Vision for Emergency Management: Conceptualizing Mission-Critical Ecosystems

Jaziar Radianti
Centre for Integrated Emergency Management
University of Agder, Norway
jaziar.radianti@uia.no

ABSTRACT

Emergency management is seldom viewed through the lens of enterprises/industries, which aim to safeguard their critical missions to deliver seamless services. This article advocates for an integrative perspective on mission-critical (eco)systems. In the digital transformation landscape, the traditional notions of "mission-critical systems," often associated with physical spaces like control facilities or hardware-software crucial for business operations, are challenged. Based on document reviews, this article argues for a holistic comprehension of an organization's mission-critical ecosystems, considering internal and external factors across physical, digital, and human aspects. The article uses renewable energy and e-health as cases. The overarching goal is to expand the research scope in emergency management by examining current concerns and current trends in emergency management domain, combining preparedness, resilience, and cybersecurity. This comprehensive approach aims to enhance our ability to navigate and respond effectively to emergencies in an increasingly complex and interconnected world.

Keywords

Mission-critical ecosystems, digital resilience, risks, cybersecurity

INTRODUCTION

Numerous studies in the emergency management domain often focus on cooperation, coordination, and collaboration among public responder agencies to save lives and protect properties. However, many organizations including private companies and industries are also vulnerable to physical and digital threats and often dependent on external actors to conduct their operations. Business entities in society play critical roles as pillars for economic resilience. Some businesses are essential in running critical services such as companies involved in supplying energy, health, and care services. In operating the businesses, there are always specific entities of private or public organizations encompass persons, information systems, and digital infrastructures that are critical, and should continuously be protected to avoid operational disruptions, i.e., mission critical functions. The sources of interruptions to mission-critical functions can originate from either inadvertently or advertently made disasters. The impacts can be harmful, ranging from the loss of reputation, trust, monetary assets to the loss of human lives. These critical units, internal infrastructure, actors, or services in this article are referred to as "mission-critical ecosystems."

Rooted from the ecology science (Mars et al., 2012), the concept of ecosystems itself has been metaphorically applied across various scientific areas (Pickett & Cadenasso, 2002), including organizational ecosystems and management (Mars et al., 2012; Pavlikakis & Tsihrintzis, 2000), or even digital ecosystem metaphor (Krivý, 2023) that can cover the whole planet. Scholars acknowledge the complexity of ecosystem concept, which is subjected to continuous change in space and time, characterized by interconnectedness, dynamics, and scales—at which ecosystem processes operate, with human playing a significant role (Pavlikakis & Tsihrintzis, 2000). Boundaries of ecosystems exist but they may be defined arbitrarily because of spatial and temporal changes of the ecosystem. The open and dynamic character of the ecosystems does not support rigid guidelines for boundary delineation

(Pavlikakis & Tsihrintzis, 2000). In this article, mission critical ecosystems (MCEs) are defined as an integration, and interconnectedness between the critical *internal arrangement* of organizations (actors, knowledge, digital platforms, critical facilities, supply chain) with *external stressors* that pressing organizations to adapt, respond or change to fulfill their goals (e.g., protect essential service functions or core businesses) which sometimes require interactions with external stakeholders. Thus, critical infrastructure can be one of the components of mission critical ecosystems, while critical services can mean the core businesses of industries fall within societal critical functions or they can mean any critical functions in organizations that vital for seamless business operations.

Indeed, there are substantial body of literature on business continuity management (BCM) and continuity of operations (COOP) planning (Cerullo & Cerullo, 2004) which addresses the maintenance of an organization's mission-critical functions during disruptions to critical infrastructure caused by various physical, cyber, public health and other hazards. This focus is also a part of governmental emergency management efforts as evidenced by publications from the US Federal Emergency Management Agency - FEMA (2018; 2020) and Cybersecurity and Infrastructure Security Agency - CISA (2024), which tackle both physical and cyber threats. Notably, as a managerial function concerned with coordinating "whole community" efforts, emergency management in these publications underscore the necessity of involving industry and community organizations in mitigation and preparedness activities to uphold essential services during crises.

COOP literature offers practical guidelines to cope with the disturbances, but they do not fully address what counted as MCEs. Moreover, MCEs are becoming blurry with recent digital transformations when industries gradually rely heavily on internet of things, cyber-physical (social) systems, internet of service and smart factory. Reliance on "interconnectedness" between devices, applications, sectors, information/ digital/ physical infrastructures are a key in the so-called industry 4.0 premise. Moreover, such "smart arrangement" often requires elevated needs of hardware, software, and services to make mission-critical infrastructure to function in a more efficient manner through outsourcing to the third parties, and sometimes go beyond the national boundaries. Thus, physical, digital, and service supply chain are unavoidably a part of the MCEs. Todays´ ubiquitous connectivity, the use of Internet of things and cloud services, digitalization of critical infrastructure including health services, and other digital trends, have triggered the needs for understanding such landscape from the organizational viewpoints, and the idea of the digital disasters (Hansen & Nissenbaum, 2009; Van der Meulen, 2013) and digital resilience (Boh et al., 2023; Magutshwa & Radianti, 2022).

