*sustainability*

MDPI

*Article*

# Critical Infrastructures: The Operational Environment in Cases of Severe Disruption

**Ossi Heino [1,*], Annina Takala [2], Pirjo Jukarainen [1], Joanna Kalalahti [1], Tuula Kekki [3] and Pekka Verho [4]**

[1] Research, Development and Innovation, Police University College, P.O. Box 123, FI-33721 Tampere, Finland; pirjo.jukarainen@poliisi.fi (P.J.); joanna.kalalahti@poliisi.fi (J.K.)

[2] Faculty of Built Environment, Tampere University, P.O. Box 600, FI-33014 Tampere, Finland; annina.takala@tuni.fi

[3] Research and Development, The Finnish National Rescue Association (SPEK), Ratamestarinkatu 11, 00520 Helsinki, Finland; tuula.kekki@spek.fi

[4] Faculty of Information Technology and Communication Sciences, Tampere University, P.O. Box 692, FI-33014 Tampere, Finland; pekka.verho@tuni.fi

* Correspondence: ossi.heino@poliisi.fi

Received: 21 December 2018; Accepted: 2 February 2019; Published: 6 February 2019

check for updates

**Abstract:** The functioning and resilience of modern societies have become more and more dependent on critical infrastructures. Severe disturbance to critical infrastructure is likely to reveal chaotic operational conditions, in which infrastructure service providers, emergency services, police, municipalities, and other key stakeholders must act effectively to minimize damages and restore normal operations. This paper aims to better understand this kind of operational environment resulting from, for example, a terrorist attack. It emphasizes mutual interdependencies among key stakeholders in such situations. The empirical contribution is based on observations from a workshop, in which participants representing the critical services and infrastructures in Finland discussed in thematic groups. Two scenarios guided the workshop discussions; nationwide electricity grid disruption and presumably intentionally contaminated water supply in a city. The results indicate that more attention should be paid to the interdependencies between critical infrastructures, as well as to the latent vulnerabilities hidden inside the systems. Furthermore, producing security seems to require continuous interaction and creation of meanings between extremely different actors and logics. This implies a need for changes in thinking, particularly concerning the ability to define problems across conventional administrative structures, geographical boundaries and conferred powers.

**Keywords:** critical infrastructure; resilience; interdependencies; water; energy; terrorism

## 1. Introduction

Today, approximately half of the world's population lives in urban areas, and it is assumed that urbanization will accelerate so that only one third will live outside urban areas by 2050 [1]. This development raises a variety of challenges that also impact the infrastructures, the reliable and effective functioning of which will determine how cities are able to respond to the demands of quality of life [2]. Some of these infrastructures are called 'critical' as societal well-being is fundamentally built on their reliability. They can be understood as the backbones of societal sustainability, safety and security of supply. The functioning of critical infrastructure impacts directly and indirectly on the prices of goods, economic competitiveness, public health, education, potential to fulfill oneself, and through all of these also societal resilience, i.e., the ability to cope and recover after crises [3–5]. Critical infrastructures provide people with access to a wide range of commodities, the availability of which is essential to the resilience of communities [6,7].

Alongside urbanization, technological networks that enable 'normal' and 'aspired' quality of life have grown in number and density while their importance has also been accentuated. As interconnectedness and interdependencies also grow, this means that the critical infrastructures are more vulnerable to systemic risks and the possibility of unpredictable and extensive failures [8]. The 'criticality' of critical infrastructures implies that more attention has to be paid to their security. Disruptions to critical infrastructures can have such strong and widespread effects that they can also deteriorate the public sense of security and trust in the structures and institutions that uphold social stability. Severe disruptions of critical infrastructure services can seriously challenge the general public's trust in the systems that have generally been seen as reliable and are expected to function efficiently in recovery after a crises [9].

This is where the interconnection of sustainability, security, and resilience is displayed in the context of critical infrastructure. Without delving too deeply into the meanings of these much used, and in many ways blurred, concepts, it can be said that their interconnections lie at the heart of societal development. Resilience has succeeded in bringing a new perspective to security discourses in which, instead of the classical probabilistic worldview, the underlying instability and the root cause of uncertainty are taken as the starting points [10]. Then again, resilience has often been applied too uncritically and as automatically good, whereas some safety investments made in the name of resilience have in fact reduced safety or hidden the resilient nature of various negative threads [11,12]. The concept of resilience has helped in understanding sustainability, and as a result, it has been possible to enhance the sustainability of systems by reinforcing their resilience. On the other hand, strong resilience has been shown to be the reason for the unsustainability of some systems [13]. It is also possible that sustainability and security can be pursued by reducing redundancy, which, as one of the essential aspects of complex infrastructure systems resilience, has produced systemic vulnerability and thus resulted in completely the opposite outcome [13]. Thus, resilience can be said to be focused on the adaptability of the system over a relatively short time span, while security and sustainability are broader and more far-reaching phenomena. The relationship between them is ambiguous. In any case, the infrastructures of urban environments are interesting in the sense that they are material compositions at the very heart of urban development, creating and modifying the ways and conditions of human co-existence [14]—they are the hard core of sustainability and security.

Severe disruption caused by humans, including terrorism, targeted at critical infrastructures undoubtedly shakes understandings of secure and sustainable living environments. Because of the essential role of critical infrastructures in society, it is easy to understand that an attack on them would match the terrorist modus operandi of causing severe disruption to societal stability. Furthermore, critical infrastructure has not been planned and built to take into account these kinds of human-induced threats. As Koppel maintains, it is difficult to add security aspects afterwards to a system that has not originally been planned to take these into account [15]. It is probable that in the case of intentional attacks and attempts to influence critical infrastructure, conventional risk preparedness will not suffice as the authorities' and utility service providers' operational environment will be considerably altered due to human threat. Thus, the central motivation of this paper is to better understand the operational environment in a situation where critical infrastructure is the target of terrorist activities or other intentional disturbance.

From the point of view of terrorism, urban environments are particularly tempting targets because cities can be seen as the nodes on the networks where people, value streams, ideas and information meet [16]. Coaffee argues, that particularly after the 9/11 terrorist attack, modern megacities have become the central scenes of terrorism as they offer a wide spectrum of economically, socially, and symbolically valuable targets and a suitable context for terrorism [17]. New forms of terrorism have revealed the vulnerabilities of urban areas and incited new forms of security production. Accordingly, it can be argued that terrorism is nowadays a part of urban redevelopment.

In addition to the fact that the operational environment is tainted by an ever more complex risk landscape, the actor network involved in preparing and responding to risks is also increasingly complex [18]. One key issue is how authorities and utility service providers are able to provide safety and security and restore normality after a severe disruption to critical infrastructure. An attack on critical infrastructure would expose unpredictable interdependencies and cause cascading effects that do not align according to the conventional structures and hierarchies of risk and safety management [19–22]. This kind of attack would challenge the vulnerabilities embedded in the conceptions of preparedness and the ability to respond both as separate entities and as part of a collaborative effort [23]; this kind of situation would, rather, necessitate self-direction, extended mandates, or even unauthorized solutions and require unforeseen capabilities within unusual roles. It would, e.g. urge authorities to exceed conferred powers, which is strictly forbidden and not even necessary in normal situations. Emergency management is primarily based on bureaucratic procedures; the strict orders, legal regulations, contingency plans, and operational guidelines are an important part of their justification and authorization. As discussed, severe disruption in critical infrastructure would challenge these premises and it is topic of interest in this paper.

This paper can be characterized as an examination of theory that is guided by empirical observations. The first goal of the paper is to illustrate the mutual interdependencies revealed by severe disturbances of critical infrastructure and thus to perceive the multi-actor situations that open up. The second goal, based on the preceding one, is to describe some of the key requirements of the main actors that emerge as a result of a serious disruption to critical infrastructure. As the paper progresses, excerpts from the empirical material are used to guide and concretize the theoretically oriented discussion.

The theme of this paper will be approached by first discussing the role and characteristics of critical infrastructure in modern societies. The empirical contribution of this paper is based on the KIVI project workshop focused on the vulnerability of critical infrastructure and the operational capability of authorities. The context and methodology are described in section three. The KIVI ("Vulnerability of critical infrastructure and operational capability of authorities") project aims to enable the anticipation of and preparedness for crises and disturbances of human origin, related to authorities and service providers of critical infrastructure. Results are discussed in section four by presenting an exploration of the key components of critical infrastructure from the point of view of severe intentional disruption. Lastly, the findings of this study are concluded in section five.

