SECURITY & DEFENCE QUARTERLY
https://securityanddefence.pl/

Preparing critical infrastructure for the future: Lessons learnt from the Covid-19 pandemic

Amelia Tomalska

aj.tomalska@uw.edu.pl

https://orcid.org/0000-0002-3717-0703

Department of Internal Security, University of Warsaw, Krakowskie Przedmieście 26/28, 00-927 Warsaw, Poland

Abstract

The objective of this paper is to provide a view on the problem of insufficient state protection of critical infrastructure throughout the Covid-19 crisis. The paper looks at this problem with regard to the definition of critical infrastructure, its content, and also the limitations of current approaches to critical infrastructure protection. The examples relating to the Covid-19 crisis show the practices adopted and suggest possible steps forward. The research methodology implemented in this research is based on a critical analysis of the existing literature. The themes described in this paper show there is an urgent need to change current critical infrastructure protection approaches to a resilience-based modus operandi. Specifically, this paper highlights the need to shift the understanding of critical infrastructure from an object-oriented approach towards essential services/functions and to highlight its complex, socio- technical nature. It also highlights the deficiencies of current, prevention-based approaches to critical infrastructure protection such as the insufficient focus on identification and management process of vulnerabilities, especially in relation to (inter)dependencies resulting from interconnections with other systems. The gravity of the situation caused by the Covid-19 pandemic, despite its negative connotations, can be used as an opportunity to examine the real condition of protection of critical infrastructure. The pandemic suggests that there is much left to be done and because of the unpredictability of the future, we need to start acting as soon as possible.

Keywords:

protection, resilience, critical infrastructure, Covid-19 pandemic

Article info
Received: 30 October 2021
Revised: 5 February 2022
Accepted: 10 February 2022
Available online: 30 March 2022
Citation: Tomalska, A. (2022) 'Preparing critical infrastructure for the future: Lessons learnt from the Covid-19 pandemic', Security and Defence Quarterly, 39(3), pp. 21–32.
doi: 10.35467/sdq/146603.

Introduction

The primary function of critical infrastructure is to provide essential services to society, such as water, transportation, energy, health services, ICT, and financial services. It is considered to be of great importance to the security of the country and the well-being of its citizens (The Organisation for Economic Co-operation and Development, 2019). In moments of uncertainty and crisis, spawned by (un)anticipated threats, the continuity of the essential services becomes even more crucial. So called "black swan" events, which are difficult to predict, and come with severe consequences, are likely to be more common in the future, especially as we are facing a growing climate crisis (Goering, 2021). We can also say that the Covid-19 pandemic is one of these "black swans" and has exposed major deficiencies in terms of protection of critical infrastructure. It has also caused many to realise the pressing need to change the approach from preventive based to resilience based and to establish effective cooperation and partnerships among various stakeholders. The crisis caused by Covid-19 presents an opportunity to look into the current status of security of critical infrastructure and to consider potential future challenges and to apply proper countermeasures in advance.

This paper aims to present many literature-based lessons learnt from the pandemic, which might in the future contribute to better, more effective protection of critical infrastructure. These involve issues such as how critical infrastructure is defined, the current approach regarding the protection of critical infrastructure with its deficiencies and possible alternative approaches that provide greater resilience. The novelty of this kind of threat requires critical infrastructure owners and operators to rethink their current approach, and to upgrade the level of preparedness and capabilities to react to future unexpected crises.

Defining critical infrastructure

To be able to protect critical infrastructure, the correct identification process needs to be conducted. Broadly speaking, critical infrastructure is a term which involves the collection of various elements that are vital to the functioning of the country and society. Many of the European Union countries before implementation of the European Union Directive on Critical Infrastructure Protection, did not have any specific measures or laws regarding identification and protection of critical infrastructure. The Directive introduced a definition of European critical infrastructure as follows: "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" (European Union, 2008). Lower case member states implemented this same or very similar definition of the critical infrastructure to their national regulations, when others decided to stick with their own, national definitions. This led to some differences in understanding the notion of critical infrastructure in European Union countries. Several of them included both assets and systems in this term, which aim to support vital societal functions, whereas other countries only focused on the critical assets (European Commission, 2019).

