Journal of Decision Systems

ISSN: (Print) (Online) Journal homepage: www.tandfonline.com/journals/tjds20

Towards a framework for improving cyber security resilience of critical infrastructure against cyber threats: a dynamic capabilities approach

Jonna Järveläinen, Duong Dang, Mike Mekkanen & Tero Vartiainen

To cite this article: Jonna Järveläinen, Duong Dang, Mike Mekkanen & Tero Vartiainen (2025) Towards a framework for improving cyber security resilience of critical infrastructure against cyber threats: a dynamic capabilities approach, Journal of Decision Systems, 34:1, 2479546, DOI: 10.1080/12460125.2025.2479546

To link to this article: https://doi.org/10.1080/12460125.2025.2479546

Published online: 28 Mar 2025.

JOURNAL OF DECISION SYSTEMS
2025, VOL. 34, NO. 1, 2479546
https://doi.org/10.1080/12460125.2025.2479546

Taylor & Francis
Taylor & Francis Group

Towards a framework for improving cyber security resilience of critical infrastructure against cyber threats: a dynamic capabilities approach

Jonna Järveläinen [a], Duong Dang [b], Mike Mekkanen [b] and Tero Vartiainen [b]

[a]Faculty of Information Technology, University of Jyväskylä, Jyväskylä, Finland; [b]Computer Science, University of Vaasa, Vaasa, Finland

ABSTRACT

Interruptions in critical infrastructures (CIs) such as energy grids, telecommunication networks, or transportation can have severe and lasting impacts on societies. CIs are vulnerable to disruptions like cyberattacks, necessitating enhanced resiliency. This conceptual paper focuses on ensuring CI resiliency with dynamic capabilities, which have been previously applied mainly in organisational resiliency literature. On the operational level, when a disruption event happens, we explore the use of an AI-enabled tool and collective mindfulness processes and consider them essential in sensing, seizing, and transforming the organisation. However, when the organisation learns, these response practices facilitate transforming the organisation on a strategic level. Two cases are used to illustrate the conceptual framework idea.

ARTICLE HISTORY
Received 29 August 2024
Accepted 4 March 2025

KEYWORDS
Critical infrastructure; resilience; dynamic capabilities; artificial intelligence tools; collective mindfulness

1. Introduction

Critical infrastructures, such as energy and telecommunication networks and healthcare organisations, are vulnerable to cyberattacks and other disruptions (Kovacevic & Nikolic, 2014). On 23 December 2015, almost a quarter of a million Ukrainians experienced a power outage for several hours, due to a series of cyberattacks (Kostyuk & Zhukov, 2017). Although the outage lasted only for hours, we can only imagine the impact (heating, Christmas preparations, etc.) in the middle of winter 2015 in a Northern European country.

Critical infrastructure (CI) resilience is a complex issue since infrastructures often are maintained by several organisations, are interdependent and have several layers of sedimented history (Cedergren et al., 2018; Niemimaa, 2016). CIs have to be reliable, so their ability to 'bounce back' after any kind of unexpected event, i.e. resilience, is essential (Cedergren et al., 2018). Prior research has concluded that reliability requires both routines and standardised practices and improvisation or continuous management of fluctuations (Weick et al., 1999), which also could be described as resilience.

CONTACT Jonna Järveläinen jonna.k.jarvelainen@jyu.fi Faculty of Information Technology, Information Systems Research Division, University of Jyväskylä, Mattilanniemi 2, Jyväskylä 40100, Finland

One possibility to reach reliability and resilience is by using the organisation's dynamic capabilities (Sinha & Ola, 2021). Dynamic capabilities emphasise the ability to react adequately and timely to changes that require a combination of multiple capabilities. In this regard, DCs can be useful in cybersecurity environments where firms should have the ability to deal adequately and timely with cybercrime, for example by using technological resources such as AI detection tools (Ozkan-Okay et al., 2024), but also managerial resources. This allows firms to survive by continuously supporting existing products or services to be made, sold, and serviced to their customers (Teece & Pisano, 2003).

According to prior research, collective mindfulness is another means to improve reliability and resiliency (Butler & Gray, 2006; Salovaara et al., 2019). Collective mindfulness is defined as the 'capability to induce a rich awareness of discriminatory detail and a capacity for action' (Weick et al., 1999) and the aim is often to improve organisational performance (Badham & King, 2021). Collective mindfulness is central in high-reliability organisations such as nuclear plants (Sutcliffe, 2011) or companies providing anti-malware services (Salovaara et al., 2019), which share similarities with CIs.

Further, current advances in artificial intelligence (AI) also have been found useful in maintaining CI resilience. Alkhaleel (2024) have summarised numerous machine-learning algorithms that can facilitate CI resilience. Sarker et al. (2024) have examined rule-based AI and its application in CI cybersecurity risk management.

Dynamic capabilities, collective mindfulness, and AI try to improve organisational performance (Badham & King, 2021; Olan et al., 2022; Steininger et al., 2022), for example by enhancing resiliency (Alkhaleel, 2024; Butler & Gray, 2006; Sinha & Ola, 2021). However, how these dynamic capabilities, collective mindfulness, and AI are linked and how they can contribute to CI resiliency is a problem that we will focus on in this paper. Moreover, the literature discusses CI resiliency often focusing on different professionals at different times with different methods for a certain system layer (Cantelmi et al., 2021; Zio, 2016). But not, for example, in a holistic way considering resources (e.g. technical, managerial), capabilities, processes, and outcomes. We thus focus on this gap.

As CI resilience is so essential for society, applying novel theoretical approaches could also offer new solutions to existing problems. We noticed that although there are a few studies on organisational or critical infrastructure resilience using collective mindfulness (Cedergren et al., 2018; Hepfer & Lawrence, 2022; van der Merwe et al., 2018), they merely mention the theory instead of utilising it in theorising. Dynamic capabilities have also been used in organisational resilience studies (e.g. Hepfer & Lawrence, 2022; Madani & Parast, 2023; Vakilzadeh & Haase, 2021) and are closely connected to the concept of resilience (Mentges et al., 2023), but they have not been explored so much in critical infrastructure resilience literature. Therefore, we ventured to examine the applicability of combining these two theoretical frameworks in the current paper.

Therefore, our research question in this paper is *How dynamic capabilities can support critical infrastructure resiliency?* We contribute to the literature by extending the usage of dynamic capabilities in the context of CI resilience, and we also propose a framework that links dynamic capabilities and CI resiliency, as well as the connection of collective mindfulness and AI tools with dynamic capabilities. Finally, our case examples can be used as a reference for the organisation in improving its CI's resiliency.

The paper is organised as follows. We introduce the background of this research in Section 2. Next, we propose a framework to improve the cybersecurity resilience of CIs in Section 3. Section 4 illustrates case examples using our proposed framework. The discussion and conclusions are presented in Sections 5 and 6.

2. Research background and theoretical framework

2.1. Critical infrastructure resilience

During the past two decades, the number of publications on CI resilience has increased (Osei-Kyei et al., 2021). New applications and topics have emerged in the areas of resilience assessment (Caetano et al., 2024), machine learning, and artificial intelligence (Alkhaleel, 2024; Sarker et al., 2024), and the use of digital twins (Brucherseifer et al., 2021; Salvi et al., 2022), just to name a few of them.

Research in this area has widened to such an extent that the concepts used in this area need clarification: Mentges et al. (2023) reviewed 93 resiliency-related concepts (e.g. avoidance, protection, situation awareness) and found that there are contrasting views on the same concepts. For the sake of simplicity, we use the definition by Cantelmi et al. (2021, p. 341) who defines CIs as 'large-scale, man-made systems that function interdependently to produce and distribute essential goods (such as energy, water, and data) and services (such as transportation, banking, and healthcare)'. They also are interconnected, and complex, and support public welfare, the growth of the economy, and public sector operations (Osei-Kyei et al., 2021).

Therefore, it is essential that CIs remain operational, well-protected, and resilient (Meydani et al., 2024; Pursiainen, 2018). Resiliency is a key property for CIs and management of resiliency is essential for the management of CIs (Cantelmi et al., 2021). Labaka et al. (2016, p. 22) define resilience as 'the ability of a system to prevent the occurrence of a crisis and the capacity to absorb the impact and recover to the normal state rapidly and efficiently when a crisis does occur'. In other words, resiliency is a holistic set of procedures encompassing the entire structure of an organisation, from the physical part, to ensure the ability to prevent, absorb, adapt, and recover from an attack, either physical or cyber. Labaka et al. (2016) further divide CI resilience into internal and external resilience as well as technical, organisational, and economic (social) resilience dimensions. Thus, those dimensions must cooperate to achieve the resiliency of the CIs, and focusing only on the technical dimension is not sufficient (see discussion on concepts of critical infrastructure resiliency in Mentges et al. (2023), Rathnayaka et al. (2022) and Wells et al. (2022)).

