, Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions – A strategy for a Secure Information Society - "Dialogue, partnership and empowerment" COM2006 251 final, Brussels, Belgium, 2006.
[18] European Commission, Communication from the Commission to the Council and the European Parliament – Critical Infrastructure Protection in the fight against terrorism, COM2004 702 final, 2004.
[19] European Commission, 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 – "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience", COM2009 149 final, Brussels, Belgium, 2009.
[20] European Commission, 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 – "Achievements and next steps: towards global cyber-security", COM2011 163 final, Brussels, Belgium, 2011.
[21] European Commission, Green Paper on a European Programme for Critical Infrastructure Protection, COM2005 576 final, Brussels, Belgium, 2005.
[22] European Commission, 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, JOIN2013 1 final, Brussels, Belgium, 2013.
[23] European Commission, Proposal for a Council Framework Decision on Combatting Terrorism, COM2001 521 final, Brussels, Belgium, 2001.
[24] European Parliament and Council of the European Union, Directive EU No. 2016/1148 of the European Parliament and of the Council, concerning measures for a high common

level of security of network and information systems across the Union, Brussels, Belgium, 2016.

[25] R. Fanelli and G. Conti, A methodology for cyber operations targeting and control of collateral damage in the context of lawful armed conflict, in *4th International Conference on Cyber Conflict* C. Czosseck, R. Ottis and K. Ziolkowski Eds., NATO CCD CoE Publications, Tallinn, Estonia, pp. 319–331, 2012.

[26] D. Geer, Cybersecurity and national policy, *Harvard National Security Journal* vol. 11, p. i–xiv, 2010.

[27] K. Geers Ed., *Cyber War in Perspective: Russian Aggression against Ukraine* NATO CCD CoE Publications, Tallinn, Estonia, 2015.

[28] Government of the Czech Republic, Government Regulation no. 432/2010 Sb., on Criteria for the Determination of the Critical Infrastructure Assets, Prague, Czech Republic, 2010.

[29] E. Groll, Did Russia Knock Out Ukraine's Power Grid?, *Foreign Policy* foreignpolicy.com/2016/01/08/did-russia-knock-out-ukraines-power-grid/, January 8, 2016.

[30] L. Hansen and H. Nissenbaum, Digital disaster, cyber security, and the Copenhagen School, *International Studies Quarterly* vol. 534, pp. 1155–1175, 2009.

[31] U. Häussler, Cyber security and defence from the perspective of Articles 4 and 5 of the NATO Treaty, in *International Cybersecurity Legal & Policy Proceedings* T. Eneken and A.-M. Talihärm Eds., NATO CCD CoE Publications, Tallinn, pp. 100–125, 2010.

[32] M. Hildebrandt, Radbruch's Rechtsstaat and Schmitt's legal order: Legalism, legality and the Institution of Law, *Critical Analysis of Law* vol. 21, pp. 42–63, 2015.

[33] K. Kaska and L. Trinberg, Regulating Cross-Border Dependencies of Critical Information Infrastructure, NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia ccdcoe.org/sites/default/files/multimedia/pdf/CII_dependencies_2015.pdf, 2015.

[34] B.-J. Koops, Should ICT Regulation be Technology-Neutral?, in *Starting Points for ICT Regulation. Deconstructing Policy One-Liners* B.-J. Koops, M. Lips, C. Prins and M. Schellekens Eds., T.M.C. Asser Press, The Hague, The Netherlands, pp. 77–108, 2006.

[35] A. Laugé, J. Hernantes and J. Sarriegi, Critical infrastructure dependencies: A holistic, dynamic and quantitative approach, *International Journal of Critical Infrastructure Protection* vol. 8, pp. 16–23, 2015.

[36] K. Lauta, Regulating a moving nerve: On legally defining critical infrastructure, *European Journal of Risk Regulation* vol. 62, pp. 176–184, 2015.

[37] R. Lee and T. Rid, OMG Cyber!, *The RUSI Journal* vol. 1595, pp. 4–12, 2014.

[38] R. Lee, M. Assante and T. Conway, German Steel Mill Cyber Attack, SANS Institute, Swansea, United Kingdom ics.sans.org/media/ICS-CPPE-case-Study-2-German-Steelworks_Facility.pdf,
2015.

[39] J. Lewis, The Role of Offensive Cyber Operations in NATO's Collective Defence, NATO Cooperative Cyber Defence Center of Excellence, Tallinn, Estonia ccdcoe.org/sites/default/files/multimedia/pdf/TP_08_2015_0.pdf, 2015.

[40] S. Lewis, The tissue issue: A wicked problem, *Jurimetrics* vol. 482, pp. 193–216, 2008.

[41] E. Luiijf, H. Burger and M. Klaver, Critical Information Infrastructure Protection in the Netherlands, in *Lecture Notes in Informatics INFORMATIK 2003 – Mit Sicherheit Informatik, Schwerpunkt "Sicherheit – Schutz und Zuverlässigkeit"* R. Grimm, H. Keller and K. Rannenberg Eds., Gesellschaft für Informatik, Bonn, Germany, pp. 9–19, 2003.

[42] K. Mačák, Military Objectives 2.0: The case for interpreting computer data as objects under International Humanitarian Law, *Israeli Law Review* vol. 481, pp. 55–80, 2015.

[43] E. Malone and M. Malone, The "wicked problem" of cybersecurity policy: Analysis of United States and Canadian policy response, *Canadian Foreign Policy Journal* vol. 192, pp. 158–177, 2013.