The understanding of critical infrastructure in terms of assets means that the protection is only limited to facilities or objects, without taking into consideration their dependencies or interdependencies. Moreover, because of such understating of critical infrastructure, crisis planning and preparing processes did not include such complexities as indirect consequences (Carvalhaes *et al.*, 2020). Countries such as Norway or Sweden define critical infrastructure as essential services, critical/vital functions. This understanding

embraces critical infrastructure as an increasingly interconnected process, systems which involve different stakeholders and also allows us to identify and prioritise essential services based on the critical consequences of infrastructure failure in the actual situation (Pursiainen, 2017). This flexibility makes a better response to society's needs possible in times of crisis.

The Covid-19 pandemic has led to a revaluation of these needs. The vulnerability of the medical oxygen supply chain as a critical service became evident at the onset of the pandemic. This chain involved many sequences of events and actions required for the production, distribution, the transportation of medical oxygen. This example, as well as a different one with personal protective equipment (PPE) that was essential for the medical staff, showed that the meaning of what is essential can drastically change over a short period of time as seen in the comment "seemingly in the course of weeks, our demands for many basic and critical services have radically shifted" (Carvalhaes *et al.*, 2020). This shift in defining critical infrastructure is a starting point to introduce and implement a resilient approach for the protection of critical infrastructure. In this way, not only the specific object or asset would be protected, but rather the final product and the outcome of what an essential service is supposed to deliver. Another important aspect regarding the definition of critical infrastructure is the content of the term.

Describing critical infrastructure as a system, often understood as a complex network of hard components such as IT hardware, devices or technology, the soft component, the human component, seems to be missing or not properly emphasised. Throughout the pandemic, the role of essential workers who interact directly with the system, and who operate or facilitate assets, facilities, systems, or networks, in addition to those responsible for decision making processes and crisis management, turned out to be indispensable. Due to travel restrictions, the flow of essential staff was halted. A shortage of personnel has been a primary issue for critical infrastructure operators during the pandemic (Galbusera *et al.*, 2021). The situation is even more serious if we realise that in the case of critical infrastructure, most of the positions cannot be filled by random personnel since they require special knowledge, skills and sometimes a security clearance. These obstacles spawned from crisis create a lengthy process, which endangers the undisturbed continuity of essential services.

Therefore, some institutions like the US Cybersecurity & Infrastructure Security Agency (CISA) introduced guidance on the essential critical infrastructure workforce. The first versions of this guidance were mostly focused on the identification of essential work functions, while the last two versions included a catalogue of identified essential workers "who conduct a range of operations and services that may be essential to continued critical infrastructure operations, including staffing operations centres, maintaining and repairing critical infrastructure, operating public safety call centres, working construction, and performing operational functions, among others" (Cybersecurity & Infrastructure Security Agency, 2021). It includes workers who support crucial supply chains and enable cyber and physical security functions for critical infrastructure. The industries supported by essential workers are "medical and healthcare, telecommunications, information technology systems, defence, food and agriculture, transportation and logistics, energy, water and wastewater, and law enforcement" (Cybersecurity & Infrastructure Security Agency, 2021). This emphasises the major role played by critical infrastructure workers in the process of securing the continuity of the operating of critical infrastructure and overall response to the pandemic. This shows that besides purely technical elements, critical infrastructure should be understood as a system or a process of multiple actions taken by people, who contribute to the system's objective, which is the delivery of the essential services to the society under all circumstances.

It should be noted that the latest initiative undertaken by European Union also supports this statement. The recently proposed European Union Directive on the resilience of critical entities defines critical infrastructure as a critical entity which provides essential services. According to the Directive, the delivery of essential services depends on infrastructure, understood as an asset, system or part thereof. The newly proposed change in defining critical infrastructure clearly indicates the much broader and complex understanding of critical infrastructure, which would be identified through the prism of the services it provides. Nevertheless, the directive still needs further clarification, since it remains vague and lacks clear description of what the term "entities equivalent to critical entities" implies (European Commission, 2020a). The proposed changes regarding the definition of critical infrastructure are in line with the revised NIS Directive - NIS 2 Directive, which relates to entities providing critical services in the digital infrastructure domain (European Economic and Social Committee, 2021).

Limitations of the current approach

Critical infrastructure is exposed to a vast array of threats, including natural hazards, intentional and unintentional attacks. For a long time, a particular focus has been placed on physical protection, asset hardening (Zio, 2016). The increased reliance on technology, and the high level of dependencies and interdependencies among various critical infrastructures has resulted in crisis, which is becoming more and more complex, interconnected and transboundary (Boin and Lagadec, 2000).