This raises the important question of managing CI resiliency to recover from incidents. Figure 1 shows the variety of CIs' responses to a disruptive event depending on their dynamic capabilities for allocating resources. In particular, CI system-C has a higher resiliency and quality of services supplied after recovery than CI system-A and CI system-B. Additional technological resources have been allocated to rebuild the system-C after the CIs have recovered from the disruption events. Therefore, the resiliency of CIs is improved by learning from disruptive events, and incidents.

In this paper, we use cyberattacks as examples of disruptions that may threaten the resiliency of CIs, although several other possible disruptions can have a drastic impact on CI resilience such as natural disasters (Osei-Kyei et al., 2021; Sakurai & Kokuryo, 2018).

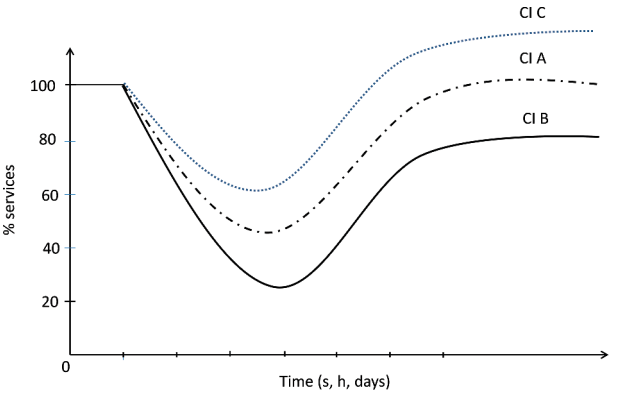

Figure 1. CIs have different resiliencies upon different responses based on different policies, picture by the authors.

2.2. Dynamic capabilities and resiliency

Dynamic capabilities refer to the ability to react adequately and timely to changes that require a combination of multiple capabilities (Eisenhardt & Martin, 2000; Teece & Pisano, 2003). In this regard, DCs can be useful in cybersecurity environments where firms require the ability to deal adequately and timely with cyber attacks (Goel et al., 2023; Kosutic & Pigni, 2021; Naseer et al., 2018). This allows firms to survive by continuously adapting their business models to ensure that existing products or services are developed, marketed, and supported for various clients. Components of DC include processes, resources (e.g., technological resources and organisational and managerial resources), environment (e.g. environmental uncertainty, external conditions), and strategies (e.g. IT strategy, business strategy) (Steininger et al., 2022; Suddaby et al., 2020).

The three processes of DCs are sensing, seizing, and transforming. These processes are important for firms as they help achieve goals, particularly in terms of resilience (Ferdinand, 2015; Jiang et al., 2021; Suddaby et al., 2020). Sensing indicates the capacity to sense, identify, and assess opportunities and threats (Teece & Pisano, 2003). In other words, sensing capacity allows a firm to deal with threats that are caused by environmental changes externally and internally. For example, sensing capability assists firms in identifying cybersecurity threats by adopting a socio-technical perspective rather than an overly technocentric approach. This enables firms to develop a holistic strategy for cybersecurity, effectively responding to cyber threats and contributing to the sustainability of energy systems (Dang & Vartiainen, 2024). Seizing refers to 'the implementation of a sensed opportunity, the mobilizing of resources to address an opportunity and capture its value' (Teece et al., 1997, p. 516). That is, seizing capability allows firms to achieve resiliency by responding and reacting quickly to the changing environments in the context of cybersecurity measures in CIs. For example, once the firm senses the opportunity, they will address it, such as, a supply chain firm can invest in the ability of systems to be resilient in dynamic environments and quickly recover from disruptions (Goel et al., 2023; Melnyk et al., 2014). This ensures they stay ahead in such environments and accelerate decision-making practices (Gu et al., 2021). Transforming refers to 'the process of resource configuration in which the organisation is continuously renewed'

(Teece, 2012). Reconfiguring is one of the key drivers for a firm's success because it helps the firm rearrange its existing resources to respond to changes or disruptions (Jiang et al., 2021; Yu et al., 2019).

Resources include both assets and capabilities (Rajala & Westerlund, 2016). Two main types of resources are 1) technological resources and 2) organisational and managerial resources (Steininger et al., 2022; Suddaby et al., 2020). Resources influence DCs, and in turn, DCs play an important role in the outcomes of an organisation. In particular, first-order outcomes related to observed organisational changes, such as the introduction of new resources, processes, or business practices, can be influenced by DCs. For example, in the digital era, firms need to change or transform their traditional business models by integrating digital technologies (e.g. robotics, cloud-based technology, artificial intelligence, digital twins, etc.) into their existing business models to ensure survival (Dang et al., 2024). DCs also affect the second-order outcomes that deal with the organisational performance effects of DCs (Cheng et al., 2014). Environments and strategies are important for organisations and their DCs. The environment can be considered an antecedent of dynamic capabilities, as competitive pressure and volatile circumstances significantly influence the formation of DCs (Steininger et al., 2022). Also, strategies (e.g. IT strategies and business strategies) are considered an antecedent of DCs, or events that are considered outcomes of DCs (Steininger et al., 2022).

With those abovementioned discussions about DCs coupled with the literature (c.f. Ferdinand, 2015; Goel et al., 2023; Kosutic & Pigni, 2021; Naseer et al., 2018), it can be argued that DCs can be used as a tool or an approach to help organisational resiliency when dealing with unstable environments, such as threats of wars, natural disasters, or cyberattacks.

2.2.1. Artificial intelligence as technological resource enhancing dynamic capabilities

Although there are many techno-centric or technological resources that can improve CI resiliency (Cantelmi et al., 2021), one technological resource might be AI. It can be used for several purposes in CIs, such as smart grids, for instance, for monitoring, analysing, controlling, interacting with markets, and detecting cyberattacks (Buettner et al., 2022). Therefore, artificial intelligence (AI) techniques can play a critical role in the modelling, analysis, and prediction of CIs' performance and resiliency (Alkhaleel, 2024; Laplante & Amaba, 2021). AI tools in CIs, such as the smart grids in the energy sector, can be classified into different kinds of expert systems, fuzzy logic, artificial neural networks, and genetic algorithms (Khosrojerdi et al., 2021).

Prior literature has presented several ways in which AI can be used to improve CI resiliency. For example, if a simulated digital twin is created of the energy grid, AI can be used for detecting anomalies and recovering from the incidents (Salvi et al., 2022). Babar et al. (2020) propose a resilient agent using machine learning to sense cyberattacks on the demand side of a smart grid. Tang et al. (2022) have identified several AI applications for enhancing the cyber threat defence of railway systems. AI and machine learning techniques have been found useful in cybersecurity solutions (Ozkan-Okay et al., 2024), although challenges also exist (Al-Hawawreh et al., 2024).

Therefore, AI can be considered a technological resource of an organisation because it can facilitate decision-making and enable timely responses. Organisations can also build their own AI systems, such as expert systems, or they can add or revise more rules, facts, or cases to the existing systems. In that sense, an AI system can be seen as the outcome of organisational learning or a capability that allows quick recovery from disruption.

2.2.2. Collective mindfulness an organisational and managerial resource enhancing dynamic capabilities

Dynamic capabilities may also be enhanced with organisational and managerial resources, for example with collective mindfulness. Aanestad and Jensen (2016), p. 14) define collective mindfulness as a 'capability of remaining "aware of something that may be important" (Merriam Webster's definition of mindful) in an open and undefined situation, where the organisational setting deems that this awareness goes beyond the individual to encompass the collective setting'. Mindful organisations have five social processes from which other organisations can learn. First, they are *preoccupied with failure* and try to use all failures (which are rare) and near-misses as learning opportunities (Weick et al., 1999). Second, they also try to investigate any kind of anomalies and listen to intuitions, not considering them as one-time-only events, but as signs of system health (Sutcliffe, 2011). This process is called *reluctance to simplify interpretations*. Third, they are *sensitive to operations* and aim to achieve a high level of situational awareness, usually as a team (Weick et al., 1999). Fourth, they are *committed to resilience* by anticipating problems and preparing for errors but also being capable of improvising when something unexpected happens. And last, they have *deference to expertise*: experts, who know the consequences of different decisions are given decision-making authority instead of relying on hierarchical decision-making (Vogus & Sutcliffe, 2017).