## 2. Critical Infrastructure as the Foundation of Normality and Security

To begin with, it is necessary to define what is meant by infrastructure and why some of it is considered to be socially critical. In this section, the definitions and most important aspects of critical infrastructure will be discussed.

### *2.1. Producing the Mundane*

By definition, infrastructures refer to structures that form the underlying base or background, enabling activities that happen in the front or above this base [24]. Infrastructures maintain the vital functions of society and regeneration, and make our everyday life foreseeable, safe and healthy. Infrastructures provide resources for the creation and renewal of everyday practices. They are, therefore, the material compositions that shape the spectrum of social practices. In shaping the dynamics of a daily life course, they impact what is considered to be normal and sufficient [25,26]. However, their wide-ranging benefits to societal and sustainable development do not always get the attention they deserve in decision-making processes [27]. As the impact of infrastructure has been embedded in mundane practices when they function as expected, they are simultaneously everywhere but not really anywhere.

The interweaving of infrastructures and social life—or the co-evolution of infrastructures and the society surrounding them [28]—results in the fact that the convenience, safety, and healthiness of everyday life are bound to, and our societal processes rely on the access to, infrastructures and their impeccability. Societies are thus increasingly vulnerable to disruptions in these infrastructures.

In other words, the more unreservedly everything relies on infrastructures, the more damaging their failures [29,30]. Infrastructures can thus become critical in relation to those who rely on them. Concretely, the criticality of an infrastructure can be assessed in the event of a disturbance, which reveals, in addition to technological vulnerabilities, how unreservedly the reliability of infrastructures is trusted. This is of particular interest because infrastructures are in many ways, and on many levels, interconnected and dependent on each other's existence and performance.

### 2.2. Criticality of Infrastructures

Some infrastructures are called critical when referring to their particular relevance or necessity. The US National Infrastructure Protection Plan 2013 [31] uses the following formulation to define critical infrastructure: "Systems and assets, whether physical or 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, or any combination of those matters". Following this definition, critical infrastructure plays an essential role, for example, in processes that are crucial for the functioning of society. They are therefore systems whose disruption or collapse would lead to serious consequences and crises of social order. Their criticality can be assessed by outlining the importance of a system for citizens, the economy or the ability of service providers to function. In this case, the factors to be taken into account in the assessment are factors related to the duration, extent, and absorption capacity of the system in case of disruption [32]. Criticality assessment can also be done by paying attention to, for example, system preparedness, interdependencies, dependence of people and activities on the systems, and relevant risks [33]. On the other hand, the definition of the criticality of infrastructures has expanded so that the systems can be called critical quite loosely. For example, Fjäder quite rightly asks: if everything is considered critical, is anything really critical anymore [34]? A similar position is maintained by Riedman, whose case studies suggest that in some cases the worst scenarios related to the so-called critical infrastructures, did not, in reality, cause particularly dramatic damage [35].

In Finland criticality is defined, for example, in the Criminal Code of Finland [36], according to which a sentence of criminal mischief is given for person who causes serious danger to "power supply, public health care, defense, administration of the law or another corresponding important societal function". Also in relation to data and communication offenses, the Criminal Code defines, with slightly different wording, actions that could endanger "the energy supply, general health care, national defense, the administration of justice or another function that is important to society and that is comparable to these".

### 2.3. Interdependencies

The aforementioned interconnection of systems is often referred to as interdependency, which, in the case of infrastructure systems, may occur between different types of systems, between different stages of system development, and between the different operational and maintenance phases of systems [37]. Interdependencies have a significant impact on the disruption dynamics of critical infrastructure. Due to the interdependencies, an abnormal event in one system may cause an impact somewhere else, which in turn may still cause further effects both to the original system and to other systems that are connected to it. Due to the interconnections and the socio-technical nature of critical infrastructure, disturbances can be very nonlinear and unforeseen. Interdependencies can act as an intensifying structure as they transport effects from different levels and places to others [38]. It is also worth noting that the diversity of systems, together with the interdependencies between them, make urban areas vulnerable to cascading effects [37].

Without discussing comprehensively cascading failures, it is worth mentioning some examples. The floods in Europe in 2002, the volcanic ash cloud created by the eruption of Eyjafjallajökull in 2010 and Hurricane Sandy in 2012 are all examples of cases where external shock caused by natural forces has caused significant cascading effects in addition to direct destruction. The power outage in Italy in

September 2003 and the Northeast blackout in the same year are examples of cases where a relatively small fault in the power plant, such as a software bug that activated in the alarm system, has had far-reaching effects. As Helbing points out, extreme events do not necessarily need a massive external shock to happen, but also the internal aspects of the system can transfer and escalate effects [8].

The interdependence of infrastructures was first highlighted in 1997, when the pioneering report Critical Foundations: Protecting America's Infrastructures was published by the President's Commission on Critical Infrastructure Protection (CIP). The report noted that national security, prosperity and social well-being depend on reliable infrastructures that are increasingly complex and interdependent [39]. For example, the National Infrastructure Protection Plan 2013 [31] defines dependency as "The one-directional reliance of an asset, system, network, or collection thereof—within or across sectors—on an input, interaction, or other requirement from other sources in order to function properly" and interdependency, respectively, as mutually reliant relationship between entities; the degree of interdependency does not need to be equal in both directions. Although 'dependencies' and 'interdependencies' are conceptually simple, as a phenomenon they are apt to increase the overall complexity of critical infrastructures dramatically and to impact the qualitative aspects of the risk and vulnerability landscape: First, the potential of cascading and escalating effects is increased. Second, it brings forth new kinds of vulnerabilities that are hidden in the qualities of interdependencies and the functionalities of various interfaces. Third, possibilities for intentional harm are also increased [40–42]. Various interdependencies may arise unnoticed when systems are designed, built and developed partly on the reliability of existing structures. In other words, it is not evident how and which other systems a system is dependent on.

Because interdependencies are a characteristic of critical infrastructures, they should also be perceived from a system-of-systems (SoS) perspective. SoS outlines the understanding of critical infrastructure as a joint formation of different components, each of which are large scale systems in their own right and can operate autonomously both technically and administratively. However, each subsystem is exposed to effects resulting from an impact to one or more other subsystems [43]. From this point of view, interaction is more important than the autonomous function [43], which motivated by systems and complexity theories, emphasizes the emergent interaction between the parts and the whole. Maier [44] emphasizes communication as a defining element of a SoS and information exchange as a prerequisite for its ability to organize. In this case, the focus is on the interfaces between different systems. The interactions and interdependencies of complex SoS systems also explain how a micro-level phenomenon can trigger dynamic processes leading to macro-level consequences [43,45,46].

In practice interdependencies are manifested, for example, when a seemingly insignificant disruption in one technical component is transmitted from one system, service, and process to another, eventually causing a severe threat to health and safety. It becomes obvious that a component level disruption may, in a suitable situation, trigger a chain reaction the final effects of which will only be seen after the interdependencies have materialized [47]. Pescaroli and Alexander outline a new perspective for understanding the vulnerability of critical infrastructures [48]. They apply the concept of panarchy referring to the dynamic interaction of the different layers of hierarchical systems. The disruption of critical infrastructure cascading to disaster can result from the vulnerabilities nested on various levels of the system. The connections in interdependent systems reinforce the structural weaknesses of these systems as they transmit these weaknesses from one level to another. In other words, a situation that escalates into a catastrophe does not need to be caused by a massive external shock, but a suitable combination of inner systemic vulnerabilities suffices [8,48]. A locally restricted component-level disruption may result in a series of non-linear development paths where the progression of the disturbances may occur faster than the recovery, and the scale of the consequences no longer correspond to scales of origin of the disturbance. In this sense, the issue of critical infrastructure security is also becoming a part of global economic and security themes [47]. Nonetheless, it is worth pointing out that the positive causal relationship between interdependencies and vulnerabilities is not always as self-evident as is implied, because of the impact of the topology of networked structures, cascade mechanisms, and interconnections of vulnerabilities between systems. In other words, it is possible that the increase in interdependencies actually reduces the risk of cascading failures [49].

