Proceedings of the 32nd European Safety and Reliability Conference (ESREL 2022)
Edited by Maria Chiara Leva, Edoardo Patelli, Luca Podofillini, and Simon Wilson
 Published by Research Publishing, Singapore.
doi: 10.3850/978-981-18-5183-4_S21-02-213-cd

Evaluation of the proposed European Commission directive on critical entities resilience and its potential to consolidate the resilience terminology

Arto Niemi, Frank Sill Torres

Department for Resilience of Maritime Systems, Institute for the Protection of Maritime Infrastructures, German Aerospace Center (DLR), Germany. E-mail: arto.niemi@dlr.de

The European Commission (EC) has proposed a new directive on critical entities resilience. The aim is to enhance the protection and to unify the approaches in different member states. The stated novelty of this directive lies in the thought that protecting the infrastructure is not sufficient. Therefore, it is necessary to reinforce the resilience of the critical infrastructure operators. This paper gives a brief overview on past legislative developments in critical infrastructure protection and attempts to evaluate the impact of the new EC proposal. We base the estimate on impact analyses past legislation. There are two key findings. EC legislation leaves the implementation to the member states, which gives them a certain freedom to interpret the text of EC directives. This has led to heterogeneous adaptation of the legislation within member states. This kind of heterogeneous impact will likely be also the result of the current proposal. Secondly, EC directives have had mandates for cooperation between member states. These have resulted in member states developing common vocabularies in the focus areas of directives. In the resilience engineering field, this may have a significant consolidating effect, as technological resilience is still a new concept associated with some ambiguity around its definition. Our paper discusses this matter and provides evidence that existing legislation had already a consolidating effect in the resilience engineering field.

Keywords: Resilience terminology, Critical infrastructure, European directive.

1. Introduction

Critical infrastructures (CI) are vital for a state's society and economy. For example, in the maritime field, certain passenger and freight transport companies, ports, energy providers, and vessel tracking services are seen as critical EC (2020a). Disruptions in these services could cause supply shortages, endanger public safety and well-being, as well as the economy. Due to their importance, states have sought to protect their CI.

This paper focuses on a new proposed directive by European Commission EC (2020a) on critical entities resilience. These are public or private CI operators. Section 2 provides key aspects of the proposal. It should receive attention, as it may affect many states. The European single market forms an area where goods, services, capital, and labor can move freely Bublitz (2018). It consists of European Union Member States (MS) and some participants, which are shown in Fig. 1.

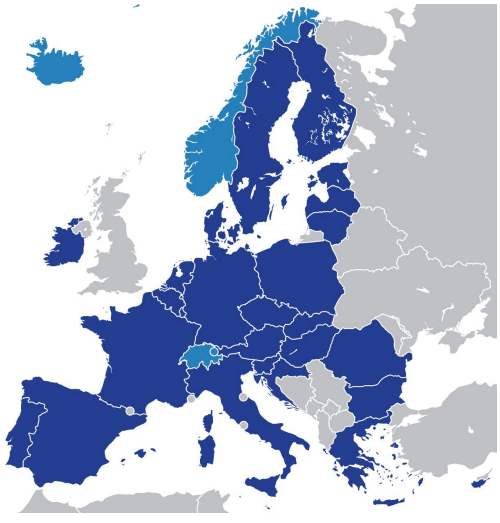

Fig. 1. EU member states in blue and other participants to the single market in cyan, Wikimedia Commons (2021).

In this setup, CI protection is not only a security matter. A risk exists that a certain MS can have more lenient regulation, which could cause a situation where businesses in this state have a competitive advantage in the single market. To avoid this problem, EC seeks to maintain a *"Level play-*

ing field" by harmonizing regulatory approaches in MS. Critical infrastructure can be owned and operated publicly or privately. Therefore, a need to harmonize regulations exists also in this area.

The impact of earlier regulations in the CI protection field is assessed in section 3.1. This assessment is used for estimating the potential impacts of the new proposal in section 3.2. EU directives have requirements for cooperation between MS. In the past, these have led to an adaptation of common terminology on the subject of a directive. This will likely be one of the most concrete impacts of the proposed directive EC (2020a). Due to the size and importance of the single market, EC regulations have had a global impact through the so-called *"Brussels effect"* Bradford (2020). While this may be true, section 2 shows that the current legislative interest to protect CI can be traced to the USA. Section 4 provides evidence that the legislation in the USA has already had a consolidating effect on resilience terminology, which may strengthen if the EU adopts a similar resilience definition.