These five processes are considered to lead to collective mindfulness, which will lead to reliable operations and services (Weick et al., 1999). Thus, the objective of collective mindfulness is to improve organisational performance (although it also could aim to enhance organisational wisdom) (Badham & King, 2021). If we take an example from a CI area, i.e., the hospital sector, preoccupation with failure could be discussions with clinical staff after possible dangerous situations in an operating room, where the idea is not to find the guilty parties but to learn to avoid the same situation in the future. Reluctance to simplify interpretations might be that employees listen to their intuition and investigate, for instance, suspicious emails containing links to notice phishing attempts (Sipior et al., 2018). Sensitivity to operations in a hospital might be that all personnel, doctors, nurses, and IT experts, have their specific roles and they communicate with each other about anomalies. Commitment to resilience might mean that all employees are highly educated, experienced experts in their speciality and, therefore, capable of improvising if something happens, for instance, a ransomware attack. Deference to expertise might mean that if a nurse notices that blood pressure is quickly decreasing, the doctors will listen to the expert and make their own decisions considering the altered situation.

If we consider the three DC processes, sensing, seizing, and transforming, and the above-mentioned five CM processes, clear links can be noticed. Sensing and monitoring the environment (Sambamurthy et al., 2003) are closely connected to the sensitivity of operations, preoccupation with failure as well as reluctance to

Table 1. Summary of definitions used for central concepts.

Central concepts	Used definitions
Critical infrastructure	"large-scale, man-made systems that function interdependently to produce and distribute essential goods (such as energy, water, and data) and services (such as transportation, banking, and healthcare)"(Cantelmi et al., 2021, p. 341).
Resiliency	"the ability of a system to prevent the occurrence of a crisis and the capacity to absorb the impact and recover to the normal state rapidly and efficiently when a crisis does occur" (Labaka et al., 2016, p. 22)
Dynamic capabilities	the ability to react adequately and timely to changes that require a combination of multiple capabilities (Eisenhardt & Martin, 2000; Teece & Pisano, 2003)
Sensing	the capacity to sense, identify, and assess opportunities and threats (Teece & Pisano, 2003)
Seizing	"the implementation of a sensed opportunity, the mobilizing of resources in order to address an opportunity and capture its value" (Teece et al., 1997, p. 516).
Transforming	"the process of resource configuration in which the organisation is continuously renewed" (Teece, 2012).
Collective mindfulness	"capability of remaining 'aware of something that may be important' (Merriam Webster's definition of mindful) in an open and undefined situation, where the organisational setting deems that this awareness goes beyond the individual to encompass the collective setting" (Aanestad & Jensen, 2016, p. 14)

simplify interpretations. Organisations try effortfully to create situational awareness (sensitivity to operations), detect anomalies, and analyse them (preoccupation with failure) to sense whether some events might risk their survival, such as a cyberattack. Gärtner and Ribeiro Soriano (2011) have proposed that when an organisation is more mindful, it enhances the "capability of sensing opportunities" (p. 264), but we can argue also that collective mindfulness enhances the capability of sensing threats.

The second DC process, seizing opportunities for action, requires being prepared to act upon those opportunities. Thus, reluctance to simplify interpretations is essential in not regarding them as one-time anomalies but regarding their worth for further investigation and possible action (Gärtner & Ribeiro Soriano, 2011). If we consider a gradually developing cyberattack, which is difficult to notice without closely monitoring the environment for a long period, it might be ignored if anomalies are not detected and investigated, but interpretations are simplified. When the cyberattack is noticed then it is possible to seize the opportunity to start response activities.

Finally, the third DC process, transforming, can be linked with a commitment to resilience and deference to expertise. Trusting cybersecurity experts in deciding on how to respond to the attack with either previously developed procedures or improvised new response actions transforms the organisational performance and allows the organisation to learn from the situation (Romme et al., 2010).

Collective mindfulness is closely connected to business continuity management and organisational resilience (Butler & Gray, 2006). Although technical preparations have traditionally been the focus of business continuity, the meaning of social processes has also been recognised (Niemimaa, 2015; Niemimaa & Järveläinen, 2013). Not only technical redundancy or carefully planned disaster recovery procedures can lead to resiliency, but the constant management of fluctuations is performed by operative persons (Niemimaa, 2015), top management support is essential (Sarkar et al., 2016) and multi-talented teams are necessary for continued operations (Järveläinen, 2016). Table 1 summarises the essential concepts.

3. Framework for improving cyber security resilience of critical infrastructures

Summarising what we have discussed, we propose a framework to enhance the resilience of CI (Figure 2). The separate phases are discussed below.

First, organisations should acknowledge that vulnerabilities (2) are often triggered by environmental and operational changes (1). For example, environmental changes could be pandemics that push employees to remote work (Margherita & Heikkilä, 2021), industrial turbulence pressuring for business model change or cost savings (Kranz et al., 2016), or national policies demanding more reporting requiring also information systems changes. Organisations may also change their operations when adopting new processes or information systems (Järveläinen et al., 2022). These changes open possibilities for malicious agents to exploit new vulnerabilities, and thus, organisations should develop strategies to help them achieve resilience (Järveläinen et al., 2022). The difficulty is that the malicious agents also have dynamic capabilities and develop new cyber threats constantly (Choo, 2011).

Second, to minimise the impact of threats, organisations should respond to those (3). First, they have to sense the changes threatening them. For example, AI-enabled tools can be seen as an effective technical solution. In more detail, the strength of AI tools in cyberattacks, for example, is first to detect them quickly (sensing, i.e., identifying and assessing opportunities) and then to respond to them also quickly by mobilising resources to capture value from those opportunities, as well as reconfiguring routines. In that sense, AI tools can be considered a technological resource that enables dynamic capabilities. The role of collective mindfulness is to enhance the DC processes, which then improve the resiliency of the CIs. In a cyberattack situation, the collective mindfulness processes have a very short-term temporal dimension since the social processes of sensing, seizing, and responding to a cyberattack have to be fast, especially in an unexpected attack

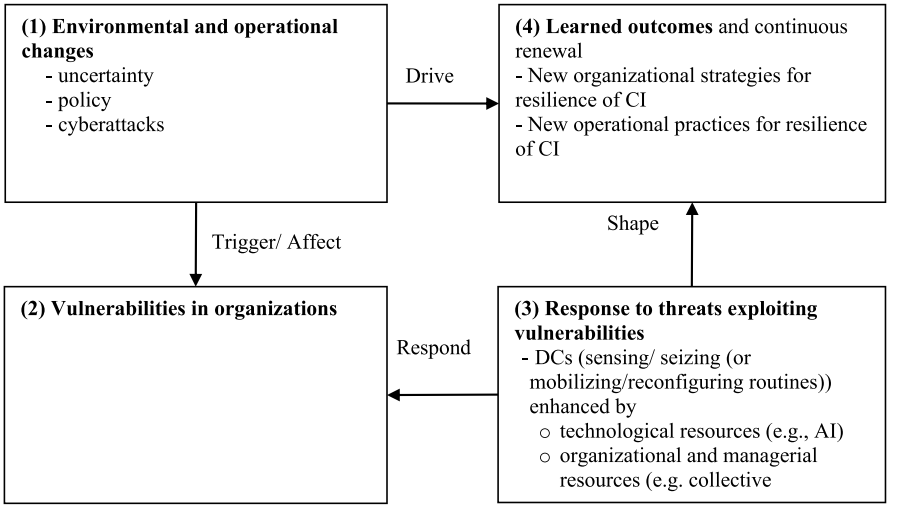

Figure 2. Framework to improve the resilience of CIs, source: the authors.

where an AI tool is not available. However, developing the collective mindfulness processes in the organisation to achieve this kind of capability takes a long time since the responding team or the whole organisation has to function well as a collective (see e.g. Erden et al., 2008). Nevertheless, if the organisation does not have high situational awareness and a capability to detect anomalies and analyse them, it is likely that they can not quickly respond to cyberattacks. When the incidents have been detected, collective mindfulness gives a possibility to seize the opportunity to respond. Often, organisations try to explain anomalies as one-time abnormalities, which mindful organisations are reluctant to do, i.e., simplify interpretations.

The timely responses utilising technological and managerial resources shape organisational learning and outcomes and continuous reviewal (4). Here, two new outcomes are shaped by the DC processes in (3). These outcomes will be continuously renewed due to the DC approach in (3). In terms of strategic level response, dynamic capabilities can be considered as an option to help organisations enhance their resilience. For example, an organisation might develop or adopt AI tools to detect and respond to cyberattacks after they have noticed that they have problems in that area. As such, AI tools now become the capabilities or strategies of an organisation. Collective mindfulness also facilitates the organisation to commit to resilience and listen to experts.