### *2.4. Systemic Resilience*

When examined from the point of view of intentional disturbance it is worth noting that the interdependence of systems forms critical nodes whose adept exploitation can cause large-scale and profound consequences to the social order and trust with relatively small effort [50,51]. Thus, critical infrastructure needs to be included in the debate on terrorism and the means of combating it. Adapting Ulrich Beck's idea of a 'risk society', a rather fertile ground has been created for extensive intentional disturbance. It is important to note that the effects of critical infrastructure disruptions may today be different from those a few decades ago as the functions and processes, which rely on critical infrastructures, have increased and become more complex. Critical infrastructures as socio-technical systems not only provide security, healthiness, and convenience, but also increase the operational reliability of those processes that manage the interoperability of different systems. It is thus part of society's system for resilience.

In this context, the resilience of critical infrastructure is seen as the system's ability to absorb disruption effects and to reorganize to maintain crucial functions, the most necessary structures and identity [52]. According to Little, the magnitude and intensity of the consequences of critical infrastructure disruptions depend on the quality of the interference, the number, and nature of the interdependences, the redundancy in the systems and the available capacity to produce countermeasures to restore the situation [53]. In this sense, the issue is also linked to the management of critical infrastructure as it has a crucial effect on the systemic vulnerability of systems with interdependencies [18]. Resilience cannot therefore be seen solely as a technocratic or sector-specific reduction, but rather as a cross-border and socially charged concept [54]. Referring to "the tragedy of the commons" phenomenon, Haimes examines the resilience of interdependent infrastructure systems from the SoS perspective, and illustrates how the different missions, goals, and schedules of different actors alone constitute a collection of human factors whose discordance with other interdependent systems' can have a significant impact on the functioning of a given SoS [43]. In this sense, the challenge is precisely to see the integration of one's own activities into entities of which no one has complete knowledge.

The impacts of management solutions are not always obvious. There are latent vulnerabilities and resident pathogens that occur during the design, construction and operation of critical infrastructures. They are hidden inside the systems for long periods of time and appear as unexpected components when disruptions cascade and the situation escalates [55–57]. In other words, there are always causal factors of a severe disruption embedded in critical infrastructure. These are invisible and inactive in normal conditions but still embedded in the depths of the socio-technical systems, waiting to be triggered when the conditions are favorable. These latent vulnerabilities determine the spread and escalation of the consequences of disturbances [8,48,58]. As Pescaroli and Alexander point out, in a system susceptible to cascade effects the magnitude of systemic vulnerabilities is more defining than the magnitude of the original phenomenon [38]. Although the triggering of cascading disruptions cannot generally be predicted, their potential can be integrated into preparedness and resilience thinking. In this respect, resilience is also the ability to ensure that the system is not overwhelmed by latent vulnerabilities.

## 3. Methodology

The main empirical material for this paper was collected in a workshop organized at the Police University College in Tampere, Finland, in January 2018 in association with a steering group meeting of the KIVI project. The workshop was facilitated by a modified Open Space method. As an orientation to the workshop, the participants were introduced to two different scenario-based exercises that reflected the model for comprehensive security defined in the national Security Strategy for Society [59] and related to the vulnerabilities identified in the National Risk Assessment 2015 [60]. In the first scenario, participants tackled a case in which a nationwide electricity grid disruption occurs in the freezing conditions of late December. The second scenario presented a situation where presumably intentionally contaminated drinking water causes serious illness and disease in a city. Both cases were severe, abnormal situations but not (yet) formally defined "states of emergency" which would have an impact on the powers of the authorities.

Unlike the original Open Space method participants did not suggest topics for discussion; instead they were invited to discuss under four preliminary prepared topics. Three of these derived from the Security Strategy for Society: formation of situation picture/awareness, competencies and resources in crisis management and crisis communications [59]. In addition to these participants were invited to provide support for the development of a new kind of self-assessment tool in terms of continuity management. In line with the Open Space method, participants were allowed to move freely between the topics (discussion groups). Researchers from the KIVI project facilitated, recorded and later analyzed and transcribed the discussions.

The workshop participants represented the following Finnish organizations: Energy Authority, Fingrid (Finland's electricity transmission system operator), Finnish Energy, the Finnish Red Cross, the Finnish Water Utilities Association, Helsinki City Rescue Department, Police University College, National Emergency Supply Agency, Tampere University of Technology, the Finnish National Rescue Association, the National Cyber Security Centre of Finnish Communications Regulatory Authority, the National Police Board, the Pirkanmaa Safety and Security Cluster, and the Security Committee. The total number of participants was sixteen. The participants represented the key actors who would be involved in scenarios such as those discussed in the workshop.

Although this paper does not deal with the case of Finland per se, it is appropriate to briefly describe the concept of security in a Finnish context, as this can be assumed to contribute to the shaping of the workshop participants' thinking processes and methods. In 2012, the Government of Finland gave a Resolution on Comprehensive Security, which emphasized the networking of society, the interconnection of threats and the consequent difficulty of forecasting. According to this, securing of critical societal functions should be carried out in collaboration between the authorities, the business sector and citizens. The Government Resolution on Comprehensive Security covers the management of disruptions, including measures taken by the responsible authority, mutual assistance between authorities, and ensuring the information exchange between the various parties to produce up-to-date situational awareness and make relevant decisions. However, Branders, in her doctoral dissertation, points out that the idea of comprehensive security takes a view that all identified security threats could be managed [61]; this differs from our view in this paper, which emphasizes systems' ability to cope in general and in particular with unpredictability.

As the workshop participants were experts responsible for preparedness actions, civil protection and/or represented organizations vital for the security of supply, much of the collected information is confidential or security sensitive. Protecting such information is an absolute prerequisite for carrying out research, and has an impact on the publishing of the results [62] (pp. 257–264). Therefore, in this paper, phenomena are treated in a way and at a level that respects the requirements of enhanced security but still strives to deepen our understanding of the phenomena being examined.

One more thing needs to be taken into account. The kinds of phenomena that are of interest in this paper are such that there is limited amount of experience of them. Thus, the situations that emerge from the workshop scenarios are novel, and discussion is based on the creative adaptation of prior experience and knowledge. It is assumed, that the workshop experts, with their vast experience, have a sophisticated understanding of many of the structural features related to critical infrastructures and their disruptions. However, the analysis provides only a limited view of the development needs for preparedness. Rather, this paper contributes to the preliminary analysis and exemplification of the research topic. Ultimately, this paper seeks to find the building blocks of the logic that determines either success or failure in the case of a severe disruption of critical infrastructure.

## 4. Critical Infrastructure in the Face of Severe Disruptions

In this section we examine the results based on the workshop discussions. Direct excerpts from the empirical material provide examples of the discussions and thus concretize the theoretically oriented results. First, attention is turned to the challenging operational environment that emerges as a result of severe disruptions to critical infrastructure. Second, the role and formation of situational awareness in decision-making are considered. Third, the new challenges facing critical infrastructure sectors are explored and their impact on vulnerability is discussed. Fourth, the potentiality of critical infrastructure as a target of terrorist attack is given serious consideration.

### *4.1. Disruption Requires an Innovative Search for Resources and Competencies*

As mentioned earlier, the convenience of modern everyday life is based on many self-evident structures. A good example of this is critical infrastructure that as a collaborative socio-technical system helps to produce normality. When it works as expected, no single service, function, or actor is distinguished from the whole that it is a collaborative part of. Such a requirement for collaboration exists in both normal and exceptional situations, but it is noteworthy that the participating actors may vary depending on the situation. An actor that is perceived as an 'outsider' in normal situations can become an important collaborator in exceptional situations. In the workshop, participants discussed the multi-actor situation emerging from the scenarios:

> "This isn't only for the police, but it is for multiple authorities. Even if there was a crime committed and that belongs in police jurisdiction there is still stuff that concerns public health, social services and what not. This would require all sorts of arrangements. I mean, this whole [city district] would be uninhabitable. And public health services, one hospital cannot cope with all these patients. This would require a collaborative effort from several authorities to get people to some habitable place."