2. Background on CI protection legislation and the new EU proposal

There has always been an interest to protect infrastructures that are essential for societal well-being. According to van der Vleuten et al. (2013), the origins of the current legislative interest to protect CI can be traced to the USA. A commission on CI protection was created by Clinton (1996) as a response to new cyber-threats. Moreover, in the early 2000s, terrorist attacks and power blackouts led to new legislation in the USA and an EC directive on CI protection in 2008 EC (2008). However, this EC directive only applies on the energy and transport sectors. But, other parallel initiatives have also helped to enhance CI protection EC (2020a).

The term *"critical infrastructure resilience"* also appears to originate from the USA. The term was already mentioned in a report NIAC (2009) and was later in the title of an executive order by Obama (2013a). Resilience is defined almost similarly in both documents. In the latter, resilience means *"the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents."* Rather similarly in EC (2020a), resilience means *"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."*

The reasons for the shift from CI protection to resilience are interesting. Rød et al. (2020) states that resilience covers the phases before, during, and after a disruptive event. This is required having in mind that complete protection can never be guaranteed. OECD (2019) defines resilience as the capacity to absorb a disturbance, recover from disruptions and adapt to changing conditions. This is required due to uncertainties surrounding disaster events. For example, climate change adaptation requires approaches that prepare CI assets and systems with capacities to be restored and rehabilitated swiftly.

The proposed European directive EC (2020a) states several motivating factors for the new legislation. Firstly, operators are not fully aware of or do not fully understand the implications of the dynamic risk landscape within which they operate. Secondly, resilience efforts diverge significantly between the Member States and sectors. Thirdly, similar types of entities are recognized as being critical by some Member States but not by others. The last two points appear specific for the Single Market, where diverging regulations can create competitive edges for certain states. Yet, the proposal gives further motivation stating that due to the interconnected nature of service provision, an insufficient level of resilience of an individual operator poses a serious risk for the others elsewhere in the internal market.

To give a summary of the legislation, the proposal contains four key items: 1) National frameworks on the resilience of critical entities, whose tasks include setting MS strategic objectives and priorities, performing periodical risk assessments, and identification of critical entities. 2) Resilience measures of critical entities, which include i) carrying out periodical risk assessments ii) having

technical and organizational measures to ensure their resilience, and iii) notifying authorities on significant disruptions. 3) Critical entities with European significance will be subject to additional oversight. 4) There will be a Critical Entities Resilience Group to facilitate cooperation between states.

3. Can legislation enhance CI protection?

3.1. *Impact assessments*

This section presents four examples of legislation with its impact assessments related to CI protection. These examples are from the USA and EU.

Example 1 Obama (2013a) mandated the Department of Homeland Security (DHS) and other federal agencies in the USA to conduct several tasks to strengthen the security and resilience of CI. The main ones were to 1) identify and prioritize CI; 2) maintain national CI centers that shall provide a situational awareness; 3) provide assistance to CI owners and operators; and 4) conduct comprehensive assessments of the CI vulnerabilities in collaboration with CI owners and operators.

The impact of this order has been in GAO (2012) and Currie (2016). One of the reported key issues was that the DHS had to conduct CI vulnerabilities surveys on a voluntary basis. This means, the DHS can only succeed at improving security if asset owners and operators were willing to participate. Furthermore, there were no requirements for the owner or the operator to take actions based on findings. This led to a situation in which, for example, the cost of security upgrades can be a barrier to implement enhancements.

Example 2 A presidential executive order Obama (2013b) led the National Institute of Standards and Technology (NIST) to publish a voluntary framework of cyber-security standards and procedures for CI sectors to adopt. However, report GAO (2020) noted that as of November 2019, most of the sector-specific (federal) agencies (SSA) had not developed methods to determine the level and type of framework adoption and had not yet reported on sector-wide cyber-security improvements. The report further states that until SSAs provide these reports, the extent to which the CI sectors are improving the protection of their infrastructures from threats will be largely unknown. Regardless of these issues, report GAO (2020) conducted interviews of 12 organizations, which reported to be already fully or partially using the framework. However, it is unclear if this finding from a small sample can be generalized for all CI organizations.

Example 3 A directive on security of Network and Information Systems (NIS) EC (2016) created new requirements for operators of essential services and digital service providers in EU member states. These include 1) identification of the operators of essential services on MS's territory; 2) MS-specific national strategy on the NIS security defining the strategic objectives and policy & regulatory measures to achieve and maintain a high level of security of these systems; 3) designation of MS-specific computer security incident response teams; 4) setting-up cooperation groups; 5) need to notify authorities of significant incidents.