Therefore, the learned outcomes (4) include organisational strategies for the resilience of CI and operational strategies for the resilience of CI. And those strategies are shaped and influenced by responses (3) but also the environmental and operational changes (1). Operational practices are those practices that facilitate organisational survival in day-to-day operations, the constant management of fluctuations (Weick et al., 1999) such as the use of AI tools or collective mindfulness processes in the cyberattack response. They can also include, for example, processes (e.g. sensing, sizing, and transforming) and resources (e.g. technological resources and organisational and managerial resources). Organisational strategies, however, are the IT strategies or even business strategies that are developed further based on the learnings from the responses to threats. Dynamic capabilities enable the improvement of an organisation in the long term when the organisation learns from disruptive events and improves its resiliency or firm performance in similar situations. For example, a CI such as a hospital or an energy distribution organisation might improve their resiliency significantly and use it as a competitive advantage with customers.

Not all CI organisations or networks have dynamic capabilities nor collective mindfulness. The network of CI organisations is broad and includes a multitude of different actors, some very small with limited resources, but also, for example, high-reliability organisations such as nuclear power stations, or electricity network operators, which typically are very prepared to act quickly and have mature cybersecurity practices. These kinds of actors create best practices that can be distributed to others in due time (Zsidisin et al., 2005) and emerging regulations such as NIS2 at the EU level also demand certain cybersecurity maturity from the CI sector (2022).

4. Illustration of framework for improving cyber security resilience of critical infrastructure against cyber threats

4.1. Illustrative cases

To illustrate how our proposal of the framework works, we used two cases in which data were (1) from the lab at the University of Vaasa and (2) from public sources i.e. Greenberg (2018), Hern (2017), and Wesley et al. (2019). This method has been employed by scholars; for instance, Haaker et al. (2017) and Niemimaa et al. (2019) adopted this method to demonstrate their models.

First, we used the FREESI laboratory[1] (Future Reliable Electricity and Energy System Integration Laboratory) at the University of Vaasa and its capabilities as a means to demonstrate the use of technological resources in the framework. The laboratory provides a co-simulation environment that imitates a real-world process and system, i.e. the physical environments of the Vaasa Harbor microgrid in Finland (see also Kumar et al., 2023). The laboratory operates on information and operational technology, which allows the illustration of different cyberattack scenarios on the Vaasa Harbor microgrid (MG). It thus provides a realistic environment for assessing the effectiveness of our framework.

We use the proposed framework as an approach to improve resilience and test an AI-enabled tool – an expert system named Microgrid Controller – in the laboratory. In energy grids, the energy frequency must be stable constantly. We simulated a scenario of a cyberattack e.g. a delay attack that would delay transmissions received by certain network nodes (Lou et al., 2020). In short, the general electricity network's microgrid is a 120kV grid-connected distribution feeder. Figure 3 shows the microgrid topology. The topology has four consumers, called loads (Load 1 to Load 4, of which the first two are critical loads), and it has distributed energy resources (e.g. combined heat and power plant, photovoltaic generation systems, and battery energy storage systems).

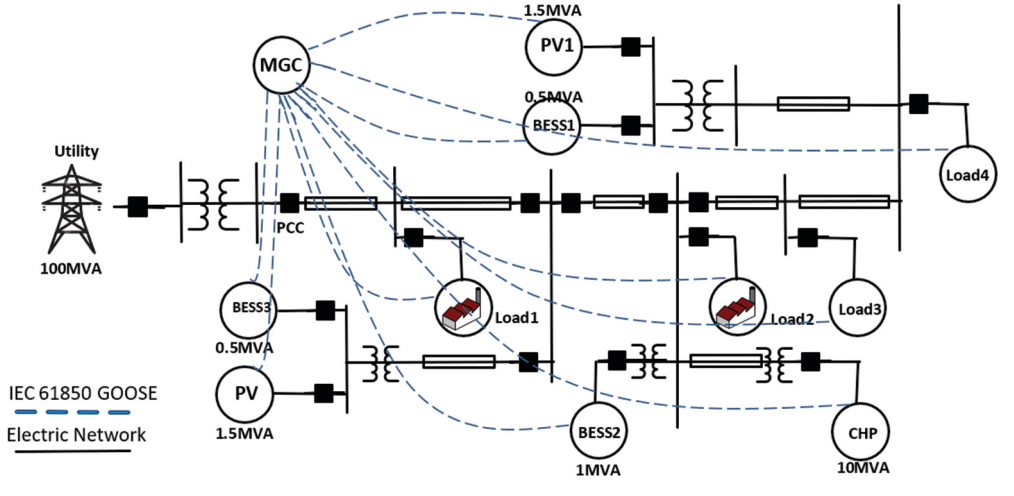

Figure 3. Energy Microgrid Topology, author generated picture.

Second, we used a case described in the literature as the MAERSK vs. NotPetya case to demonstrate the framework. In particular, we aim to illustrate the connection between dynamic capabilities and collective mindfulness in the following known case written based on several scientific sources (Greenberg, 2018; Hern, 2017; Wesley et al., 2019). On 27 June 2017, the NotPetya ransomware attack hit Maersk with 80.000 employees globally, in 574 offices of 8 business units in 130 countries. After the attack, Maersk started to cooperate with consulting company Deloitte and set up a recovery centre in London, England, to recover from the devastating attack that had shut down nearly all devices and systems in the company. This shows the changes in environments, as well as the threats.

4.1.1. Technical resilience of critical infrastructure: energy microgrid

Environmental and operational changes. As energy (micro)grids have become even smarter, they are managed with sensors, information networks, and information systems, although technicians are also essential for their resiliency (Niemimaa, 2016). Ports are critical infrastructures as they are essential hubs for human transportation but also central in supply chains (Romero-Faz & Camarero-Orive, 2017), and smart microgrids are necessary for port operations. Port operators and authorities try to achieve energy efficiency and reduction of emissions by using smart microgrids (Canepa et al., 2020).

Vulnerabilities in organisations. The digitality of the infrastructure allows constant monitoring and easy identification of possible problems, but on the other hand, the connectivity makes them vulnerable to cyberattacks (Niemimaa, 2023). Smart microgrids in ports are also vulnerable to various cyberattacks such as unauthorised access to a system or device, message relays, etc (Canepa et al., 2020). Since a balanced energy frequency (between energy consumption and generation) is critical for the operation of a microgrid, tampering with the messages that facilitate the balancing task – load-shedding tasks – is one possible vulnerability in the smart microgrid. Normally, so-called standardised GOOSE messages are used within the load-shedding task, which is a time-critical communication protocol maintaining balance in energy frequency. If the balance is lost, one possible impact is a blackout due to a mismatch between the generated power and the load.

In the designed scenario tested in the FREESI laboratory, the idea was that a cyberattack would separate (or island) the MG from Load 4 (Figure 3). This would cause an unbalanced energy frequency in the microgrid. In Figure 4, the cyberattack happened in second 1 causing the islanding of the MG. This created an imbalance between the generated and consumed energy leading to frequency fluctuation (and MG RMS value degradation). However, in the MG resiliency evaluation scenario, a delay attack was applied to the GOOSE trip command packets sent from the MG controller to Load 4. This developed scenario would cause problems (hardening) for the MG operation stability and the load-shedding function may fail to operate in the required timeframe (Figure 4, middle row). MG operation would face severe frequency and voltage oscillations due to the mismatch between the generated power and the load demand. In this real-time simulation setup, the EXata cyber system emulator was used to launch the cyber delay attack and applied to a specific communication link or a specific GOOSE message, and the reactions of the physical system can be seen in Figure 4 (middle row).

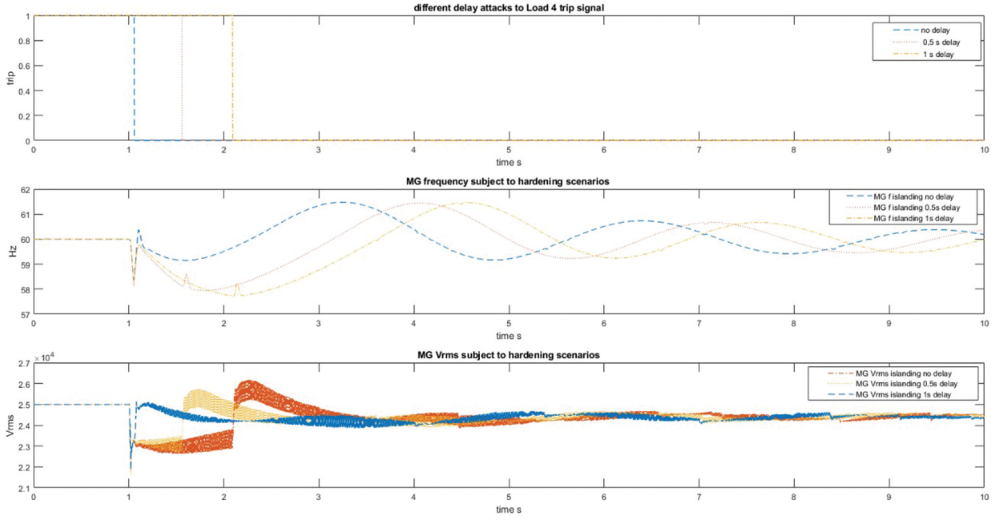

Figure 4. Microgrid real-time simulation subject to a delay attack, author generated picture.