Moreover, due to high connectivity, critical infrastructure is becoming more vulnerable to cascading disruptions across sectoral boundaries (Pescaroli and Alexander, 2016). The term cascading impacts is related to highly interconnected systems, in which a failure or disruption in one of the systems leads to malfunctions in other systems (Federal Emergency Management Agency, 2020). As in the case of recent events, according to the Chartered Institute of Procurement and Supply, 86% of supply chains have been impacted by the COVID-19 pandemic (Remko, 2020). Three types of risks have been reported by the supply chain executives in their study which included: supply risks such as shipping delays in long pipelines, gaps in preparedness and contingency plans and logistical bottlenecks; demand risks, depending on the demand, and fast reductions or spikes in demand of the products. This also includes control risks, with a tendency to focus on seeking priority and collaboration and also passing some of the financial pressure to suppliers (Remko, 2020). During the Covid-19 pandemic, critical infrastructure has not been exempt from its consequences.

The escalation of the crisis on a global scale forced critical infrastructure into untested waters (Galbusera *et al.,* 2021). The system that has arguably been the most heavily affected with high patient pressure is the health system. The dependence of the healthcare system on other systems, such as transport, has created shortages of many goods and equipment such as ventilators and PPE which were intended for frontline health care workers. Before the outbreak of the Covid-19 pandemic, China was responsible for the production of approximately half the world's medical face masks (Ranney *et al.*, 2020). Due to the pandemic, the production and distribution of these were halted in China sparking shortages that reverberated throughout the world (Ranney *et al.*, 2020). This shows that a strong dependence on global suppliers in times of uncertainty, and possible obstacles in production or transportation of goods, can create a potential, critical situation. This requires critical infrastructure operators to be more flexible, to be able to adjust to the current situation and to look in advance for different suppliers or back-up systems.

Because of strong interdependence between healthcare and other sectors, the responsibility to prevent disruptions in any sectors demands joint actions, information sharing and also coordination by national authorities and agencies. The importance of cooperation between private stakeholders (producers of essential supplies) and public institutions responsible for national logistics of delivery of the goods plays a major role in the functioning of critical infrastructure. Since the pandemic began, some useful initiatives have been proposed and implemented, such as resource sharing by international technical companies that provided some of the communication tools to medical staff and creation of open-access platforms that have been established in critical infrastructure networks and are designed to provide exchange of good practices of risk management and mitigation measures related to the Covid-19 crisis (Galbusera *et al.*, 2021). Nevertheless, the effective participation of government in coordinating the delivery of critical services in times of crisis still needs more attention.

The occurrence of health emergencies, crises, and disasters fosters the appearance of hybrid threats (Europol, 2020). According to a recent Interpol report, an increased number of cyber-attacks against governments, critical infrastructure and the healthcare sector have taken place (Interpol, 2020). Moreover, many EU Member States have noted a rise in disinformation campaigns and media interference aimed to undermine public trust in national institutions and the credibility of governments (Europol, 2020). The surge of disinformation, misinformation and rumours (the so called "infodemics") has endangered the effectiveness of public response to the crisis and recovery efforts. As a response, the World Health Organisation (WHO) established the WHO Network for Information in Epidemics (EPI-WIN), which aims to provide evidence-based information on the public health situation that is verified by trusted sources (World Health Organization, 2020).

This demonstrates the importance of establishing good communication channels between government, society and media, with clear responsibilities and good cooperation, which is crucial for the overall security of the critical infrastructure.

The Covid-19 pandemic has led many to realise that natural hazards are still present and might be even more difficult to predict in future (Clark-Ginsberg *et al.*, 2020). The pandemic has offered a new type of threat namely one of a constant, permanent character. This kind of threat could be a new normal which we have to adjust to. The outbreak of Covid-19 found many of the critical infrastructure operators in a state of surprise and sometimes panic. In many cases, the lack of business continuity planning that encompasses the means to identify risks, set the objectives and established adequate practices in mitigating and managing risk, endangered the continuity of the service (Schmid *et al.*, 2021).