Report EC (2020b) was critical for the heterogeneous implementation of the directive, as a lack of definitions left room for interpretation in MS. However, Drougkas et al. (2021) surveyed 947 organizations in 27 MS. As depicted in Fig. 2, one of the findings was that about 67 % of the surveyed organizations had made investments as a result of directive EC (2016). The average amount was

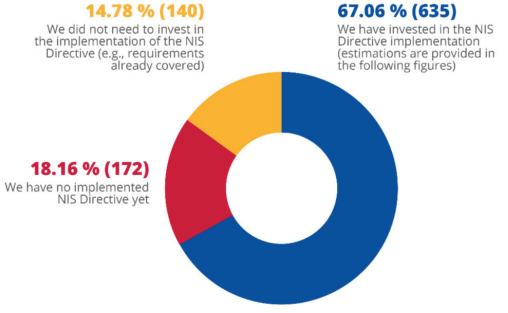

Fig. 2. The majority of organizations surveyed in Drougkas et al. (2021) have invested in security to implement directive EC (2016).

98,000 € and the median 40,000 €. The average value is about 10 % of the total information security spending for a typical operator of essential services or a digital service provider. One can assume that these investments led to improvements. Almost half of the organizations evaluated that the directive had a significant or very significant impact on their security posture.

Example 4 is the most interesting one, as the proposed directive EC (2020a) may repeal the directive EC (2008) on CI protection. Reports EC (2012) and EC (2019b) assessed the impact of this directive. The latter is more comprehensive and it was done over a decade after the legislation was introduced. Due to these reasons, we based our assessment on it.

EC (2008) mandates the following activities:

(1) Identification and designation of *"European"* CI (ECI) located in MS, the disruption or destruction of which would have a significant impact on at least two MS;
(2) Drafting of operator security plans that documents critical assets and security measures as well as identification of security liaison officers to serve as the point of contact between the ECI owner/operator and the MS authorities;
(3) Identification of ECI protection contact points to coordinating issues within and between MS and with the EC;
(4) Conduction of an initial threat assessment for designated ECI and reporting generic data on risks, threats and vulnerabilities on a summary basis to the EC every two years.
(5) EC supports ECI owners and operators through MS authorities by providing access to available best practices and methodologies as well training and the exchange of information.

The directive affected energy and transport sectors. However, many MS were already carrying out threat assessments in these sectors. Report EC (2019b) found that not all identified ECI were designated. Out of 93 designated ones only five were in the transport sector and others in the energy sector. One must highlight that only 10 MS had designated an ECI and 60 % of them were in just two MS.

A second major issue was also related to heterogeneous implementation measures. According to EC (2019b), each MS adopted the operator security plans using their interpretations of what needed to be done. This led to the adoption of different criteria for use in assessing risks for each MS. Each country could also define the competent authorities within an MS. On average three different actors are involved per MS. These actors further vary between MS leading to a fragmented approach.

On the positive side, the directive introduced a common European vocabulary, which is a prerequisite for effective cross-border dialogue and mutual understanding. 11 MS for the first time introduced legislation and other measures aimed at identifying CI, and 10 MS began carrying out threat assessments within the energy and transport sectors. However, there was value perceived by those MS with a CI protection framework already in place before 2008.

For example, Pursiainen (2018) compared the solutions in Nordic countries to the current EC-sponsored approaches. He found that these countries have based their policies on securing vital societal functions rather than the individual infrastructures that support these functions. Thanks to this, these countries have arguably a better starting point for making their CI resilient than most of the EU. Where the current approach has focused on protecting sector-specific infrastructures mainly against security threats, while in the Nordic countries the focus has been on societal resilience using an all-hazards approach.

3.2. *Potential impact of the critical entities resilience directive*

This section compares the proposed directive on critical entities resilience EC (2020a) against findings of the impact analyses in section 3.1. As it is an EC proposal, the priority is given to impact analyses of EU legislation. Also, unlike the reviewed items Obama (2013a) and Obama (2013a) from the USA, directive EC (2008) and the new proposed directive EC (2020a) are not voluntary

and give MS a mandate to perform assessments with CI owners and operators.

Despite the mandate, review EC (2019b) found that not all MS were designating ECI. The review states that the identification of ECI has been difficult because of the complexity of the procedure and the criteria that have to be met. These issues exist especially with regard to the application of the transboundary element and reaching an agreement with other MS. Review EC (2019b) further states that the directive EC (2008) lacks a monitoring and evaluation framework and dedicated funding to support its implementation.