Response to threats exploiting vulnerabilities. The organisation has to respond to possible cyberattacks to maintain the resiliency of its infrastructures. In particular, the AI-enabled tool (Microgrid Controller) can be used to extract and proceed with the measurements from the received GOOSE messages within the MG. The Microgrid Controller attempted to shed the settable Load 4 (Figure 3) to maintain the MG frequency stability. For example, if the differences between the total power generation and the total load consumption exceed 3 megawatts for any MG, the controlling algorithm output (dispatching signal) will be sent back to the model via additional new GOOSE messages. Furthermore, it detects the MG information system accepting delay limits and how the MG operational technology system determines if it will exceed these limits. This can be done by using Microgrid Controller intelligent electronic device-based AI in compliance with the IEC 61,850 standard (see e.g. Boas Leite et al., 2018).

Outcome. Considering the proposed framework, the expert system based on AI decision-making solutions can be seen as a resource and a capability for an organisation. In this case, AI was used as a response to react to the cyberattack, to seize it. However, when the organisation develops AI tools as they learn what kind of tools are effective and efficient, they can also facilitate the transformation of an organisation, as it allows them to reach an even better capability to respond to cyberattacks. AI tools first need to be developed by an organisation, then, it becomes their capability as an outcome of the process of dealing with threats. Also, they can be used for organisational operations as a response strategy.

4.1.2. Organisational resilience of critical infrastructure: the MAERSK vs. NotPetya case

Environmental and operational changes. The wide adoption of digital technologies in large corporations has led to IT-enabled or digital transformation, where organisations

either use information technologies to gain operational efficiencies or transform their business model and organisational identity (Wessel et al., 2021). The operational efficiency is enhanced with connectivity, which may turn global corporations into attractive targets for cybercriminals.

Vulnerabilities in organisations. A cyberattack is considered one of the main threats in securing critical infrastructure as it could have a wide and serious impact not only on an organisation but also on society (Venkatachary et al., 2018). In the Maersk vs. NotPetya case, an unprecedented cyberattack hit a global company, Maersk, operating numerous ports and ships around the world. The attack caused serious vulnerabilities to Maersk, as the company had to shut down nearly all devices and systems, which were infected within 15 minutes from the first detection of a cyberattack.

Response to threats exploiting vulnerabilities. In response to the attack, 400 Maersk IT and other personnel cooperated with 200 Deloitte staffers to first make sense of the situation. Together they had to be *sensitive to operations* since one person cannot create a useful and reliable situational awareness in such a vast scenario. Since possibly all computers were infected, together they decided that no Maersk laptops were allowed to access the Maersk network but new laptops and pre-paid Wi-Fi hotspots were bought from electronics stores nearby. Thus, the new disaster organisation was *preoccupied with failure*, they wanted to ensure that the ransomware would not affect the disaster organisation as well, and also showed *commitment to resilience* when they improvised in a difficult situation. In DC concepts, this could be called transforming.

Quickly the recovery centre noticed that three to seven days old backups of Maersk servers were available, but the domain controllers having the details of the network map, configurations, and access privileges (active directory) were lost. The domain controllers had been planned to synchronise with each other, but the company had not prepared for a scenario where all servers were simultaneously disrupted. Despite the scope of the disruption, the search for domain controller backup continued. That is, they were *reluctant to simplify the interpretation* that all was lost. In fact, one server in Ghana had suffered from a power outage before the attack and therefore still had a domain controller backup. They were *sensitive to operations* and seized the opportunity to use these backups.

Alongside this IT recovery, other global Maersk staff tried to operate ports with instant messages, email, and spreadsheets. They replaced some of the functionalities from the normal maerskline.com system with these improvised tools. This shows that staff was *committed to resilience*, and they were allowed to operate with the available tools since container vessels were still arriving at ports and many companies relied on Maersk's ability to ship their cargo. Staff had the expertise, so the company relied on that and had *deference to expertise*. In DC terms, Maersk was able to transform itself quickly to the new situation. That is, the company was resilient.

Outcome. Nowadays, Maersk regards cybersecurity as so important that it has a separate section in the company Code of Conduct (Maersk Code of Conduct, n.d.) and Cybersecurity terms for vendors (Cyber Security Schedule | Maersk Terms, n.d.), both publicly available. These could be regarded as part of an organisational cybersecurity strategy, which manifests the underlying operational practices. Therefore, we can

conclude that the learnings from ransomware recovery have improved the resiliency of Maersk.

5. Discussion and contributions

Several approaches can be considered to improve the cybersecurity resilience of CI organisations (Harrop & Matteson, 2013). Those approaches include, for example, technical (e.g. intrusion detection systems, firewalls, and software), organisational (e.g. appointing IT security officer, rules, monitoring of information security), and frameworks/standards (e.g. access management, awareness models, and assessment standards) (Lykou et al., 2018). Unfortunately, organisations often implement those approaches by using different professionals at different times with different methods for a certain system layer. This would create vulnerabilities that bad actors can exploit.

In this paper, we propose a holistic approach that would have the potential to cover technical, organisational, and social dimensions at many levels of an organisation as a theoretical contribution. Our idea is based on dynamic capabilities improving the resiliency of CIs. We explore the operational level capabilities such as AI-enabled tools and collective mindfulness processes and how they can be used in sensing, seizing, and transforming firstly in the incident response, at the operational level but later when the organisation learns, on the strategic, organisational level.

From prior literature, we know that components of DC include resources (e.g. technological resources; organisational and managerial resources), environment (e.g. environmental uncertainty; external conditions), and strategies (e.g. IT strategy; business strategy) (Steininger et al., 2022). Organisations often use technical approaches at the operational level to maintain the resilience of CIs (Gouglidis et al., 2018). AI-enabled tools are especially good at sensing the cybersecurity environment and quickly responding or seizing. Our framework covers this perspective by including resources as a part of responding features to threats, caused by environmental and operational changes (Figure 3). When technological tools become essential for an organisation, it will learn to rely on them for instance in responding to cyber threats and thus the resources will also help improve or transform the organisation.

The proposed framework covers further organisational and managerial resources by suggesting that collective mindfulness processes should be considered as a part of threat response processes. Not all cyber threats can be sensed by technological tools, which often are created after a new attack type has emerged. Therefore, mindful employees are needed in sensing and seizing activities, but later also in transforming the organisation for example by strategically putting more emphasis on the development of technological tools. The collective mindfulness processes will enhance the dynamic capabilities of an organisation to avoid and respond to interruptions and thus develop the organisation's resiliency on a higher level.

6. Conclusions

In conclusion, we suggest that dynamic capabilities can be used to ensure the organisational resilience of critical infrastructures. This is because dynamic capabilities help organisations to purposefully adapt an organisation's resource base to

address rapidly changing environments (Teece et al., 1997). Also, they help organisations do the right things rather than doing things right (Shuen et al., 2014). In terms of outcomes, our framework helps the organisation improve its resiliency not only in operational practices but also in organisational strategies. In this context, the framework provides guidance for practitioners to assess their organisations' readiness to respond to threats and offers strategies to address vulnerabilities. For instance, to evaluate an organisation's preparedness, managers can use this framework to map potential vulnerabilities (i.e. (2) in Figure 2) against their existing technological, organisational, and managerial resources (i.e. (3) in Figure 2). This assessment can be conducted by adhering to established standards (e.g. ISO, 2016; NIST, 2020) or by employing the Delphi method (Turoff, 1970). The Delphi method can also be utilised by policymakers to gather diverse perspectives on strategies when applying the framework at a national level for the protection of critical infrastructure.

The paper has limitations. As a conceptual paper, we only have demonstrated how the AI tool might function within the laboratory environment at the University of Vaasa's FREESI laboratory, as well as how collective mindfulness can be considered as part of dynamic capabilities with the MAERSK case. Our framework has not yet been tested or verified in other environments nor has a proof of concept from a real organisation. We thus call for future empirical studies to test the framework. For example, researchers can set up different scenarios in 'Environmental and Operational Changes' (Figure 2). These changes will lead to a potential list of 'Vulnerabilities in Organisation' (Figure 2). From this, researchers can study how different organisations respond to threats and how these responses shape organisational strategies for cybersecurity resilience. This can be achieved, for instance, by using case studies, as this method involves an in-depth examination of a phenomenon within its real-world context

Although in this paper, our case examples focus on technological and managerial resources separately, in a socio-technical organisational environment both resources are needed for ensuring the resilience of CIs. We also call for researchers to study the interplay of technical and managerial resources or human-AI interaction in CIs. Furthermore, as has been established, the CIs are usually a complex network maintained by several organisations, and our focus is on the organisational not inter-organisational level.