It is noteworthy that exceptional circumstances necessitate effective collaboration even if the actors are institutionally fragmented. Critical infrastructures have been the subject of substantial reform and change over the last decades. As part of fragmented urbanism, the management of critical infrastructures has shifted to the hands of highly specialized professional groups [63]. This has enabled each group to focus on maintaining and enhancing their own area of expertise. The underlying problem of this development is that the understanding of systemic vulnerabilities has deteriorated.

Through fragmentation, the security and resilience of critical infrastructures are largely seen as an inter-organizational issues, i.e., processes formed in various contractual networks and interaction relationships. Then again, the deterioration of the understanding of systemic entities suggests that connections to the meta-strategies of comprehensive security are weakened. If this is true, seeing infrastructure management as part of the context of internal and external security, the prevention of terrorism and crisis management become increasingly distant. To counteract this, the Nordic countries, for example, have been striving to reinforce the principles of comprehensive security and a broader concept of security that interweave public administration, business, non-governmental organizations, and citizens to improve the resilience of society [64]. The role of such actors may be vital in exceptional situations; they may be essential for continuity even if they are not thought to be relevant when designing systems or managing them in normal situations.

A further feature of a severe disturbance in critical infrastructure is that many of the resources needed by key actors will become inadequate with respect to the level of needs in the situation. At the same time as the available resources and information seem inadequate decisions should be taken to manage the situation and to protect citizens. One example of this was manifested as the workshop participants discussed the congestion of the emergency response centre and the decision-making pressure in the water scenario.

> "112 [emergency number] will probably be congested just by the relevant phone calls, as there will be so many of them. And then the capacity, I have to get back to the fact that there is no such resource that if in real life an area of this size was badly polluted that there would be any chance to have a system to treat the patients. [ . . . ] Of course, there are antidotes for the poison, but how quickly can they be taken into use, well, I suspect it won't be very quick."

> "In these situations, there's a need to make big decisions very rapidly. Prohibition of water use, closing water taps, moving people, full mandatory evacuation at some point . . . well, I wouldn't want to be the one making these decisions."

### *4.2. Shared Situational Awareness and Collaborative Sense-Making Are a Necessity*

One major theme in the workshop discussions was the formation of a situational picture and awareness. In normal situations much of the information is such that one specific actor can keep it to him or herself, but in a case of disturbance this information must be efficiently shared so that decision-making can be based on appropriate understanding of the overall situation. Participants in the workshop maintained that the formation of more or less uniform situational awareness is a key prerequisite for decision-making. It is noteworthy, however, that the preconditions for the shared situational awareness are formed long before the real need for information exchange and joint analysis materializes; preconditions are comprised of operational practices and cultures, levels of trust, judicial frameworks, and their interpretations.

> "It would be absolutely essential that we could make the right conclusions. After the right conclusions have been made, it is a different story what happens then. But the point is how to reach the [conclusions], you will most definitely need information from other actors. [ . . . ] Once we have formed the right situation picture and awareness only then can action proceed and the right measures be taken. Before that it is quite unclear."

> "This comes down to the fact of how well the cooperation between the healthcare, the police and the rescue has been built, so that a situation picture can be formed. Environmental health [department], water utility, all these [actors]."

> "And then, how can this be identified as regional or local. So, how do different provinces and hospital districts talk to each other? So, the formation of a kind of nationwide picture of this, on top of everything."

Multiagency situational awareness and a picture are the essential elements in decision-making when talking about the ability of key actors to function in dynamically changing operating environments such as in the case of critical infrastructure disruptions. For example, Pescaroli emphasizes the importance of access to information and the preconditions for establishing a dialogue in coordinating cooperation [19]. Baber and McMaster talk about 'collaborative sensemaking' highlighting that it is important not only to participate in the information gathering and sharing processes, but also to understand who should be involved in these processes [65] (p. 14). It is necessary so that the key actors can effectively focus scarce resources on the most important issues. Baber and McMaster further point out that the idea of collaborative sensemaking is not to ensure that each actor has the same schema and knowledge structure as the knowledge needs and the responses generated based on the information are actor-specific [65] (p. 66–69). In other words, it needs to be noted that the situational awareness has a tendency to develop from interaction between actors, and each actor has their own interpretation of the emerging patterns and no one can claim sole ownership for them. One workshop participant discussed this issue in the following way:

> "This is an important question. We have been thinking about this a lot in our organization. Should an authority that is generally responsible for leadership in the situation be sharing its own situation picture or an overall shared situation picture? If it shares its own picture, other actors may not understand anything about it. [...] When every sector has their own language (and mode of action) that others do not understand. It would be good to get them into understandable language and to all the important actors. But it really requires that you are in touch with each other and talk about what the situation actually is. If one authority, let's say rescue, tries to make a situation picture of its own, then it goes down the drain."

As can be seen in the above citation, the multi-actor situation opened up by the severe disruption of critical infrastructure also causes management challenges. The widespread nature of the effects of disruption complicates the division of tasks and responsibilities, especially in situations where no prior experience exists. But above all, the difficulty is accentuated by the change of context: if, in a normal situation, critical infrastructure systems can be seen as technical objects severe disruption forces them to be examined anew. Working in the framework of comprehensive security, collaboration and shared situational awareness is not just a continuation of normal activities, but a different way of thinking. It was also emphasized that, instead of exclusively sector-specific tasks and responsibilities, key actors also have common requirements necessitating collaboration. A severe disruption brings forth actors whose ability to contribute to a collaborative set-up is essential to the system's ability to recover. Such capabilities are determined as the disruption is triggered and the scale and severity of the situation begin to become evident. As Boin and Smith point out, it is not even always evident from the beginning, which infrastructures and actors prove to be critical in a particular case [66]. The disruption reveals actors whose functional capacity is essential for the recovery and functioning of the entire system of collaboration.

The communication and information processing practices adopted by organizations are also latent factors in the system, which may, in the face of severe disruption weaken the collaborative capabilities of actors [56]. Their consequences may become tangible when collaboration is needed, even though they might have previously been difficult to identify and out of the reach of the established ways of thinking and traditional risk management. When looking at the communication of organizations, the focus should therefore be on the interdependencies, collaborative sensemaking and the presence of ignorance and unpredictability [65,67]. Workshop participants illustrate the difficulty of sharing information with an example of health care in a situation where information related to the state of health and symptoms should be rapidly dispersed:

> "If we are now thinking about the health side of things, for example. When in a situation described by the scenario, the patient is brought in, so he trusts that information will not be revealed, but that health issues are kept secret. There may be a big threshold to give out information."

> "And what really interferes with much of the cooperation, even between authorities, are these privacy protections; they cannot share information about people with each other. It is a continuous problem, especially in major accidents. Help does not reach those in need because of these information security challenges."

### *4.3. Threats against the Cyber Domain Have Increasingly Serious Repercussions in Urban Environments*

In addition to the characteristic interdependencies of critical infrastructures, it needs to be noted that due to the development and strengthening of automation and telecommunications technology, the systems are ever more merged into the ubiquitous 'social fabric'. With smart technologies, the Internet of Things (IoTs), automation of transportations, and so on, algorithms that guide telecommunications and operations have become part of the foundation of modern living. At the same time, they offer additional opportunities for intentional criminal mischief and terrorist acts. One workshop participant describes a denial-of-service attack and points out, for example, how individual households may unintentionally become part of the attack.

> "There was recently this one case where a boiler had supposedly been hacked. But in reality the case was that the boiler was directly connected to the Internet, and when it was online, a malware that scanned only IoTs with vulnerabilities, got access to the boiler and started a denial-of-service attack on the other side of the world. And as the boiler is not designed for that, it crashed. So, there needs to be no direct cyber influence on the boiler, but it can still be involved with something else inadvertently. And the big problem is that when the number of devices online is growing so damn fast, and no manufacturer of refrigerators has probably done any software before, they are bound to repeat the mistakes made by IT experts a long time ago. So the quality of the software can go back to the beginning of the 1990s and all the same basic problems will return. Then we have a terrible pile of crappy devices. And, as a result of these enormous amounts of devices, the attack potential will become huge. Denial-of-service attacks can be made with a large number of inefficient devices."