Regarding the first point, the scope of the new directive EC (2020a) is different from the previous one. It is unnecessary that a disruption of a critical entity must have an impact in at least two MS. That means, identification in one MS is sufficient. In a case when an entity has been identified as critical by two or more MS, they shall engage in consultation with each other to reduce the burden on the entity. Additionally, there is a specific category for entities of which operation disruption could affect more than one third of MS. These entities will be subject to specific oversight on the EC level. For other critical entities, supervision and enforcement of the directive are left to MS.

EC (2008) has been criticized to be too specific and vague at the same time. Review EC (2019b) criticizes EC (2008) for only applying to energy and transport sectors, and Pursiainen (2018) notes that the focus is mainly on security threats. On the other hand, review EC (2019b), criticizes EC (2008) for being vague on actual requirements for the threat analyses and operator security plans.

Proposal EC (2020a) partially addresses these criticisms. Firstly, similar to the NIS directive EC (2016), the scope of the sectors is much wider. Secondly, mandated risk analysis has an all-hazards approach. That means, it shall account for all relevant natural and man-made risks, including accidents, natural disasters, public health emergencies, and antagonistic threats, including terrorist offenses.

In directive EC (2008), the requirements for an operator security plan has to cover at least: 1) identification of important assets; 2) conduct a risk analysis based on *major* threat scenarios, asset vulnerabilities, and potential impact; and 3) identification, selection, and prioritization of counter-measures. The countermeasures were further divided between permanent and graduated security measures, where the latter can be activated based on risk or threat level. In proposal EC (2020a), the required level of detail of the risk assessment is hard to assess, but the assessment will be more holistic. The assessment will cover: 1) measures to prevent incidents, including disaster risk reduction and climate adaptation; 2) physical protection of sensitive areas; 3) measures to resist and mitigate the consequences of incident; 4) measures to recover from incidents, taking into an account business continuity and the identification of alternative supply chains; and 5) employee security management. Points 1, 3, and 4 show that the focus of the proposal is on the resilience of critical entities, instead of just the protection of the physical infrastructures.

Considering the implementation, both the NIS directive EC (2016) and the proposal EC (2020a) have similar scopes and mandates for MS authorities to implement and enforce the obligations of the directive. While Drougkas et al. (2021) shows that operators of essential services have invested in security measures, according to the review EC (2020b) implementation has been highly heterogeneous. This is both in terms of what has been identified as an essential service provider and how many providers have been identified EC (2020b, 2019a).

Different MS can use individual criteria on what is considered an essential service. This includes thresholds, level of granularity of definition, and what additional services are included under the same definition[a]. Due to different thresholds, for example, a hospital with a certain size may be considered essential in one MS, while not in another.

There was also a concern that certain authorities do not have to fulfill their obligations, and that different security measures required by individual MS may lead to an uneven level of preparedness

[a]Beyond the services identified in EC (2016).

to cyber-security incidents. Report EC (2020b) is further critical of MS's efforts to supervise and enforce compliance to the directive. Regardless of this critique, the report concludes that the directive can be considered as a major first step in raising the common level of cyber-security among MS.

Interestingly, both the reviews on CI protection directive EC (2019b) and the NIS directive EC (2020b) state that these directives have greatly contributed to cooperation between MS. Specifically, EC (2019b) affirms that the directive led to the introduction of a common European vocabulary on CI protection. This is required for effective cross-border dialogue and mutual understanding. This kind of consolidation of resilience terminology will likely be one of the main outcomes of the proposed directive EC (2020a). Section 4 elaborates on this topic in the resilience engineering field.

4. Evidence of terminology consolidation as an effect of legislation

While the term *"resilience"* is used in various fields of science, this section focuses on its use in engineering. The origins of this term are in Latin where the word *"resilire"* stands for *"to jump back"* or *"to recoil"* Merriam-Webster (2021).

The use of this term in the system engineering field can be traced back to a concept by Holling (1996), who incorporated ideas from the stability of ecological systems into engineering systems. His concept originates from theories on how the population sizes of species change over time. It considers the 1) what is the magnitude of disturbance that a system can absorb unaltered or becoming extinct; 2) how strongly the system resists the disturbance, and 3) how quickly a system can recover to a normal state after a disturbance. This approach has been further developed by Hollnagel and Nemeth (2022) to formulate a success-oriented view on system safety.