Future research can use our framework as a starting point to develop or revise a better framework for cybersecurity resilience in CIs and study what kind of dynamic capabilities are effective when enhancing the resilience of CIs and how they are developed. We also would like to invite future researchers to examine CI resiliency at the inter-organisational level.

Note

1. The laboratory is used for 'testing and training the IEC 61,850 based protection systems as well as OPAL-RT OP5600 real-time simulator platform, which at present time, enables controller hardware in the loop (CHIL) simulations of Smart Grids. The FREESI-lab is connected to the Sundom Smart Grid living lab environment, which is a real medium voltage grid providing a continuous IEC 61,850-based data stream from twenty nodes' (University of Vaasa, 2023)

Disclosure statement

No potential conflict of interest was reported by the author(s).

ORCID

Jonna Järveläinen http://orcid.org/0000-0003-2032-489X
Duong Dang http://orcid.org/0000-0002-9325-5496
Mike Mekkanen http://orcid.org/0000-0001-7300-0819
Tero Vartiainen http://orcid.org/0000-0003-3843-8561

References

Aanestad, M., & Jensen, T. B. (2016). Collective mindfulness in post-implementation is adaptation processes. *Information and Organisation*, *26*(1–2), 13–27. https://doi.org/10.1016/J.INFOANDORG.2016.02.001

Al-Hawawreh, M., Baig, Z., & Zeadally, S. (2024). AI for critical infrastructure security: Concepts, challenges, and future directions. *IEEE Internet of Things Magazine*, *7*(4), 136–142. https://doi.org/10.1109/IOTM.001.2300181

Alkhaleel, B. A. (2024). Machine learning applications in the resilience of interdependent critical infrastructure systems-A systematic literature review. *International Journal of Critical Infrastructure Protection*, *44*, 100646. https://doi.org/10.1016/j.ijcip.2023.100646

Babar, M., Tariq, M. U., & Jan, M. A. (2020). Secure and resilient demand side management engine using machine learning for IoT-enabled smart grid. *Sustainable Cities and Society*, *62*, 102370. https://doi.org/10.1016/j.scs.2020.102370

Badham, R., & King, E. (2021). Mindfulness at work: A critical re-view. *Organisation*, *28*(4), 531–554. https://doi.org/10.1177/1350508419888897

Boas Leite, J., Sanches Mantovani, J.R., & Kezunovic, M. (2018). Distribution system self-healing implementation using decentralized ied-based multi-agent system. *2018 IEEE PES Transmission & Distribution Conference and Exhibition - Latin America (T & amp;D-LA)* (pp. 1–5). https://doi.org/10.1109/TDC-LA.2018.8511788

Brucherseifer, E., Winter, H., Mentges, A., Mühlhäuser, M., & Hellmann, M. (2021). Digital Twin conceptual framework for improving critical infrastructure resilience. *At - Automatisierungstechnik*, *69*(12), 1062–1080. https://doi.org/10.1515/auto-2021-0104

Buettner, R., Breitenbach, J., Gross, J., Krueger, I., Gouromichos, H., Listl, M., Leicht, L., & Klier, T. (2022). A systematic literature review of machine learning approaches for detecting events and disturbances in smart grid systems. *2022 IEEE 46th Annual Computers, Software, and Applications Conference (COMPSAC)* (pp. 1786–1791). https://doi.org/10.1109/COMPSAC54236.2022.00284

Butler, B. S., & Gray, P. H. (2006). Reliability, mindfulness, and information systems. *MIS Quarterly*, *30*(2), 211. https://doi.org/10.2307/25148728

Caetano, H. O., Desuó, L., Fogliatto, M. S. S., & Maciel, C. D. (2024). Resilience assessment of critical infrastructures using dynamic Bayesian networks and evidence propagation. *Reliability Engineering and System Safety*, *241*, 109691. https://doi.org/10.1016/j.ress.2023.109691

Canepa, M., Frugone, G., Bozzo, R., & Schauer, S. (2020). Micro smart micro-grid and its cyber security aspects in a port infrastructure. *American Journal of Information Science and Technology*, *4*(1), 1. https://doi.org/10.11648/j.ajist.20200401.11

Cantelmi, R., DiGravio, G., & Patriarca, R. (2021). Reviewing qualitative research approaches in the context of critical infrastructure resilience. *Environment Systems and Decisions*, *41*(3), 341–376. https://doi.org/10.1007/s10669-020-09795-8

Cedergren, A., Johansson, J., & Hassel, H. (2018). Challenges to critical infrastructure resilience in an institutionally fragmented setting. *Safety Science*, *110*, 51–58. https://doi.org/10.1016/J.SSCI.2017.12.025

Cheng, J. H., Chen, M. C., & Huang, C. M. (2014). Assessing inter-organisational innovation performance through relational governance and dynamic capabilities in supply chains. *Supply Chain Management: An International Journal*, *19*(2), 173–186. https://doi.org/10.1108/SCM-05-2013-0162/FULL/PDF

Choo, K. -K. R. (2011). The cyber threat landscape: Challenges and future research directions. *Computers & Security*, *30*(8), 719–731. https://doi.org/10.1016/j.cose.2011.08.004

Cyber Security Schedule | Maersk Terms. (n.d.). Retrieved April 28, 2023, from https://vendorterms.maersk.com/cybersecurity

Dang, D., & Vartiainen, T. (2024). Exploring socio-technical gaps in the cybersecurity of energy informatics for sustainability. In E. Ziemba & J. Wątróbski (Eds.), *Adoption of emerging information and communication technology for sustainability* (pp. 288–304). CRC Press.

Dang, D., Vartiainen, T., & Do, T. (2024). Explanation of a sustainable digital transformation process in a firm. In N. H. Thuan, D. Dang-Pham, H.-S. Le, & T. Q. Phan (Eds.), *Information systems research in Vietnam, Volume, 2: A shared vision and new frontiers* (pp. 137–151). Springer Nature. https://doi.org/10.1007/978-981-99-4792-8_10

Eisenhardt, K. M., & Martin, J. A. (2000). Dynamic capabilities: What are they? *Strategic Management Journal*, *21*(10–11), 1105–1121. https://doi.org/10.1002/1097-0266(200010/11)21:10/11<1105::AID-SMJ133>3.0.CO;2-E

Erden, Z., von Krogh, G., & Nonaka, I. (2008). The quality of group tacit knowledge. *Journal of Strategic Information Systems*, *17*(1), 4–18. https://doi.org/10.1016/j.jsis.2008.02.002

Ferdinand, J. (2015). Building organisational cyber resilience: A strategic knowledge-based view of cyber security management. *Journal of Business Continuity & Emergency Planning*, *9*(2), 185–195. https://doi.org/10.69554/PRJY4917

Gärtner, C., & Ribeiro Soriano, D. (2011). Putting new wine into old bottles: Mindfulness as a micro-foundation of dynamic capabilities. *Management Decision*, *49*(2), 253–269. https://doi.org/10.1108/00251741111109142/FULL/PDF

Goel, L., Russell, D., Williamson, S., & Zhang, J. Z. (2023). Information systems security resilience as a dynamic capability. *Journal of Enterprise Information Management*, *36*(4), 906–924. https://doi.org/10.1108/JEIM-07-2022-0228

Gouglidis, A., Green, B., Hutchison, D., Alshawish, A., & de Meer, H. (2018). Surveillance and security: Protecting electricity utilities and other critical infrastructures. *Energy Informatics*, *1*(1), 1–24. https://doi.org/10.1186/s42162-018-0019-1

Greenberg, A. (2018, August 22). *The untold story of NotPetya, the most devastating cyberattack in history | WIRED*. *Wired*. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Gu, M., Yang, L., & Huo, B. (2021). The impact of information technology usage on supply chain resilience and performance: An ambidexterous view. *International Journal of Production Economics*, *232*, 107956. https://doi.org/10.1016/j.ijpe.2020.107956

Haaker, T., Bouwman, H., Janssen, W., & de Reuver, M. (2017). Business model stress testing: A practical approach to test the robustness of a business model. *Futures*, *89*, 14–25. https://doi.org/10.1016/j.futures.2017.04.003

Harrop, W., & Matteson, A. (2013). Cyber resilience: A review of critical national infrastructure and cyber security protection measures applied in the UK and USA. *Journal of Business Continuity & Emergency Planning*, *7*(2), 149–162. https://doi.org/10.69554/NWXJ2946

Hepfer, M., & Lawrence, T. B. (2022). The heterogeneity of organisational resilience: Exploring functional, operational and strategic resilience. *Organisation Theory*, *3*(1), 26317877221074701. https://doi.org/10.1177/26317877221074701