The pandemic is an example of what might occur in the future. It represents a new type of threat to which critical infrastructure operators will have to adapt and react to more easily and quickly. Many crises, especially cascading ones, cannot be fully prevented in high complexity systems. Therefore, the focus should be placed on preparedness to act and better understanding of the system, including identification, analysis of the vulnerabilities and implementation of countermeasures before the events occur (Pescaroli and Alexander, 2016). It requires a shift in the current approach regarding protection of critical infrastructure from preventive into resilient. In a current approach based on a crisis management cycle, the prevention, planning, response, recovery and learning phases can be distinguished. As previously mentioned, we should bear in mind that there are and always will be some barriers, whether political, cognitive, informational, cultural or resource related, to being able to prevent every possible threat to critical infrastructure (Boin and

Lagadec, 2000). Therefore, the methodology based on prevention that aims to keep all the bad thing(s) from happening cannot be effective during "black swan" events or emerging threats (Longstaff, 2005). Contingency planning is important, but should not be overestimated. Developing plans for a vast array of scenarios may not only be impossible but also time-consuming and very expensive (Boin and Lagadec, 2000). Therefore, there is an urgent need to implement a new approach focused on identification and management of vulnerabilities and effective organisational capabilities.

Post Covid-19 approach based on resilience

Resilience is a broad and complex term, for which exists many different definitions. Some of them focus only on actions after the adverse event, when others include also the actions before the adverse event, such as anticipation, planning, preparedness (Carlson *et al.*, 2012). For example, resilience can be defined as: "the capacity of a system to absorb disturbance, undergo change, and retain essentially the same function, structure, identity, and feedbacks" (Longstaff *et al.*, 2010). The emphasis in this definition is put on capacity of the critical infrastructure to overcome a crisis after the incident. This means that the approach is not focused on building barriers or any fortification strategies that would prevent the occurrence of threat at all costs, but rather on the abilities of the critical infrastructure to deal with the adverse event. It includes the capability to reduce, absorb the impact of the event, to reduce the time of recovery, and also to adapt, evolve through the development of specific processes (Curt and Tacnet, 2018).

When above mentioned definition compared to the Presidential Policy Directive from 2013, which defines resilience as "the ability of an infrastructure to prepare to cope with changing conditions and adapt to them, and to resist and recover rapidly from disruption, including deliberate attacks, accidents or natural events," the preparation element – the pre-crisis component – is also present (Presidential Policy Directive, 2013). The differences in defining resilience are also apparent in the proposal of the new European Directive on resilience of critical entities. In this new directive, the notion of resilience refers to "the ability to prevent, resist, mitigate, absorb, accommodate to and recover from an incident that disrupts or has the potential to disrupt the operations of a critical entity" (European Commission, 2020a). The major difference in this definition to the one in the Presidential Policy Directive is the prevention component. The inclusion of measures aimed at preventing incidents from happening, rather than preparing critical infrastructure to withstand identified or unidentified threats, seems to be contradictory to the intended outcomes, namely disaster risk reduction and climate change adaptation. Nevertheless, the shift in protection of critical infrastructure to resilience-based approach has not been yet fully incorporated into the European Union and national frameworks (European Commission, 2020b).

In this paper, resilience of critical infrastructure is understood as an umbrella term that includes the ability of an entity to anticipate, resist, absorb, respond to, adapt to, and recover from any kind of disturbance (Carlson *et al.*, 2012).

To begin with, a set of characteristics that defines resilience has been developed in the literature and includes the following properties:

- robustness understood as an ability of the systems or elements to perform despite the challenges. It can be assumed that critical infrastructure is robust when it is able to withstand any kind of disturbance and does not suffer degradation or loss of function;

- redundancy, refers to the substitutability of the elements or systems. It emphasises the role of backup capabilities and systems that in the event of disruption, degradation or loss of functionality of the main system can take over;

- resourcefulness, includes the actions aiming to cope with a dynamic environment, especially by having proper resources to manage a future potential crisis. This involves actions such as problem identification, setting up the priorities and resources mobilisation process to mitigate the damage;

- rapidity, relates to the ability to restore the functionality of the system in a short period of time, after the adverse event, to avoid further losses (Bruneau, *et al.*, 2003; Longstaff, 2005).

Bearing in mind the above mentioned definitions and characteristics of a resilient system, some actions can be proposed for improving the protection of critical infrastructure where future "black swans" and unknown unknowns are concerned.

With regard to unpredictable future threats, the identification and assessment of vulnerabilities play a crucial role in the process of building a resilient entity. Vulnerability is a multidimensional term that can be defined as a "physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard" (Department of Homeland Security, 2010) or as a "concept that describes the degree to which a system is susceptible to a specified degree of loss resulting from a specified initiating threat event" (McGill and Ayyub, 2007). Even though vulnerability is a major component of risk, (risk understood as a sum of threat, vulnerability and consequences), there are methodologies where the vulnerability element is missing or is equated to probability of adversary success. This marginalisation of vulnerability might be the result of a lack of explicit definition and agreed understanding of what vulnerability aims to measure (McGill and Ayyub, 2007; Petit *et al.*, 2013). To grasp the meaning of this term and how it affects the security of critical infrastructure, two kinds of vulnerabilities can be distinguished: protection vulnerabilities and response vulnerabilities.