Recently, a thorough literature review by Mottahedi et al. (2021) identifies the 20 most common terms used today for defining resilience in engineering science. The review concluded that technological resilience is still a new concept associated with some ambiguity around its definition. Further, an article by Kimber (2019) analyzes the use of the term resilience within the United Nations (UN). The UN defines resilience as *"the ability of a system, community or society exposed to hazards to resist, absorb, accommodate to and recover from the effects of a hazard in a timely and efficient manner, including through the preservation and restoration of its essential basic structures and functions"*. Kimber (2019) concludes that this term is used in the UN as a vague and flexible concept to signify a sense of direction.

In contrast to these findings, this section shows evidence that the resilience terminology has started to consolidate after it was included in CI protection legislation. We further conclude that this trend will strengthen if proposal EC (2020a) is approved. We base our analysis on comparing definitions of resilience before and after the report NIAC (2009) was published. We use articles Haimes et al. (2008) and Woods (2006) to assess the past view on resilience and compare this view to more recent articles by Woods (2015) and Mottahedi et al. (2021).

Haimes et al. (2008) defines resilience as the ability of the system to withstand a major disruption within acceptable degradation parameters and to recover within an acceptable cost and time. Their article also links the terms robustness and redundancy into the resiliency concept. For them, redundancy refers to the ability of certain system components to assume the functions of failed ones, without appreciably affecting the system performance. Robustness refers to the degree of insensitivity of a system's performance 1) to errors in the assumptions of design parameters, and 2) variations in the operational environment that may result in adverse operating conditions. On the other hand, Woods (2006) wants to reserve the resilience to concern the ability to recognize and adapt to handle *unanticipated* perturbations and to emphasize the system's ability to handle events that fall outside its design envelope.

The report NIAC (2009) defines infrastructure resilience as the ability to reduce the magnitude and/or duration of disruptive events. The effectiveness of a resilient infrastructure or enterprise depends upon its ability to anticipate, absorb,

adapt to, and/or rapidly recover from a potentially disruptive event. Similar ideas can be found in a later article by Woods (2015), which defines four concepts of resilience. These are rebound, robustness, graceful extensibility, and sustained adaptability.

The extent of how these terms are used currently is assessed based on a literature review by Mottahedi et al. (2021). However, the challenge is that Woods (2015) defines graceful extensibility as a system's ability to handle surprises, while robustness is understood as its ability to respond to known situations. Sustained adaptability is defined as the ability to adapt to future surprises as conditions evolve. It is not clear if these distinctions are understood similarly in other literature.

The most common term in the review of Mottahedi et al. (2021) is robustness. It is defined as the ability to resist disruption and absorb its effects without significantly reducing performance. Many of the other terms listed by the review link to similar ideas. These include *"absorptive & adaptive capabilities"*, *"vulnerability to disruption"*, *"reliability"*, *"survivability"*, and *"stability"*, which could be considered to reflect robustness. In addition, Mottahedi et al. (2021) mentions the term *"redundancy"* , which can be understood to improve robustness. There is some overlap. Definitions of adaptive capabilities and *"flexibility"* given by Mottahedi et al. (2021) are similar to the definition of graceful extensibility by Woods (2015). Further, the concept of sustained adaptability in Mottahedi et al. (2021) is covered by the term *"learning capacity*, which was only used in 1.6% of the analyzed papers.

The second most common term in review by Mottahedi et al. (2021) is *"recoverability"*. Again, there are many other terms linked this idea. These include *"rapidity of recovery"*, *"restorative capabilities"* and *"maintainability"'*. This links to the concept of rebound by Woods (2015). However, this specific term was not in the list.

Interestingly, Mottahedi et al. (2021) includes the term *"early warning and predictability"*, which is connected to prognostics and health management. One can imagine that it improves systems' rebound capability as defects can be corrected before they result in failures. Mottahedi et al. (2021) further lists the term *"availability"*, which can be seen to be a result of a resilient system.

To further understand how the resilience concept has evolved, we use motivations given in OECD (2019) and Rød et al. (2020). Unlike in Woods (2006), the emphasis is not only on absorbing unanticipated perturbations. OECD (2019) states that the shift from protection to resilience was prompted by uncertainties in magnitude and impact of disruptive events. Due to this, it is necessary to have absorptive, recovery, and adaptive capabilities. Therefore, the view on resilience is closer to the later paper by Woods (2015). Rød et al. (2020) states that resilience covers the phases before, during, and after a disruptive event. The reason is that complete protection can never be guaranteed, as it is impossible to safeguard against all threats, even the known ones. Also, achieving the desired level of protection is normally not cost-effective in relation to the actual threats. One can derive that when protection cannot be guaranteed, the abilities for absorption and quick recovery become necessities.