The effects of the development of telecommunications technology are most evident in urban environments. A person in the city is inadvertently served by a number of different IT systems. Industrial systems that are controlled over the Internet have also been incorporated into critical infrastructure management. Simply put, increasing numbers of people, devices, and objects are interconnected. The structural functionality of modern cities is thus also defined by the underlying algorithms, software and their security. Due to this threat, discussion of management and safeguarding of critical infrastructure has incorporated terms like cyber warfare and cyber terrorism [68,69].

This development has provided undeniable benefits, but it has also increased the potential for hybrid influencing in densely populated urban environments, where attacks on computer networks and infrastructures are not only harmful due to increased dependency of digitalized services, but can also be effectively combined with other methods of hostile influencing. Hybrid influencing refers to the coordinated use of economic, political or military means such as cyber, physical, and economic operations. The term hybridity emphasizes the attempt to combine two or more commonly separately used systems to produce the desired synergistic effects [70]. This also manifests the fact that critical infrastructure is seen as a potential target and in some cases an instrument of terrorism.

### *4.4. Potential Terrorist Target*

As a severe disruption of critical infrastructure is likely to cause widespread and profound implications for the convenience and security of everyday life, inflicting disruptions can be seen as a means of causing deliberate harm [71]. In addition to direct and immediate impacts, attacks on critical infrastructure would undermine the stability-maintaining structures and create a climate of insecurity; it would be a psychological shock that would have an impact on people's sense of fear and attitudes towards governance to a much larger extent than the actual attack [72–74]. Like any purposeful organization, terrorist groups seek to find cost-effective solutions that could produce the desired effect, such as harnessing the leverage of social structures to advance their own agenda. Critical infrastructure, with all its interdependencies, forms a metasystem of societal welfare, and by intervening in its functionality, it is possible to turn the system against itself [75,76]. Thus, the sophistication of society also means increasing its vulnerability; the strength, progression, and capacity of a system are at the same time its Achilles heel [76].

If one thinks about water services, the context of one of the scenarios covered in the workshops, modern societies have invested heavily in order to organize water services so that that they cover as large a part of the population as possible, and the quality is high. People can trust the quality of the water services. Intentional contamination of drinking water, for example, biologically or chemically would alter the systems producing public health and mundane convenience to a system spreading disease, death, mistrust, and fear in a way that would make it one of the most effective instruments for terrorism [75,77,78]. From a mechanical point of view, the system would work impeccably, but its ultimate purpose and quality would have been manipulated. According to Meinhard, the intentional contamination of water would also cause unforeseen difficulties for health care [79]. This kind of a situation would create an operational environment where the central actors have hardly any prior experience, and where the element of surprise is of considerable proportions [80].

> "As a citizen, I think that this would cause such horror. When there is no clear cause [of illnesses and deaths] known, then that is the most horrible situation. And the doubt of whether I can count on the authorities to tell me the truth. One starts to doubt everything. [...] Then the rumors break out that this is terrorism or what is it?"

Critical infrastructure can thus be seen as a structure that intensifies disruptions and social distrust, and therefore it is an interesting instrument from the point of view of terrorists [81–86]. In this regard, one dimension when assessing the criticality of critical infrastructure should be the extent of impact one can achieve by changing the functional identity of the system. By exploiting critical infrastructure, terrorists can manifest and symbolize the vulnerability of social order. At the same time, the influence would target structures that are present in the formation of everyday well-being and terrorists would thus be able to convey a psychologically important message that no one is safe [73].

The potential of critical infrastructure to be the target is increased by the terrorist tendency to attack so-called soft targets, the tendency to increase the complexity of attacks, and the tendency to maximize the number of victims [66,87–90]. When targeting critical infrastructure, the aim would be to cause disruption to services that people strongly rely on, and to undermine citizens' confidence in the ability of government to protect citizens [72]. This has been manifested by the terrorist attacks in Madrid in 2004 and a year later in London. In this sense, it is not particularly surprising that according to intelligence data the water services networks, in addition to other critical infrastructures, have been identified as objects of interest for terrorist organizations [91,92]. The participants of the working group note that the intentionality of the disruption impacts the way it is handled:

> "Yes, this is a really tricky case, even though one could identify the toxic substance, but to identify the cause to be able to do something about it. But the reason behind it will also impact what is to be done, what to prepare for and what places to protect."

> "The nasty thing when dealing with human beings is that if they don't get caught, then they can continue. In that sense, the cause does not disappear before that person has been found."

If critical infrastructure were the target of a terrorist attack, this would mean a very different kind of operational logic in comparison to cases with disturbance caused by, for example, a storm, malfunction, or human error. When the cause is of intentional human origin, then the cause responds actively and intelligently at least in the light of its own purpose. As a result, restoring the situation becomes essentially more difficult. Awareness that the attacker is intentionally trying to cause damage has an impact on the restoration process. In addition, scarce resources would be needed not only to deal with the acute disruption and its effects in a life-threatening environment, but also to anticipate and prepare for possible future strikes. For example, the terrorist attacks in Paris in November 2015 illustrated how in the case of one attack, the authorities had to focus their attention on the potential for subsequent strikes that could occur, for example, on the other side of a metropolis. Moreover, because of the human origin of the disturbance, the possibility of hybrid operations cannot be excluded; concrete physical attacks can be prepared for a long time by a continuous means of influence to maximize the desired effect.

## 5. Conclusions

Looking at urban environments and critical infrastructures as their central components, it can be seen that sustainability is linked to securing the preconditions of continuity and development. The focus is on the creation and maintenance of vitality, and avoidance of societal collapse, whether it is a fast or slow process [93]. Adapting Romero-Lankao et al. [94], it can be said that urban sustainability, security and resilience surface from a dialogue about desired futures. This paper has examined this very broad and complex issue in the context of critical infrastructure vulnerability and disruption. It is time to sum up the key findings of this paper and reflect on the future directions they provide in the framework of security, sustainability, and resilience.

First, it is necessary to underline the intensification of complexity, the importance of which is particularly emphasized in urban areas. Interconnected systems construct fertile soil for disruptions to spread through cascade-effects. For example, Helbing describes this phenomenon through the concepts of systemic risk and hyper-risk, where the number of possible cascade paths and non-linearity are characteristic [8]. The situation is twofold in the sense that, on the one hand, there is a strong aspiration in society, with the help of risk management and contingency planning, to prevent the emergence of catastrophes and curb their adverse effects. On the other hand, this orientation, together with the development of society, lays the groundwork for even worse vulnerabilities. This is mostly a matter of improving performance in the field of modern threat scenarios and the realities of the operational environment, which differs from the more traditional risk management field in which critical infrastructure producers and other key actors have demonstrated their capacities [95]. In this regard, it could be argued that strengthening resilience requires understanding that the traditional way of tackling vulnerabilities through identification, knowledge and management does not do the trick in a world of systemic and interdependent vulnerabilities.

Second, this paper illustrated the socio-technical nature of critical infrastructures. A severe disruption in the system can go beyond geographical, organizational, and administrative boundaries, thus activating a multifaceted set of actors whose ability to collaborate is required to restore the situation. The workshop discussions illustrated some of the challenges associated with the coordination of various human subsystems. For example, the importance of reliable, up-to-date information from other key actors was highlighted throughout the discussions as a driving force for their own actions. The primary guiding principle seems to be that taking the necessary action requires the presence of sufficient certainty. In this regard, it is argued that strengthening resilience requires understanding that the information available in a situation of severe disruption to critical infrastructure may inevitably be undesirable both in quantity and quality, but still the expectations and requirements for the effective management of the situation remain. The required activity may not be able to claim legitimacy from established administrative-legal institutions, so the ability to cross different conventional boundaries becomes one of the factors determining the resilience of the overall system. Producing security requires continuous interaction and creation of meanings between extremely different actors and logics.