The first kind of vulnerability, the protection vulnerability, determines the probability and scale of consequences and damages in respect of a threat event. In the case of consequences that cannot be prevented following an adverse event, critical infrastructure is vulnerable, unless is able to control the following losses with appropriate strategies. This notion includes capabilities to successfully detect the possible threats (McGill and Ayyub, 2007). However, the spectrum of threats should not be narrowed down to only the most common, anthropological and external threats that are difficult to prevent and foresee, such as natural disaster(s), insider threats and terrorist attacks. It should rather include the currently present threats resulting from dependencies and interdependencies within critical infrastructure and among other systems. The dependence on remote sources, overreliance on single or few factories for supplies can create a major threat to critical infrastructure. Instead, operators of critical infrastructure should ensure alternative and flexible sources and include local or nearby sourcing. The operators should prepare the backup sources and inventory buffers in advance and establish an efficient information sharing mode between all the stakeholders involved in the supply chain (Remko, 2020). To map the dependencies and interdependencies, the entity must have the capabilities to observe and correctly interpret the environment in which critical infrastructure operates. To spot the early warning signs of potential threats, an entity needs to be aware of and understand the connections between systems.

The second kind of vulnerability, the response vulnerability, influences the degree of loss and the probability of the damage after an adverse event occurs. It relates mostly to

internal procedures, plans and to capabilities of the system to respond and recover. The level of vulnerability determines critical infrastructure's capability to resist, absorb and to adapt to the current situation (Petit *et al.*, 2013; Remko, 2020). It is essential that the vulnerability mitigation and reduction strategies are determined by the state of organisational resilience of the critical infrastructure. The strengths and deficiencies of organisational structure would directly influence the system's capacity to respond to a crisis situation and to recover (Pescaroli and Alexander, 2016). The ability of critical infrastructure to prioritise and allocate adequate resources is very important in times of crisis, so as to ensure the undisturbed continuity of essential services. The phase of reaction, the way critical infrastructure responds to a crisis, plays a major role in the overall process of building resilience.

In literature, three post-crisis turnaround stages have been distinguished: the defensive phase, consolidation phase and offensive phase. The first phase – the defensive phase – occurs immediately after the crisis event and is characterised by intense threat and surprise. The effective turnaround in this phase should include contingency planning, communications and systems' coupling and complexity. During this stage, the entity is forced to operate under much pressure and uncertainty because of the limited availability of the information. The coupling and complexity of the system have been included not only because they are the factors that usually create crisis situations, but also because it is crucial for the organisation to know the root cause of the crisis and to eradicate it as soon as possible. In the early stage of the crisis, some of the constraints regarding communication, not only internal but also external, are present. However, the entity needs to provide any required information to the public, media and also to all of the parties that could be affected. The establishment of effective communication channels can prevent the generation of disinformation and fake-news that might hamper the response actions to the crisis and cause irreversible damage. The control of speculation, by information and image management, can help overcome a crisis and to gain trust among stakeholders.

During the second phase, the consolidation phase, the organisation focuses on long-term strategies including restructuring and organisational recovery. In this stage, the entity needs to make an effort to restore confidence among various stakeholders. The third phase, the offensive phase, relates to changes made to the organisation's configuration and culture. The organisation has to ensure stakeholders of its actions aimed at preventing a future crisis and improvements to internal communication (Smith and Sipika, 1993). Moreover, the entity should develop a security culture that promotes resilience within its organisation and externally, involving the entities that might be affected directly or indirectly by any disturbances and the ones contributing to restoring functionality of the critical infrastructure. It should be emphasised that the resilience is a dynamic, ongoing process that requires constant improvement, especially after each crisis. Therefore, the exercises, trainings, simulations and constant attention to real-life incidents are essential in terms of building resilience.