Hern, A. (2017, December 30). WannaCry, Petya, NotPetya: How ransomware hit the big time in 2017. *The Guardian*. http://www.theguardian.com/technology/2017/dec/30/wannacry-petya-notpetya-ransomware

ISO. (2016). *ISO/IEC 27000: 2016-information technology-security techniques-information security management systems-overview and vocabulary*. http://www.iso.org/iso/catalogue_detail?csnumber=66435

Järveläinen, J. (2016). Integrated business continuity planning and information security policy development approach. *Thirty Seventh International Conference on Information Systems* (pp. 1–13). https://aisel.aisnet.org/icis2016/ISSecurity/Presentations/4/

Järveläinen, J., Niemimaa, M., & Zimmer, M.P. (2022). Designing a thrifty approach for SME business continuity: Practices for transparency of the design process. *Journal of the Association for Information Systems*, *23*(6), 1557–1602. https://doi.org/10.17705/1jais.00771

Jiang, Y., Ritchie, B. W., & Verreynne, M. -L. (2021). Developing disaster resilience: A processual and reflective approach. *Tourism Management*, *87*, 104374. https://doi.org/10.1016/j.tourman.2021.104374

Khosrojerdi, F., Gagnon, S., & Valverde, R. (2021). Applications of artificial intelligence in smart grids: Present and future research domains. *2021 IEEE 9th International Conference on Smart Energy Grid Engineering (SEGE)* (pp. 7–12). https://doi.org/10.1109/SEGE52446.2021.9534914

Kostyuk, N., & Zhukov, Y. M. (2017). Invisible digital front: Can cyber attacks shape battlefield events? *The Journal of Conflict Resolution*, *63*(2), 317–347. https://doi.org/10.1177/0022002717737138

Kosutic, D., & Pigni, F. (2021). Cybersecurity: Investing for competitive outcomes. *The Journal of Business Strategy*, *43*(1), 28–36. https://doi.org/10.1108/JBS-06-2020-0116

Kovacevic, A., & Nikolic, D. (2014). Cyber attacks on critical infrastructure: Review and challenges. *Handbook of Research on Digital Crime, Cyberspace Security, and Information Assurance*, 1–18. https://doi.org/10.4018/978-1-4666-6324-4.CH001

Kranz, J. J., Hanelt, A., & Kolbe, L. M. (2016). Understanding the influence of absorptive capacity and ambidexterity on the process of business model change - the case of on-premise and cloud-computing software. *Information Systems Journal*, *26*(5), 477–517. https://doi.org/10.1111/isj.12102

Kumar, J., Mekkanen, M., Karimi, M., & Kauhaniemi, K. (2023). Hardware-in-the-loop testing of a battery energy storage controller for harbour area smart grid: A case study for Vaasa harbour grid. *Energy Reports*, *9*, 447–454. https://doi.org/10.1016/j.egyr.2023.01.068

Labaka, L., Hernantes, J., & Sarriegi, J. M. (2016). A holistic framework for building critical infrastructure resilience. *Technological Forecasting & Social Change*, *103*, 21–33. https://doi.org/10.1016/J.TECHFORE.2015.11.005

Laplante, P., & Amaba, B. (2021). Artificial intelligence in critical infrastructure systems. *Computer*, *54*(10), 14–24. https://doi.org/10.1109/MC.2021.3055892

Lou, X., Tran, C., Tan, R., Yau, D. K. Y., Kalbarczyk, Z. T., Banerjee, A. K., & Ganesh, P. (2020). Assessing and mitigating impact of time delay attack: Case studies for power grid controls. *IEEE Journal on Selected Areas in Communications*, *38*(1), 141–155. https://doi.org/10.1109/JSAC.2019.2951982

Lykou, G., Anagnostopoulou, A., & Gritzalis, D. (2018). Implementing cyber-security measures in airports to improve cyber-resilience. *2018 Global Internet of Things Summit, GioTS 2018*. https://doi.org/10.1109/GIOTS.2018.8534523

Madani, F., & Parast, M. M. (2023). An integrated approach to organisational resilience: A quality perspective. *International Journal of Quality & Reliability Management*, *40*(1), 192–225. https://doi.org/10.1108/IJQRM-07-2020-0229

Maersk Code of Conduct. (n.d.). Retrieved April 26, 2023, from https://www.maersk.com/about/code-of-conduct

Margherita, A., & Heikkilä, M. (2021). Business continuity in the COVID-19 emergency: A framework of actions undertaken by world-leading companies. *Business Horizons*, *64*(5), 683–695. https://doi.org/10.1016/J.BUSHOR.2021.02.020

Measures for a High Common Level of Cybersecurity across the Union NIS 2 Directive, Pub. L. No. 2022/2555, 02022L2555-20221227. (2022). https://eur-lex.europa.eu/eli/dir/2022/2555/2022-12-27/eng

Melnyk, S. A., Closs, D. J., Griffis, S. E., Zobel, W. C., & Macdonald, J. R. (2014, January 1). Understanding supply chain resilience. *Supply Chain Management Review*, *18*(January–February), 34–41.

Mentges, A., Halekotte, L., Schneider, M., Demmer, T., & Lichte, D. (2023). A resilience glossary shaped by context: Reviewing resilience-related terms for critical infrastructures. *International Journal of Disaster Risk Reduction*, *96*, 103893. https://doi.org/10.1016/j.ijdrr.2023.103893

Meydani, A., Shahinzadeh, H., Ramezani, A., Nafisi, H., & Gharehpetian, G. B. (2024). A review and analysis of attack and countermeasure approaches for enhancing smart grid cybersecurity. *2024 28th International Electrical Power Distribution Conference (EPDC)* (pp. 1–19). https://doi.org/10.1109/EPDC62178.2024.10571761

Naseer, H., Maynard, S. B., Ahmad, A., & Shanks, G. (2018, December 13). Cybersecurity risk management using analytics: A dynamic capabilities approach. *ICIS, 2018 : Bridging the Internet of People, Data and Things : Proceedings of the 39th International Conference on Information Systems*. 39th International Conference on Information Systems, San Francisco, California, USA. https://dro.deakin.edu.au/articles/conference_contribution/Cybersecurity_risk_management_using_analytics_A_dynamic_capabilities_approach/27132546/1

Niemimaa, M. (2015). Interdisciplinary review of business continuity from an information systems perspective: Toward an integrative framework. *Communications of the Association for Information Systems*, *37*(1). http://aisel.aisnet.org/cais/vol37/iss1/4

Niemimaa, M. (2016). Entanglement of infrastructures and action: Exploring the material foundations of technicians' work in smart infrastructure context. *Proceedings of the 37th International Conference on Information Systems*, Dublin, Ireland.

Niemimaa, M. (2023). Evaluating compliance for organisational information security and business continuity: Three strata of ventriloqual agency. *Information Technology & People* (ahead-of-print). https://doi.org/10.1108/ITP-03-2022-0156

Niemimaa, M., & Järveläinen, J. (2013). It service continuity: Achieving embeddedness through planning. *2013 Eighth International Conference on Availability, Reliability and Security (ARES)* (pp. 333–340). https://doi.org/10.1109/ARES.2013.45

Niemimaa, M., Järveläinen, J., Heikkilä, M., & Heikkilä, J. (2019). Business continuity of business models: Evaluating the resilience of business models for contingencies. *International Journal of Information Management*, *49*, 208–216. https://doi.org/10.1016/j.ijinfomgt.2019.04.010

NIST. (2020). *Technical guide to information security testing and assessment*. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf

Olan, F., Ogiemwonyi Arakpogun, E., Suklan, J., Nakpodia, F., Damij, N., & Jayawickrama, U. (2022). Artificial intelligence and knowledge sharing: Contributing factors to organisational performance. *Journal of Business Research*, *145*, 605–615. https://doi.org/10.1016/j.jbusres.2022.03.008

Osei-Kyei, R., Tam, V., Ma, M., & Mashiri, F. (2021). Critical review of the threats affecting the building of critical infrastructure resilience. *International Journal of Disaster Risk Reduction*, *60*, 102316. https://doi.org/10.1016/J.IJDRR.2021.102316

Ozkan-Okay, M., Akin, E., Aslan, Ö., Kosunalp, S., Iliev, T., Stoyanov, I., & Beloev, I. (2024). A comprehensive survey: Evaluating the efficiency of artificial intelligence and machine learning techniques on cyber security solutions. *Institute of Electrical and Electronics Engineers Access*, *12*, 12229–12256. https://doi.org/10.1109/ACCESS.2024.3355547

Pursiainen, C. (2018). Critical infrastructure resilience: A Nordic model in the making? *International Journal of Disaster Risk Reduction*, *27*, 632–641. https://doi.org/10.1016/J.IJDRR.2017.08.006

