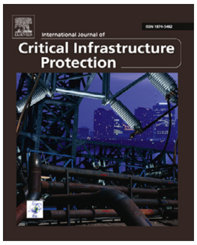
Available online at www.sciencedirect.com
ScienceDirect
journal homepage: www.elsevier.com/locate/IJCIP



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*