Third, the importance of the preparedness and contingency thinking is emphasized. As Kachali et al. point out, a preparedness perspective going beyond sectoral boundaries should be integrated in the development of activities [18]. The challenge is that the development of the activities is often driven by the calculations between the inputs and the benefits gained, but the benefits of taking the preparedness perspective are not realized in concrete sense. Their realization is, at best, that the unwanted does not happen. In general, the causal relationships between inputs and non-occurrence are not easily perceived. In addition, even when the benefits are manifest, they are not known at the investment stage. From the point of view of the input-output perspective, preparedness may at worst appear as a no-win situation. In this regard, it can be stated that the strengthening of resilience requires understanding that the development of functions from the point of view of normal situations does not necessarily say much about the capacity to perform in exceptional circumstances. As noted in the workshop discussions, the severe disturbance of critical infrastructure is likely to create an operational environment in which many of the things that are taken for granted in normal circumstances are called into question. These observations also align with the SoS-perspective formulated by Haimes, according to which such complex SoS emergent properties should guide the processes of strategic preparedness, response and recovery. These emergent features are "system features that are not designed in advance, but rapidly evolve based on sequences of events that create the motivation and responses that ultimately develop into features characterizing the Complex SoS.” [43] (p. 667).

Fourth, the paper also emphasized that the sectors of critical infrastructure should be prepared to fight and also to face the attacks organized by a malicious actor whether it be of governmental origin or something else. Producing security and sustainability in this context would seem to require the ability of key players to perceive themselves as a networked organization. However, the idea of a networked organization is not easily adopted by the authorities, infrastructure producers and other key players. In line with the SoS typology by Maier [44], the issue is, especially for the authorities, how essentially ‘directed’ systems that are based on the implementation of specific goals in a centralized manner, are able to adapt the methods of ‘collaborative’ systems, where systems have to work more or less voluntarily on a common goal. However, the need for a more networked ‘defense’ is emphasized in the face of the development of threats such as organized crime, hybrid action and terrorism in an increasingly networked, diverse and technically sophisticated direction. For example, Simon argues that the next wave of terrorism will be heavily technology-inspired, turning the power of society’s own technological advancement against itself [96]. Information and communication technologies are one aspect of this; i.e., cyber terrorism, whereby interest is focused firstly on cyber-attacks against the critical infrastructure control systems, and secondly, on “cyber facilitated” terrorism, in which the idea is to utilize cyber in the planning of a traditional attack and to enhance its impacts. In this sense, enhancing the resilience of a system necessitates new ways to protect and produce safety. The introduction of critical infrastructure into the context of terrorism reflects the idea discussed throughout this paper that what makes our society stronger also weakens it. It should also be noted that the established ways of producing security are not necessarily suited to the new challenges. To conclude, it can be said that societal development itself has inspired an operating environment in which the limitations of systemic understanding can become the main vulnerability of our time.

**Author Contributions:** The authors have contributed to the article accordingly: conceptualization, O.H.; methodology, O.H., A.T. and P.J.; investigation, O.H., P.J., J.K., T.K. and P.V.; writing—original draft preparation, O.H. and A.T.; writing—review and editing, O.H, P.J. and A.T; project administration, P.J.

**Funding:** This research was funded by Academy of Finland (decision no: 315074) and The European Union [Internal Security Fund (ISF) of EU Home Affairs Funds (project no: SMDno-2016-1525)].

**Acknowledgments:** The authors want to express their gratitude to the workshop participants. In addition, the authors wish to thank the anonymous reviewers whose comments helped to significantly improve this paper.

**Conflicts of Interest:** The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, or in the decision to publish the results.

## References

1. UN (United Nations). World Urbanization Prospects: The 2018 Revision, Key Facts. 2018. Available online: https://population.un.org/wup/Publications/Files/WUP2018-KeyFacts.pdf (accessed on 10 November 2018).
2. Riffat, S.; Powell, R.; Aydin, D. Future cities and environmental sustainability. *Future Cities Environ.* **2016**, *2*, 1–23. [CrossRef]
3. Palei, T. Assessing the Impact of Infrastructure on Economic Growth and Global Competitiveness. *Procedia Econ. Finance* **2015**, *23*, 168–175. [CrossRef]

4. Bell, S. Engineers, Society, and Sustainability. In *Synthesis Lectures on Engineers, Technology, and Society*; Morgan & Claypool Publishers: San Rafael, CA, USA, 2011; ISBN 978-1-6084-5790-8.
5. National Research Council. *Sustainable Critical Infrastructure Systems: A Framework for Meeting 21st Century Imperatives*; National Academies Press: Washington, DC, USA, 2009; ISBN 978-0-309-13792-8.
6. Hay, A.H.; Willibald, S. Making Resilience Accessible. Access: An Enabler of Community Resilience. Southern Harbour. 2017. Available online: https://www.southernharbour.net/assets/docs/SH_Access%20WhitePaper_2017_0307%C6%92.pdf (accessed on 14 January 2019).
7. Hay, A. Surviving catastrophic events: Stimulating community resilience. In *Infrastructure Risk and Resilience: Transportation*; IET: Stevenage, UK, 2013; pp. 41–46.
8. Helbing, D. Globally networked risks and how to respond. *Nature* **2013**, *497*, 51–59. [CrossRef] [PubMed]
9. Petersen, L.; Fallou, L.; Reilly, P.; Serafinelli, E. Public expectations of critical infrastructure operators in times of crisis. *Sustain. Resil. Infrastruct.* **2018**. [CrossRef]
10. Lay, E.; Branlat, M. Noticing Brittleness, Designing for Resilience. In *Becoming Resilient: Resilience Engineering in Practice*; Nemeth, C.P., Hollnagel, E., Eds.; Ashgate: Farnham, UK, 2014; Volume 2, pp. 139–155. ISBN 9781472425164.
11. Brassett, J.; Vaughan-Williams, N. Security and the performative politics of resilience: Critical infrastructure protection and humanitarian emergency preparedness. *Secur. Dialogue* **2015**, *46*, 32–50. [CrossRef]
12. Berkes, F.; Ross, H. Community Resilience: Toward and Integrated Approach. *Soc. Nat. Resour.* **2013**, *26*, 5–20. [CrossRef]
13. Saunders, W.S.A.; Becker, J.S. A discussion of resilience and sustainability: Land use planning recovery from the Canterbury earthquake sequence, New Zealand. *Int. J. Disaster Risk Reduct.* **2015**, *14*, 73–81. [CrossRef]
14. Coward, M. Between us in the City: Materiality, Subjectivity, and Community in the Era of Global Urbanization. *Environ. Plan. D Soc. Space* **2012**, *30*, 468–481. [CrossRef]
15. Koppel, T. *Lights Out: A Cyberattack, a Nation Unprepared, Surviving the Aftermath*; Crown Publishers: New York, NY, USA, 2015; ISBN 978-0-553-41996-2.
16. Smelser, N.J. *The Faces of Terrorism. Social and Psychological Dimensions*; Princeton University Press: Princeton, NJ, USA, 2007; ISBN 978-0-691-13308-9.
17. Coaffee, J. *Terrorism, Risk and the Global City. Towards Urban Resilience*; Ashgate: Farnham, UK, 2009; ISBN 978-0-7546-9046-7.
18. Kachali, H.; Storsjö, I.; Haavisto, I.; Kovács, G. Inter-sectoral preparedness and mitigation for networked risks and cascading effects. *Int. J. Disaster Risk Reduct.* **2018**, *30*, 281–291. [CrossRef]
19. Pescaroli, G. Perceptions of cascading risk and interconnected failures in emergency planning: Implications for operational resilience and policy making. *Int. J. Disaster Risk Reduct.* **2018**, *30*, 269–280. [CrossRef]
20. Pescaroli, G.; Nones, M.; Galbusera, L.; Alexander, D. Understanding and mitigating cascading crises in the global interconnected system. *Int. J. Disaster Risk Reduct.* **2018**, *30*, 159–163. [CrossRef]
21. Chang, S.E.; McDaniels, T.; Fox, J.; Dhariwal, R.; Longstaff, H. Toward Disaster-Resilient Cities: Characterizing Resilience of Infrastructure Systems with Expert Judgments. *Risk Anal.* **2014**, *34*, 416–434. [CrossRef] [PubMed]
22. Luiijf, E.; Klaver, M. Insufficient situational awareness about critical infrastructures by emergency management. In Proceedings of the NATIO Symposium on C31 for Crisis, Emergency and Consequence Management, Bucharest, Romania, 11–12 May 2009; pp. 1–10.
23. Boin, A.; McConnell, A. Preparing for Critical Infrastructure Breakdowns. *J. Conting. Crisis Manag.* **2007**, *15*, 50–59. [CrossRef]
24. Edwards, P.N.; Jackson, S.J.; Bowker, G.C.; Williams, R. Introduction: An Agenda for Infrastructure Studies. *J. Assoc. Inf. Syst.* **2009**, *10*, 364–374. [CrossRef]
25. Shove, E.; Watson, M.T.; Spurling, N. Conceptualising connections: Energy demand, infrastructures and social practices. *Eur. J. Soc. Theory* **2015**, *18*, 274–287. [CrossRef]
26. Hand, M.; Shove, E.; Southerton, D. Explaining Showering: A Discussion of the Material, Conventional, and Temporal Dimensions of Practice. *Sociol. Res. Online* **2005**, *10*. [CrossRef]
27. Langdon, M.; Gillott, M.; Rodrigues, L.; Parry, T. The case for internalising externalities in a sustainable rail asset base. *Infrastruct. Asset Manag.* **2016**, *3*, 97–105. [CrossRef]
28. Ramaswamy, V.; Ozcan, K. *The Co-creation Paradigm*; Stanford University Press: Redwood City, CA, USA, 2014; ISBN 978-0-8047-9075-8.