Rajala, R., & Westerlund, M. (2016). Business models – A new perspective on firms' assets and capabilities. *The International Journal of Entrepreneurship and Innovation*, *8*(2), 115–125. https://doi.org/10.5367/000000007780808039

Rathnayaka, B., Siriwardana, C., Robert, D., Amaratunga, D., & Setunge, S. (2022). Improving the resilience of critical infrastructures: Evidence-based insights from a systematic literature review. *International Journal of Disaster Risk Reduction*, *78*, 103123. https://doi.org/10.1016/j.ijdrr.2022.103123

Romero-Faz, D., & Camarero-Orive, A. (2017). Risk assessment of critical infrastructures – New parameters for commercial ports. *International Journal of Critical Infrastructure Protection*, *18*, 50–57. https://doi.org/10.1016/j.ijcip.2017.07.001

Romme, A. G. L., Zollo, M., & Berendsy, P. (2010). Dynamic capabilities, deliberate learning and environmental dynamism: A simulation model. *Industrial and Corporate Change*, *19*(4), 1271–1299. https://doi.org/10.1093/ICC/DTQ031

Sakurai, M., & Kokuryo, J. (2018). Fujisawa sustainable smart town: Panasonic's challenge in building a sustainable society. *Communications of the Association for Information Systems*, *42*, 19. https://doi.org/10.17705/1CAIS.04219

Salovaara, A., Lyytinen, K., & Penttinen, E. (2019). High reliability in digital organizing: Mindlessness, the frame problem, and digital operations. *MIS Quarterly*, *43*(2), 555–578. https://doi.org/10.25300/MISQ/2019/14577

Salvi, A., Spagnoletti, P., & Noori, N. S. (2022). Cyber-resilience of critical cyber infrastructures: Integrating digital twins in the electric power ecosystem. *Computers & Security*, *112*, 102507. https://doi.org/10.1016/j.cose.2021.102507

Sambamurthy, V., Bharadwaj, A., & Grover, V. (2003). Shaping agility through digital options: Reconceptualizing the role of information technology in contemporary firms. *MIS Quarterly*, *27*(2), 237–264. https://doi.org/10.2307/30036530

Sarkar, A., Wingreen, S., & Ascroft, J. (2016). Top management team decision priorities to drive is resilience: Lessons from jade software corporation indicate. *Proceedings of AMCIS 2016. The 22nd Americas Conference on Information Systems*, San Diego, USA.

Sarker, I. H., Janicke, H., Ferrag, M. A., & Abuadbba, A. (2024). Multi-aspect rule-based AI: Methods, taxonomy, challenges and directions towards automation, intelligence and transparent cybersecurity modeling for critical infrastructures. *Internet of Things*, *25*, 101110. https://doi.org/10.1016/j.iot.2024.101110

Shuen, A., Feiler, P. F., & Teece, D. J. (2014). Dynamic capabilities in the upstream oil and gas sector: Managing next generation competition. *Energy Strategy Reviews*, *3*(C), 5–13. https://doi.org/10.1016/J.ESR.2014.05.002

Sinha, R., & Ola, A. (2021). Enhancing business community disaster resilience. A structured literature review of the role of dynamic capabilities. *Continuity & Resilience Review*, *3*(2), 132–148. https://doi.org/10.1108/CRR-03-2021-0009

Sipior, J. C., Bierstaker, J., Borchardt, P., & Ward, B. T. (2018). A ransomware case for use in the classroom. *Communications of the Association for Information Systems*, *43*(1), 598–614. https://doi.org/10.17705/1CAIS.04332

Steininger, D. M., Mikalef, P., Pateli, A., & Ortiz De Guinea, A. (2022). Dynamic capabilities in information systems research: A critical review, synthesis of current knowledge, and recommendations for future research. *Journal of the Association for Information Systems*, *23*(2), 447–490. https://doi.org/10.17705/1jais.00736

Suddaby, R., Coraiola, D., Harvey, C., & Foster, W. (2020). History and the micro-foundations of dynamic capabilities. *Strategic Management Journal*, *41*(3), 530–556. https://doi.org/10.1002/smj.3058

Sutcliffe, K. M. (2011). High reliability organisations (HROs). *Best Practice & Research: Clinical Anaesthesiology*, *25*(2), 133–144. https://doi.org/10.1016/j.bpa.2011.03.001

Tang, R., De Donato, L., Bešinović, N., Flammini, F., Goverde, R. M. P., Lin, Z., Liu, R., Tang, T., Vittorini, V., & Wang, Z. (2022). A literature review of artificial intelligence applications in railway systems. *Transportation Research Part C: Emerging Technologies*, *140*, 103679. https://doi.org/10.1016/j.trc.2022.103679

Teece, D. J. (2012). Next-generation competition: New concepts for understanding how innovation shapes competition and policy in the digital economy. *Journal of Law, Economics and Policy*, *9*(1), 97–118.

Teece, D. J., & Pisano, G. (2003). The dynamic capabilities of firms. *Handbook on Knowledge Management*, 195–213. https://doi.org/10.1007/978-3-540-24748-7_10

Teece, D. J., Pisano, G., & Shuen, A. (1997). Dynamic capabilities and strategic management. *Strategic Management Journal*, *18*(7), 509–533. https://doi.org/10.1002/(SICI)1097-0266(199708)18:7<509:AID-SMJ882>3.0.CO;2-Z

Turoff, M. (1970). The design of a policy delphi. *Technological Forecasting & Social Change*, *2*(2), 149–171. https://doi.org/10.1016/0040-1625(70)90161-7

University of Vaasa. (2023, November 20). *FREESI-Lab*. VBIC Laboratories. https://www.uwasa.fi/en/research/research-platforms/vebic/vebic-laboratories

Vakilzadeh, K., & Haase, A. (2021). The building blocks of organisational resilience: A review of the empirical literature. *Continuity & Resilience Review*, *3*(1), 1–21. https://doi.org/10.1108/CRR-04-2020-0002

van der Merwe, S. E., Biggs, R., & Preiser, R. (2018). A framework for conceptualizing and assessing the resilience of essential services produced by socio-technical systems. *Ecology and Society*, *23* (2). https://doi.org/10.5751/ES-09623-230212

Venkatachary, S. K., Prasad, J., & Samikannu, R. (2018). Cybersecurity and cyber terrorism-in energy sector – A review. *Journal of Cyber Security Technology*, *2*(3–4), 111–130. https://doi.org/10.1080/23742917.2018.1518057

Vogus, T. J., & Sutcliffe, K. M. (2017). Commentary on mindfulness in action: Discovering how US navy SEALs build capacity for mindfulness in high-reliability organisations (HROs). *Academy of Management Discoveries*, *3*(3), 324–326. https://doi.org/10.5465/amd.2017.0047

Weick, K.E., Sutcliffe, K.M., & Obstfeld, D. (1999). Organising for high reliability: Processes of collective mindfulness. In R. S. Sutton & B. M. Staw (Eds.), *Research in organisational behavior* (Vol. 3, Issue 1, pp. 81–123). JAI Press.

Wells, E. M., Boden, M., Tseytlin, I., & Linkov, I. (2022). Modeling critical infrastructure resilience under compounding threats: A systematic literature review. *Progress in Disaster Science*, *15*, 100244. https://doi.org/10.1016/j.pdisas.2022.100244

Wesley, D. T. A., Dau, L. A., & Roth, A. (2019). *Cyberattack: The Maersk global supply-chain meltdown*. *Harvard Business Publishing Education Case*. https://hbsp.harvard.edu/product/W19132-PDF-ENG?activeTab=include-materials&itemFindingMethod=

Wessel, L., Baiyere, A., Ologeanu-Taddei, R., Cha, J., & Jensen, T. B. (2021). Unpacking the difference between digital transformation and it-enabled organisational transformation. *Journal of the Association for Information Systems*, *22*(1), 102–129. https://doi.org/10.17705/1JAIS.00655

Yu, W., Jacobs, M. A., Chavez, R., & Yang, J. (2019). Dynamism, disruption orientation, and resilience in the supply chain and the impacts on financial performance: A dynamic capabilities perspective. *International Journal of Production Economics*, *218*, 352–362. https://doi.org/10.1016/j.ijpe.2019.07.013

Zio, E. (2016). Challenges in the vulnerability and risk analysis of critical infrastructures. *Reliability Engineering and System Safety*, *152*, 137–150. https://doi.org/10.1016/J.RESS.2016.02.009

Zsidisin, G. A., Melnyk, S. A., & Ragatz, G. L. (2005). An institutional theory perspective of business continuity planning for purchasing and supply management. *International Journal of Production Research*, *43*(16), 3401–3420. https://doi.org/10.1080/00207540500095613