[44] H. Menashri and G. Baram, Critical infrastructures and their interdependence in a cyber attack – The case of the U.S., *Military and Strategic Affairs* vol. 71, pp. 79–100, 2015.

[45] T. Minárik, National Cyber Security Organisation: Czech Republic, 2nd, revised edition, NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_CZE_032016.pdf, 2016.

[46] Ministry of Defence of the Czech Republic, The Long Term Perspective for Defence 2030, Prague, Czech Republic www.army.cz/images/id_8001_9000/8503/THE_LONG_TERM_PERSPECTIVE_FOR_DEFENCE_2030.pdf, 2015.

[47] Ministry of Foreign Affairs of the Czech Republic, Security Strategy of the Czech Republic, Prague, Czech Republic www.mzv.cz/public/2a/57/16/1375879_1259981_Security_Strategy_CZ_2015.pdf, 2015.

[48] J. Moteff, Critical Infrastructures: Background, Policy, and Implementation, Congressional Research Service, Washington, DC www.fas.org/sgp/crs/homesec/RL30153.pdf, 2015.

[49] J. Mueller and B. Friedman, The Cyberskeptics, CATO Institute, Washington, DC www.cato.org/research/cyberskeptics, 2014.

[50] T. O'Rourke, Critical infrastructure, interdependencies, and resilience, *The Bridge* vol. 371, pp. 22–29, 2007.

[51] M. Ouyang, Review on modeling and simulation of interdependent critical infrastructure systems, *Reliability Engineering & System Safety* vol. 121, pp. 43–60, 2014.

[52] Parliament of the Czech Republic, Act no. 181/2014 Sb., on Cyber Security, Prague, Czech Republic, 2014.

[53] Parliament of the Czech Republic, Act no. 240/2000 Sb., on Crisis Management, Prague, Czech Republic, 2000.

[54] P. Pederson, D. Dudenhoeffer, S. Hartley and M. Permann, Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research, Idaho National Laboratory, Idaho Falls, Idaho cip.management.dal.ca/publications/Critical%20Infrastructure%20Interdependency%20Modeling.pdf, 2006.

[55] I. Porche, J. Sollinger and S. McKay, A Cyberworm that Knows No Boundaries, RAND Corporation, Santa Monica, California www.rand.org/pubs/occasional_papers/OP342.html, 2011.

[56] M. Power, *The Risk Management of Everything. Rethinking the Politics of Uncertainty* Demos, London, United Kingdom, 2004.

[57] R. Prieto, Business community views, *Technology in Society* vol. 254, pp. 517–522, 2003.

[58] C. Pursiainen, The challenges for European critical infrastructure protection, *Journal of European Integration* vol. 316, pp. 721–739, 2009.

[59] C. Reed, Taking sides on technology neutrality, *ScriptED* vol. 43, pp. 263–284, 2007.

[60] S. Rinaldi, J. Peerenboom and T. Kelly, Identifying, understanding and analyzing critical infrastructure interdependencies, *IEEE Control Systems* vol. 216, pp. 11–25, 2001.

[61] H. Rittel and M. Webber, Dilemmas in a general theory of planning, *Policy Sciences* vol. 42, pp. 155–169, 1973.

[62] N. Roberts, Wicked problems and network approaches to resolution, *International Public Management Review* vol. 11, p. 1–19, 2000.

[63] M. Schmitt Ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* Cambridge University Press, Cambridge, United Kingdom, 2013.

[64] S. Shackelford and R. Andres, State responsibility for cyber attacks: Competing standards for a growing problem,

Georgetown Journal of International Law vol. 424, pp. 971–1016, 2011.

[65] The President's Commission on Critical Infrastructure Protection, Critical Foundations: Protecting America's Infrastructures, Washington, DC www.fas.org/sgp/library/pccip.pdf, 1997.

[66] The White House, National Security Strategy, Washington, DC ccdcoe.org/sites/default/files/strategy/USA_NSS2015.pdf, 2015.

[67] The White House, The National Strategy to Secure Cyberspace, Washington, DC www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf, 2003.

[68] W. Tolone and M. Armstrong, Integrated analytics: Understanding critical infrastructure behaviors for resilience analysis, *The Homeland Security Review* vol. 53, pp. 241–258, 2011.

[69] U.S. Department of Defense, Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, Washington, DC archive.defense.gov/transcripts/transcript.aspx?transcriptid=5136, 2012.

[70] H. Zech, Information as property, *JIPITEC – Journal of Intellectual Property, Information Technology and E-Commerce Law* vol. 63, pp. 192–197, 2015.

[71] K. Zetter, A Cyberattack has Caused Confirmed Physical Damage for the Second Time Ever, *Wired* www.wired.com/2015/01/german-steel-mill-hack-destruction, July 1, 2015.

[72] K. Zetter, Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid, *Wired* www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid, March 3, 2016.

[73] P. Zhang and S. Peeta, A generalized modeling framework to analyze interdependencies among infrastructure systems, *Transportation Research Part B: Methodological* vol. 453, pp. 553–579, 2011.

[74] R. Zimmerman, Social implication of infrastructure network interactions, *Journal of Urban Technology* vol. 83, pp. 97–119, 2001.

Please cite this article as: J. Harašta, Legally critical: Defining critical infrastructure in an interconnected world, International Journal of Critical Infrastructure Protection (2018), https://doi.org/10.1016/j.ijcip.2018.05.007