A good example of a resilient approach towards unexpected threats is Israel. During the first wave of the pandemic (March–May 2020), Israel's government decided to engage its intelligence services in crisis management activities to more effectively handle the situation. Even though the country struggled at the beginning of the pandemic because of lack of sufficient information on the virus, its possible impacts and shortages of health equipment and critical components, it was still able, in a relatively short period of time, to obtain the necessary resources. The actions undertaken rapidly by Israel's intelligence services, such as acquisition of medical equipment, technological information and manufacturing designs of medical equipment, enabled Israeli's local factories to start producing needed equipment and stop relying on external providers. The clear allocation of responsibilities

between different intelligent agencies contributed to prompt decision making, its implementation and constant evaluation. Moreover, the close relationship between government and intelligence services helped support the government in its evidence-based decision-making process by providing continuous analysis of the situation and predicting the possible outcomes and information on hotspots and places of large-scale contamination. As a result of these actions, the healthcare system was not overwhelmed and the number of deaths was relatively low (Shpiro, 2021).

The Covid-19 pandemic has shown that the role and engagement of government in coordination efforts to make sure that essential resources are distributed on the basis of demand and that areas hit the most receive necessary equipment, is crucial (Ranney *et al.*, 2020). An effective coordination process from the national level is necessary to ensure faster and more adequate distribution of essential resources. However, the framework of cooperation between different stakeholders remains a challenge. The reasons are the divergent interests of each group of stakeholders, especially between business-motivated interests of operators of critical infrastructure and state administration responsibility for public safety. Nevertheless, the state should try to establish a clear communication process that would include roles, responsibilities and obligations regarding crisis situations. The stakeholders should settle what type of information should be exchanged and by which means (e.g. by using secure information sharing platforms) (Bach *et al.*, 2013). In addition, joint exercises to build and to test the effectiveness of coordination, communications, information-sharing and to raise awareness of dependencies and interdependencies among them, would enable private and public entities to understand the complexity of the system and to prepare adequate plans, strategies and programmes of critical infrastructure protection, including post-crisis activities (Fisher and Gamper, 2017).

Society should also be engaged in the process of building critical infrastructure resilience. Even though government cannot make all of the people resilient, by providing information about potential risks and by giving support society might turn out to be very helpful during crisis situations. It can provide essential information about certain events to first responders that would ensure the gravity of the situation is recognised more quickly and to identify what type of equipment is needed (Bach *et al.*, 2013). Moreover, during health crisis situations, the prevention and mitigation of disinformation require the active participation of civil society in terms of preparedness and response. The spread of unreliable information can weaken society's capacity to respond to a crisis and hamper an effective public health response. Only the collaborative effort of all sectors (government, business, society) makes it possible to sustain the continuity of essential services and reduce threats to the functioning of society (Gradoń *et al.*, 2021). All of these actions would help in more rapid restoration of critical infrastructure after a crisis and would reduce the risk of disruption to the continuity of essential services.

Conclusions

The gravity of the situation caused by the Covid-19 pandemic, despite its negative connotations, can be used as an opportunity to examine the real condition of protection of critical infrastructure. The pandemic has shown that there is much left to be done and in unpredictable times, we need to start acting as soon as possible. First of all, it is crucial to understand critical infrastructure in terms of essential services/functions rather than mere physical objects or assets. This would make it possible for critical infrastructure to be seen as a system of systems, which because of its cross- sectoral nature and its dependencies and interdependencies, cannot be limited to only one sector (Dunn-Cavelty and Suter, 2009). Moreover, the human aspect in terms of critical infrastructure should become more

evident. Furthermore, the current approach to protection of critical infrastructure needs to be upgraded. In light of recent, unexpected events, the current focus on preventive actions needs to be changed. It should be replaced by an approach based on resilience, which would identify and reduce the vulnerabilities and, therefore, minimise the effects of potential threats. This approach would also allow the importance of the capabilities of the entities carrying out response and recovery actions to be stressed. This would also help with smoother adaptation to a new situation and after- crisis environment (Rehak et al., 2018). Moreover, critical infrastructure operators should focus on the identification of vulnerabilities within the organisation and among systems and apply adequate countermeasures. The protection of critical infrastructure depends on different entities. It involves the state, critical infrastructure operators as well as society and the media. Therefore, the establishment of a framework of horizontal and vertical cooperation and communication among stakeholders would contribute greatly to the process of building more secure, resilient critical infrastructure.

Funding

This research received no external funding.

Data Availability Statement

Not applicable.

The author has read and agreed to the published version of the manuscript.

Disclosure statement

No potential conflict of interest was reported by the author.