Digital resilience often includes building resilience of entities that are vulnerable to cyberthreats including human, technologies, and digital infrastructures. Thus, cybersecurity aspects are inseparable from societal security. The Covid-19 pandemic can be considered as a health disaster, that further triggers emergency management, and the need for understanding cybersecurity better, because solution services are delivered digitally (Magutshwa, 2022; Magutshwa & Radianti, 2022). Another example, many countries such as Norway are in the energy transition from usage of fossil-based energy fuel to renewable energy and battery technology. There have been intensive political and scientific discussions for building more energy sources such as offshore and onshore wind power (Dahl et al., 2022), moving toward battery sources for ground, air, and sea transports (Figenbaum, 2023; Schulz & Rode, 2022; Thorne, Hovi, et al., 2021; Veisten et al., 2024).

The significant shift in Europe, particularly in Norway, aims to prepare for future scenarios with limited fossil fuels by exploring new forms of renewable energy beyond hydroelectric power (Skjærseth & Rosendal, 2023), as one of the oldest and largest sources of renewable energy. While various renewable energy sources exist (solar, geothermal, and bioenergy), Norway leans towards among other things offshore and onshore wind power, aligning with higher prominence in the political agenda (NOU, 2023a). Additionally, battery power emerges as a pivotal energy storage, especially with the increasing adoption of electric vehicles in Norway. For instance, in 2023, 83.4% of new cars sold in the country were electric (source: www.elbil.no), equipped with 40-50 kilowatt-hours (kWh) batteries (Innovasjon-Norge, 2023). City buses as critical transport infrastructures are gradually adopting batteries with an average capacity of 125 kWh.

The infrastructures controlling these new sources of renewable energy are also changed, and more digitalized. From a societal perspective, companies provide critical services facing unknown risks, challenges, societal conflicts, and potential disasters, including digital disasters, which require new understanding of emergency management. Again, the MCE is a way to entangle interrelated aspects of future emergency management involving new digital-related challenges and digital disasters.

Moreover, the increasing use of digital health services, as evidenced in the e-health case example (Helsedirektoratet, 2023), will require a robust communication infrastructure. This transformation undoubtedly elevates the demand for a more seamless electricity supply (Thorne, Aguilar Lopez, et al., 2021). This change is intricately linked to the current green ambitions in Europe towards achieving net-zero emissions. This overarching

goal is encapsulated in the vision to "Make Europe the first climate-neutral continent by 2050" (EU-Commission, 2023).

This paper argues on the need of moving our understanding from mission-critical *environment* and *systems* to *mission-critical ecosystems*. In the industrial context, numerous layers of entities, units, and environments interact to influence MCEs, which are essential for delivering sustainable services. I propose the following research questions:

- RQ1 How to define a framework for studying mission critical ecosystems?
- RQ2 How to apply the mission critical ecosystem framework to derive emerging issues within critical services?

We need to gain better understanding of what are counted as MCEs. This paper aims at contributing to research agendas to define and expand the idea of MCE as one of potential future direction for emergency management research. The cases and examples were taken from European setting especially Norwegian example, with two selected critical services, i.e., the e-health service and energy sectors.

This paper´s contributions are threefold. *First*, it proposes a definition of the MCE concept that guides this study to find the research gaps in existing literature related to business continuity/ emergency management. *Second*, the MCE concept is essentially examining the wider set of components not only infrastructural interdependency, but also issues such as green shift, new emergency management knowledge and competencies due to changing threat landscape. Current approaches to business continuity/emergency management planning and preparedness efforts are likely to overlook these dependencies, rendering essential services vulnerable during crises. *Third*, the paper proposes an integrated framework i.e., MCEs and applies to examine strategic documents to identify future new challenges that are worth research.

LITERATURE REVIEW

In this section two interrelated concepts are elaborated based on the literature review, i.e., mission critical systems and business continuity planning. Finally, the section summarizes research gaps and highlights this paper's position.

Mission-Critical Systems in the Literature

The complexities described earlier trigger the need to build a new understanding of "mission-critical (eco)systems" that are now becoming blurry. Traditionally, mission-critical systems are often associated with the critical physical infrastructure and facilities, and often are associated with the 24/7 environments such as operation centers, network equipment rooms, standby emergency power, business continuity and technology recovery room, business operation control room, command center—to name few (Curtis, 2021; Hebert et al., 2018). There are many specific rooms and areas within facilities in today's ever-changing environment. In this book, Curtis (2021), defines the Critical Environment (CE) as the "*physical space and the systems within a facility that are uniquely configured, sized and dedicated to supporting specific critical business operations as defined by the user*". Before 2010, mission-critical systems often were associated with Mission-critical Computer Resources (MCCR) such as hardware/software/firmware (Austin & Larkey, 1992) and critical servers (Johnson, 1999).

Table 1 summarizes various definitions used in the literature, to broaden our understanding, how the concept has been applied in contexts beyond "critical facilities" and "critical systems."