29. Graham, S.; McFarlane, C. *Infrastructural Lives: Urban Infrastructure in Context*; Routledge: Oxon, UK, 2015; ISBN 978-1-315-77509-8.
30. Trentmann, F. Disruption is normal: Blackouts, Breakdowns and the Elasticity of Everyday Life. In *Time, Consumption and Everyday Life. Practice, Materiality and Culture*; Shove, E., Trentmann, F., Wilk, R., Eds.; Berg: Oxford, UK, 2009; pp. 67–84. ISBN 978-184788-365-0.
31. NIPP. Partnering for Critical Infrastructure Security and Resilience. Homeland Security. 2013. Available online: https://www.dhs.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf (accessed on 10 January 2019).
32. Fekete, A. Common criteria for the assessment of critical infrastructures. *Int. J. Disaster Risk Sci.* **2011**, *2*, 15–24. [CrossRef]
33. Katina, P.F.; Hester, P.T. Systemic determination of infrastructure criticality. *Int. J. Crit. Infrastruct.* **2013**, *9*, 211–225. [CrossRef]
34. Fjäder, C.O. National Security in Hyper-connected World. In *Exploring the Security Landscape: Non-Traditional Security Challenges*; Masys, A.J., Ed.; Springer International Publishing: Cham, Switzerland, 2016; pp. 31–58. ISBN 978-3-319-27914-5.
35. Riedman, D. Questioning the Criticality of Critical Infrastructure: A Case Study Analysis. Homeland Security Affairs. 2016, Volume 12. Available online: https://www.hsaj.org/articles/10578 (accessed on 14 January 2019).
36. The Criminal Code of Finland 39/1889, Amendments up to 766/2015 Included (Translation from Finnish). FINLEX Database, Ministry of Justice. Available online: https://www.finlex.fi/en/laki/kaannokset/1889/en18890039_20150766.pdf (accessed on 10 January 2019).
37. Alinizzi, M.; Chen, S.; Labi, S.; Kandil, A. A Methodology to Account for One-Way Infrastructure Interdependency in Preservation Activity Scheduling. *Comput.-Aided Civil Infrastruct. Eng.* **2018**, *33*, 905–925. [CrossRef]
38. Pescaroli, G.; Alexander, D. A definition of cascading disasters and cascading effects: Going beyond the "toppling dominos" metaphor. *Planet@Risk* **2015**, *2*, 58–67.
39. Critical Foundations. Protecting America's Infrastructures: The Report of the President's Commission on Critical Infrastructure Protection. 1997. Available online: https://fas.org/sgp/library/pccip.pdf (accessed on 10 January 2019).
40. Peerenboom, J.P.; Fisher, R.E. System and sector interdependencies: An overview. In *Wiley Handbook of Science and Technology for Homeland Security*; Voeller, J.G., Ed.; John Wiley & Sons: Hoboken, NJ, USA, 2010; pp. 1161–1171. ISBN 978-0-471-76130-3.
41. Macaulay, T. *Critical Infrastructure: Understanding Its Component Parts, Vulnerabilities, Operating Risks, and Interdependencies*; CRC Press: Boca Raton, FL, USA, 2009; ISBN 9781420068351.
42. Rinaldi, S.M.; Peerenboom, J.P.; Kelly, T.K. Control Systems, IEEEIdentifying, Understanding, and Analyzing Critical Infrastructure Interdependencies. *IEEE Control Syst.* **2001**, *21*, 11–25. [CrossRef]
43. Haimes, Y.Y. *Modeling and Managing Interdependent Complex Systems of Systems*; John Wiley & Sons, Inc.: Hoboken, NJ, USA, 2019; ISBN 9781119173700.
44. Maier, M.W. Architecting Principles for System of Systems. *Syst. Eng.* **1998**, *1*, 267–284. [CrossRef]
45. Thissen, W.A.H.; Herder, P.M. System of Systems Perspectives on Infrastructures. In *System of Systems Engineering. Innovations for the 21st Century*; Jamshidi, M., Ed.; John Wiley & Sons, Inc.: Hoboken, NJ, USA, 2009; pp. 257–274. ISBN 978-0-470-19590.
46. Eusgeld, I.; Nan, C.; Dietz, S. "System-of-systems" approach for interdependent critical infrastructures. *Reliab. Eng. Syst. Saf.* **2011**, *96*, 679–686. [CrossRef]
47. Xu, T.; Masys, A.J. Critical Infrastructure Vulnerabilities: Embracing a Network Mindset. In *Exploring the Security Landscape: Non-Traditional Security Challenges*; Masys, A.J., Ed.; Springer International Publishing: Cham, Switzerland, 2016; pp. 177–194. ISBN 978-3-319-27914-5.
48. Pescaroli, G.; Alexander, D. Critical infrastructure, panarchies and the vulnerability paths of cascading disasters. *Nat. Hazards* **2016**, *82*, 175–192. [CrossRef]
49. Korkali, M.; Veneman, J.G.; Tivnan, B.F.; Bagrow, J.P.; Hines, D.H. Reducing Cascading Failure Risk by Increasing Infrastructure Network Interdependence. *Sci. Rep.* **2017**, *7*, 44499. [CrossRef]
50. Bennett, B.T. *Understanding, Assessing, and Responding to Terrorism. Protecting Critical Infrastructure and Personnel*; John Wiley & Sons: Hoboken, NJ, USA, 2007; ISBN 978-0-471-77152-4.