References

Bach, C., Bouchon, S., Fekete, A., Birkmann, J. and Serre, D. (2013) 'Adding value to critical infrastructure research and disaster risk management', *The Resilience Concept, S.A.P.I.EN.S*, 6(1), pp. 1–12.

Boin, A. and Lagadec, P. (2000) 'Preparing for the future: Critical challenges in crisis management', *Journal of Contingencies and Crisis Management*, 8, pp. 185–191. doi: 10.1111/1468-5973.00138.

Bruneau, M., Chang, S., Eguchi, R., Lee, G., O'Rourke, T., Reinhorn, A., Shinozuka, M., Tierney, K., Wallace, W. and Von Winterfeldt, D. (2003) 'A framework to quantitatively assess and enhance seismic resilience of communities', *Earthquake Spectra*, (19)4, pp. 733–752. doi: 10.1193/1.1623497.

Carlson, L., Bassett, G., Buehring, W., Collins, M., Folga, S., Haffenden, B., Petit, F., Phillips, J., Verner, D. and Whitfield, R. (2012) *Resilience Theory and Applications*, Argonne National Laboratory, Decision and Information Sciences Division, ANL/DIS-12-1, Argonne, IL. doi: 10.2172/1044521.

Carvalhaes, T., Markolf, S., Helmrich, A., Kim, Y., Li, R., Natarajan, M., Bondank, E., Ahmad, N. and Chester, M. (2020) 'COVID-19 as a Harbinger of Transforming Infrastructure Resilience', *Frontiers in Built Environment*, 6, pp. 1–8, doi: 10.3389/fbuil.2020.00148.

Clark-Ginsberg, A., Rueda, I.A., Monken, J., Liu, J. and Chen, H. (2020) 'Maintaining critical infrastructure resilience to natural hazards during the COVID-19 pandemic: Hurricane preparations by US energy companies', *Journal of Infrastructure Preservation and Resilience*, 1(1), doi: 10.1186/s43065-020-00010-1.

Curt, C. and Tacnet, J. (2018) 'Resilience of critical infrastructures: Review and analysis of current approaches', *Risk analysis*, 38(11), pp. 2441–2458, Wiley. doi: 10.1111/risa.13166.

Cybersecurity & Infrastructure Security Agency (2021) *Guidance on the essential critical infrastructure workforce: Ensuring community and national resilience in COVID-19 response version 4.1*, Office of the Director, Washington, DC.

Department of Homeland Security (2010) *DHS Risk Lexicon – 2010 edition*, Washington, DC. Available at: http://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf (Accessed: 6 October 2021).

Dunn-Cavelty, M. and Suter, M. (2009) 'Public-private partnerships are no silver bullet: An expanded governance model for critical infrastructure protection', *International Journal of Critical Infrastructure Protection,* 2, pp. 179–187. doi: 10.1016/j.ijcip.2009.08.006.

European Commission (2019) *Commission staff working document, evaluation study of Council Directive 2008/114 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection*, Brussels: European Commission.

European Commission (2020a) *Proposal for a directive of the European Parliament and the Council on the resilience of critical entities*, Brussels: European Commission.

European Commission (2020b) *Commission staff working document. Impact assessment. Accompanying the document proposal for a Directive of the European Parliament and of the Council on the resilience of critical entities*, Brussels: European Commission.

European Economic and Social Committee (2021) *Opinion, European Economic and Social Committee, Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 and Proposal for a Directive of the European Parliament and of the Council on the resilience of critical entities*, Brussels: Council of the European Union.

European Union (2008) *Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection*, Brussels: Official Journal of the European Union.

Europol (2020) *Catching the virus cybercrime, disinformation and the COVID-19 pandemic. Report of the European Union Agency for Law Enforcement Cooperation*, Hague: Europol.

Federal Emergency Management Agency (2020) *2020 National preparedness report*, Washington, DC: Department of Homeland Security.

Fisher, M.K. and Gamper, C. (2017) *Policy evaluation framework on the governance of critical infrastructure resilience in Latin America*, Washington DC: Inter-American Development Bank, doi: 10.18235/0000819.

Galbusera, L., Cardarilli, M. and Giannopoulos, G. (2021) 'The ERNCIP Survey on COVID-19: Emergency & business continuity for fostering resilience in critical infrastructures,' *Safety Science*, 105161, 139, doi: 10.1016/j.ssci.2021.105161.