5. Conclusions

This paper presented a short history of CI protection legislation and the transition from protection to resilience and four examples of impact assessments that were conducted on these pieces of legislation. Our paper used these assessments to evaluate the potential impact of the proposed European Commission directive on critical entities resilience EC (2020a).

While the past directives have improved CI protection, individual member states have had a chance to interpret how to best implement directives. Due to this, these directives have had a heterogeneous impact in member states. This kind of heterogeneous impact will likely be also the result of the current proposal. However, one of the most concrete impacts of EC directives has resulted from the cooperation mandates between states. These have led to an introduction of common vocabularies in the focus areas of directives. In the resilience engineering field, this may have

a significant consolidating effect, as technological resilience is still a new concept associated with some ambiguity around its definition.

References

Bradford, A. (2020). *The Brussels Effect*. Oxford University Press.

Bublitz, E. (2018). The European single market at 25. *Intereconomics 53*, 337 – 342.

Clinton, W. J. (1996). Executive order 13010, The White House.

Currie, C. (2016). Testimony GAO-16-791T, United States Government Accountability Office.

Drougkas, A., V. Paggio, J. Gomez Prieto, P. Abel, F. Gratiolet, and E. Maaskant (2021). NIS investements. Report, The European Union Agency for Cybersecurity (ENISA). (CC BY 4.0).

EC (2008). Directive 2008/114/EC, European Commission.

EC (2012). Commission staff working document SWD(2012) 190 final, European Commission.

EC (2016). Directive 2016/1148, European Commission.

EC (2019a). Report COM(2019) 546 final, European Commission.

EC (2019b). 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. Final report, European Commission.

EC (2020a). Directive proposal COM/2020/829 final, European Commission.

EC (2020b). Staff working document SWD(2020) 345 final, European Commission. Annex 5.

GAO (2012). Report to Congressional requesters GAO-12-378, United States Government Accountability Office.

GAO (2020). Report to Congressional Committees GAO-20-299, United States Government Accountability Office.

Haimes, Y. Y., K. Crowther, and B. M. Horowitz (2008). Homeland security preparedness: Balancing protection with resilience in emergent systems. *Syst. Eng. 11*, 287 – 308.

Holling, C. S. (1996). Engineering resilience versus ecological resilience. In *Engineering with ecological constraints*, pp. 31–44. National Academy Press.

Hollnagel, E. and C. P. Nemeth (2022). From resilience engineering to resilient performance. In *Advancing Resilient Performance*, pp. 1 – 9. Springer.

Kimber, L. R. (2019). Resilience from the United nations standpoint: The challenges of "vagueness". In *Exploring Resilience*, pp. 89 – 96. Springer.

Merriam-Webster (2021). "resile". [Online].

Mottahedi, A., F. Sereshki, M. Ataei, A. Nouri Qarahasanlou, and A. Barabadi (2021). The resilience of critical infrastructure systems: A systematic literature review. *Energies 14*, 1571.

NIAC (2009). Critical infrastructure resilience – Final report and recommendations. Report, National Infrastructure Advisory Council.

Obama, B. (2013a). Presidential Policy Directive PPD 21, The White House.

Obama, B. (2013b). Executive order 13636, The White House.

OECD (2019). *Good Governance for Critical Infrastructure Resilience*. OECD Publishing.

Pursiainen, C. (2018). Critical infrastructure resilience: A Nordic model in the making? *Int. J. Disaster Risk Reduct. 27*, 632 – 641.

Rød, B., D. Lange, M. Theocharidou, and C. Pursiainen (2020). From risk management to resilience management in critical infrastructure. *J. Manag. Eng. 36*, 04020039.

van der Vleuten, E., P. Högselius, A. Hommels, and A. Kaijser (2013). Europe's critical infrastructure and its vulnerabilities – Promises, problems, paradoxes. In *The Making of Europe's Critical Infrastructure*, pp. 3–19. Palgrave Macmillan.

Wikimedia Commons (2021). EU single market. [Online].

Woods, D. D. (2006). Essential characteristics of resilience. In *Resilience Engineering: Concepts and Precepts*, pp. 21–34. CRC Press.

Woods, D. D. (2015). Four concepts for resilience and the implications for the future of resilience engineering. *Reliab. Eng. Syst. Saf. 141*, 5–9.