51. Dobson, I. Analysis of cascading infrastructure failures. In *Wiley Handbook of Science and Technology for Homeland Security*; Voeller, J.G., Ed.; John Wiley & Sons: Hoboken, NJ, USA, 2010; pp. 1334–1343. ISBN 978-0-471-76130-3.
52. Folke, C. Resilience: The emergence of a perspective for social-ecological systems analyses. *Glob. Environ. Chang.* **2006**, *16*, 253–267. [CrossRef]
53. Little, R.G. Controlling Cascading Failure: Understanding the Vulnerabilities of Interconnected Infrastructures. *J. Urban Technol.* **2002**, *9*, 109–123. [CrossRef]
54. Rodina, L. Defining "water resilience": Debates, concepts, approaches, and gaps. *WIREs Water* **2018**. [CrossRef]
55. Masys, A.J. Critical Infrastructure and Vulnerability: A Relational Analysis through Actor Network Theory. In *Networks and Network Analysis for Defence and Security*; Masys, A.J., Ed.; Springer: Cham, Switzerland, 2014; pp. 265–280. ISBN 978-3-319-04147-6.
56. Maurino, D.E.; Reason, J.; Johnston, N.; Lee, R.B. *Beyond Aviation Human Factors*; Routledge: New York, NY, USA, 2016; ISBN 978-1840149487.
57. Alpaslan, C.M.; Mitroff, I.I. *Swans, Swine, and Swindlers. Coping with the Growing Threat of Mega-Crises and Mega-Messes*; Stanford University Press: Stanford, CA, USA, 2011; ISBN 978-0-8047-7137-5.
58. Alexander, D. A magnitude scale for cascading disaster. *Int. J. Disaster Risk Reduct.* **2018**, *30*, 180–185. [CrossRef]
59. *Security Strategy for Society: Government Resolution*; The Security Committee: Helsinki, Finland, 2017; ISBN 978-951-25-2963-6.
60. *National Risk Assessment 2015*; Ministry of the Interior Publication: Helsinki, Finland, 2016; ISBN 978-952-324-060-5.
61. Branders, M. *Kokonainen Turvallisuus? Kokonaisturvallisuuden Poliittinen Kelpoisuus ja Hallinnollinen Toteutettavuus. Doctoral Dissertation*; Tampere University Press: Tampere, Finland, 2016; ISBN 978-951-44-9996-8.
62. Yin, R.K. *Qualitative Research from Start to Finish*; Guilford Press: New York, NY, USA, 2011; ISBN 978-1-60623-701-4.
63. Graham, S.; Marvin, S. *Splintering Urbanism: Networked Infrastructures, Technological Mobilities and the Urban Condition*; Routledge: London, UK, 2001; ISBN 0-203-45220-8.
64. Pursiainen, C. Critical infrastructure resilience: A Nordic model in the making? *Int. J. Disaster Risk Reduct.* **2018**, *27*, 632–641. [CrossRef]
65. Baber, C.; McMaster, R. *Grasping the Moment. Sensemaking in Response to Routine Incidents and Major Emergencies*; CRC Press: Boca Raton, FL, USA, 2016; ISBN 978-1-4724-7080-5.
66. Boin, A.; Smith, D. Terrorism and Critical Infrastructures: Implications for Public–Private Crisis Management. *Public Money Manag.* **2006**, *26*, 295–304. [CrossRef]
67. Lewis, T.G. *Infrastructure Protection in Homeland Security. Defending a Networked Nation*; John Wiley & Sons: Hoboken, NJ, USA, 2006; ISBN 978-0-471-78954-3.
68. Brenner, J.F. Eyes wide shut: The growing threat of cyber attacks on industrial control systems. *Bull. At. Sci.* **2013**, *69*, 15–20. [CrossRef]
69. Clarke, R.A.; Knake, R.K. *Cyber War: The Next Threat to National Security and What to Do About It*; Harper Collins: New York, NY, USA, 2010; ISBN 978-0-0619-6224-0.
70. Dengg, A.; Schurian, M.N. On the Concept of Hybrid Threats. In *Networked Insecurity—Hybrid Threats in the 21st Century*; Schriftenreihe der Landesverteidigungsakademie: Vienna, Austria, 2016; pp. 25–80. ISBN 978-3-903121-01-0.
71. Steele, W.E.; Hussey, K.; Dovers, S. What´s Critical about Critical Infrastructure? *Urban Policy Res.* **2017**, *35*, 74–86. [CrossRef]
72. Braithwaite, A. The Logic of Public Fear in Terrorism and Counter-terrorism. *J. Police Crim. Psychol.* **2013**, *28*, 95–101. [CrossRef]
73. Neumann, P.R.; Smith, M.L.R. *The Strategy of Terrorism. How it Works, and Why it Fails*; Routledge: London, UK, 2008; ISBN 978-0-203-93700-6.
74. Friedland, N.; Merari, A. The psychological impact of terrorism: A double-edged sword. *Polit. Psychol.* **1985**, *6*, 591–604. [CrossRef]

75. Zoli, C.; Steinberg, L.J.; Grabowski, M.; Hermann, M. Terrorist critical infrastructures, organizational capacity and security risk. *Saf. Sci.* **2018**, *110*, 121–130. [CrossRef]
76. Barker, J. *The No-Nonsense Guide to Terrorism*; New Internationalist Publications: London, UK, 2003; ISBN 1-85984-433-2.
77. Cinturati, F. The Bioterrorism Act and Water Utilities Protection: How to Proceed from Policy to Practice. *J. Appl. Secur. Res.* **2014**, *9*, 97–108. [CrossRef]
78. Ranstorp, M.; Normark, M. Detecting CBRN terrorism signatures—Challenges and new approaches. In *Unconventional Weapons and International Terrorism. Challenges and New Approaches*; Ranstorp, M., Normark, M., Eds.; Routledge: New York, NY, USA, 2009; pp. 1–10. ISBN 978-0-203-88195-8.
79. Meinhardt, P.L. Water and Bioterrorism: Preparing for the Potential Threat to U.S. Water Supplies and Public Health. *Annu. Rev. Public Health* **2005**, *26*, 213–237. [CrossRef] [PubMed]
80. Ginsberg, M.D.; Hock, V.F. Terrorism and security of water distribution systems: A primer. *Def. Secur. Anal.* **2004**, *20*, 373–380. [CrossRef]
81. Glass, T.A.; Schoch-Spana, M. Bioterrorism and the People: How to Vaccinate a City against Panic. *Clin. Infect. Dis.* **2002**, *34*, 217–223. [CrossRef] [PubMed]
82. Boin, A.; Lagadec, P.; Michel-Kerjan, E.; Overdijk, W. Critical Infrastructures under Threat: Learning from the Anthrax Scare. *J. Conting. Crisis Manag.* **2003**, *11*, 99–104. [CrossRef]
83. Schmid, A.P. Introduction. In *The Routledge Handbook of Terrorism Research*; Schmid, A.P., Ed.; Routledge: New York, NY, USA, 2011; pp. 1–38. ISBN 0-203-82873-9.
84. Jordán, F. Predicting target selection by terrorists: A network analysis of the 2005 London underground attacks. *Int. J. Crit. Infrastruct. Prot.* **2008**, *4*, 206–214. [CrossRef]
85. Richardson, L. *What Terrorists Want. Understanding the Enemy, Containing the Threat*; Random House: New York, NY, USA, 2007; ISBN 978-0-8129-7544-4.
86. Horgan, J. *The Psychology of Terrorism*; Routledge: New York, NY, USA, 2005; ISBN 0-203-49696-5.
87. Gunaratna, R. Global Threat Forecast. *Count. Terror. Trends Anal.* **2017**, *9*, 3–11.
88. Hesterman, J. *Soft Target Hardening. Protecting People from Attack*; CRC Press: Boca Raton, FL, USA, 2015; ISBN 978-1-4822-4422-9.
89. Graham, B.; Talent, J.; Allison, G.; Cleveland, R.; Rademaker, S.; Roemer, T.; Sherman, W.; Sokolski, H.; Verma, R. *World at Risk. The Report of the Commission on the Prevention of WMD Proliferation and Terrorism*; Vintage Books: New York, NY, USA, 2008; ISBN 978-0-307-47326-4.
90. Gurr, N.; Cole, B. *The New Face of Terrorism. Threats from Weapons of Mass Destruction*; I.B. Tauris Publishers: London, UK, 2002; ISBN 1-86064-825-8.
91. Maiolo, M.; Pantusa, D. Infrastructure Vulnerability Index of drinking water systems to terrorist attacks. *Cogent Eng.* **2018**, *5*, 1–21. [CrossRef]
92. Monroe, J.; Ramsey, E.; Berglund, E. Allocating countermeasures to defend water distribution systems against terrorist attack. *Reliab. Eng. Syst. Saf.* **2018**, *179*, 37–51. [CrossRef]
93. Achour, N.; Pantzartzis, E.; Pascale, F.; Price, A.D.F. Integration of resilience and sustainability: From theory to application. *Int. J. Disaster Resil. Built. Environ.* **2015**, *6*, 347–362. [CrossRef]
94. Romero-Lankao, P.; Gnatz, D.M.; Wilhelmi, O.; Hayden, M. Urban Sustainability and Resilience: From Theory to Practice. *Sustainability* **2016**, *8*, 1224. [CrossRef]
95. Thurlby, R.; Warren, K. Understanding and managing the threat of disruptive events to the critical national infrastructure. *J. Facil. Manag.* **2014**, *12*, 231–246. [CrossRef]
96. Simon, J.D. *Lone Wolf Terrorism. Understanding the Growing Threat*; Prometheus Books: New York, NY, USA, 2016; ISBN 9781633882379.