Goering, L. (2021) 'As climate impacts surge, UN science report to examine "black swan" events', Thomson Reuters Foundation, 20 July. Available at: https://news.trust.org/item/20210720155814-cldk3/ (Accessed: 4 October 2021).

Gradoń, K., Hołyst, J., Moy, W., Sienkiewicz, J. and Suchecki, K. (2021) 'Countering misinformation: A multidisciplinary approach', *Big Data & Society*, 8, pp. 1–14, doi: 10.1177/20539517211013848.

Interpol (2020) *Cybercrime: COVID-19 impact*. Report of the Interpol, Lyon: Interpol.

Longstaff, P. (2005) *Security, resilience, and communication in unpredictable environments such as terrorism, natural disasters, and complex technology*, Center for Information Policy Research, Cambridge, Massachusetts: Harvard University.

Longstaff, P., Armstrong, N., Perrin, K., Parker, W.M. and Hidek, M. (2010) 'Building resilient communities: A preliminary framework for assessment', *Homeland Security Affairs*, 6(3), pp. 1–23, Monterey: Naval Postgraduate School.

McGill, W. and Ayyub, B. (2007) 'The meaning of vulnerability in the context of critical infrastructure protection', in *Critical infrastructure protection: Elements of risk*, Fairfax: George Mason University, pp. 25–48.

Pescaroli, G. and Alexander, D. (2016) 'Critical infrastructure, panarchies and the vulnerability paths of cascading disasters', *Natural Hazards*, 82, pp. 1–18, doi: 10.1007/s11069-016-2186-3.

Petit, F.D.P., Bassett, G.W., Black, R., Buehring, W.A., Collins, M.J., Dickinson, D.C., Fisher, R.E., Haffenden, R.A., Huttenga, A.A., Klett, M.S., Phillips, J.A., Thomas, M., Veselka, S.N., Wallace, K.E., Whitfield, R.G. and Peerenboom, J.P. (2013) *Resilience measurement index: An indicator of critical infrastructure resilience*, Office of Scientific and Technical Information (OSTI), Argonne National Laboratory.

Presidential Policy Directive – PPD21 (2013) *Critical infrastructure security and resilience*. Available at: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil (Accessed: 9 October 2021).

Pursiainen, C. (2017) 'Critical infrastructure resilience: A Nordic model in the making?', *International Journal of Disaster Risk Reduction*, 27, pp. 632–641, doi: 10.1016/j.ijdrr.2017.08.006.

Ranney, M.L., Griffeth, V. and Jha, A.K. (2020) 'Critical supply shortages – The need for ventilators and personal protective equipment during the Covid-19 pandemic', *New England Journal of Medicine*, 382(e41). doi: 10.1056/nejmp2006141.

Rehak, D., Senovsky, P. and Slivkova, S. (2018) 'Resilience of critical infrastructure elements and its main factors', *Systems*, 6(2), pp. 125–138, doi: 10.3390/systems602002.

Remko, V.H. (2020) 'Research opportunities for a more resilient post-COVID-19 supply chain – Closing the gap between research findings and industry practice', *International Journal of Operations and Production Management*, 40, pp. 341–355. doi: 10.1108/IJOPM-03-2020-0165.

Schmid, B., Raju, E. and Jensen, P.K.M. (2021) 'COVID-19 and business continuity – Learning from the private sector and humanitarian actors in Kenya', *Progress in Disaster Science*, 11, pp. 1–8, doi: 10.1016/j.pdisas.2021.100181.

Shpiro, S. (2021) 'Israeli intelligence and the coronavirus crisis', *International Journal of Intelligence and CounterIntelligence*, 34(1), pp. 1–16. doi: 10.1080/08850607.2020.1805711.

Smith, D. and Sipika, C. (1993) 'Back from the brink-post-crisis management', *Long Range Planning*, 26, pp. 28–38. doi: 10.1016/0024-6301(93)90230-D.

The Organisation for Economic Co-operation and Development (OECD) (2019) *Good governance for critical infrastructure resilience*, OECD Reviews of Risk Management Policies, Paris: OECD Publishing. doi: 10.1787/ 02f0e5a0-en.

World Health Organization (WHO) (2020) *Coronavirus disease 2019 (COVID-19)*, Situation report – 45, Geneva: WHO.

Zio, E. (2016) 'Challenges in the vulnerability and risk analysis of critical infrastructures', *Reliability Engineering and System Safety*, 152, pp. 137–150. doi: 10.1016/j.ress.2016.02.009.