Table 1 Overview of the mission critical concepts derived from literature.

Main Concepts	Definition
Systems or Process (Bernardini et al., 2013; Magutshwa & Radianti, 2021; Weger et al., 2023)	**A system or process** is one in which a failure or interruption comes with intolerable operational or human cost. The system is **essential to the survival of an organization** and **will adversely affect society when it fails.**
Systems health state; socio-technical interaction (Bernardini et al., 2013)	A 'mission-critical system' is a system whose '**health state**' is crucial to the successful completion of an organization's core operations. Many mission-critical systems can be characterized as **complex socio-technical systems**, that depend on the interactions among human and social factors and technical infrastructures.
Criticality scale (Microsoft, 2023), *Approaches, and methods* (LeSaint et al., 2015)	**A criticality scale** that covers significant financial cost (business-critical) or human cost (safety-critical) **associated with unavailability or underperformance**. As an approach, it refers to methods for assessing vulnerability in mission-critical systems.

Table 2 Overview of the mission critical concepts derived from literature.

Main Concepts	Definition
Function or Critical Services (Zuo, 2013)	**A function whose failure would lead to catastrophic consequences** that would place public security at risk. Mission-critical systems provide **vital services and must be reliable and dependable** to withstand malicious attacks and system failures (e.g., the electric power grid, telecommunications networks, healthcare systems, water management systems), hardware and software failures, operator errors, power outages, environmental disasters, and attacks by adversaries
Hardware, software, applications, communication facility, IoT (Ali & Ware, 2021; Austin & Larkey, 1992; Cao et al., 2021; Johnson, 1999; Weger et al., 2023)	**The hardware, software, and communication facilities**, that allow mission-critical users to communicate with each-other and liaise with command centres securely for providing mission-critical services, wherever and whenever the services are needed. It includes applications that critical, e.g. to support Internet of Things (IoT) that essential for autonomous driving, factory automation and tele-surgery.
Business Ecosystems (Mattos et al., 2020)	**Continuous process in a business-to-business (B2B**) mission-critical systems: customer and users can be different customer can subscribe for their users, or they become users in itself; Ownership products and data issues
Leadership (Yip et al., 2009)	**Leadership as a mission-critical:** Horizontal and vertical boundaries, requirements for groups to work across boundaries. Traditionally, managers learn to manage vertically — to work with senior colleagues and downward with direct reports. In today's interconnected world, it is critical for managers to work effectively across functions, locations, and with external stakeholders
Innovations in public agencies (Breznitz et al., 2018)	**Enhancing innovations**: mission-critical systems have been linked into the need for tools and structure of successful innovation agencies to be one of the following organizational typologies: upgrader, productivity facilitator, state disruptors, transformation enabler
Organizational capacity (Hannah et al., 2009)	One or more extreme events are occurring or are likely to occur that may **exceed the organization's capacity** to prevent and result in an extensive and intolerable magnitude of physical, psychological, or material consequences to – or in close physical or psycho-social proximity – to organization.

The usage of the "mission-critical" concept in Table 1 shows the varieties of this concept applications, which are then aggregated to define the component of MCEs. The learning points from this review are:

- "Mission-critical" (systems, processes) are often treated as a singular topic, either specifically discussing the concept within a particular application area or in a very general sense to refer to important activities.
- The term refers to both the technical development of mission-critical software, apps, and communication, and to the critical spaces, or facilities.
- In the organizational context, the term is often associated with risks, the sustainability of business operations, structure, leadership, and the organizational capacity to cope with stress. Frequently, the term is related to the concept of "cascading effects" resulting from the failure of one critical service, impacting other sectors and business units.

Literature on Business Continuity Planning (BCP)

A related perspective in the literature that addresses the maintenance of business operations is CP framework. BCP entails preplanning disruptive events (Reid, 2021), establishing a plan to counter mitigate risks and minimize the impact of a crisis while reducing the time needed to restore conditions to normal operations (Cerullo & Cerullo, 2004). The aim of BCP is to prepare for, provide to, and maintain control and capabilities for managing an organization's overall ability to prevent operational discontinuity during disruption (Mukherjee et al., 2020).

Reid (2021) points out that BCP is analogous to Continuity of Operations Planning (COOP), with the distinction that BCP is often applicable for private sectors, while COOP typically refers to continuity of government or public sectors, which has been accepted as a part of the emergency preparedness landscape since 1955 in the US (Rucks et al., 2011), and continuously updated (FEMA, 2020). Rucks et al. (2011) that suggest templates developed for emergency management agencies during planning stages and their utility during activations or response phases. FEMA also provides practical examples of templates for continuity plans (FEMA, 2020). Thus, BCP is often manifested as a playbook designated to guide response in the event of disruptions. Specifically, COOP illuminates the efforts within individual organizations to ensure that essential functions continue during disruption of normal operations (FEMA, 2018, 2021). Typical instruments to identify critical functions include conducting Business

Impact Analysis (BIA), assessing associated risks, and formulating mitigation plans (Cerullo & Cerullo, 2004; FEMA, 2019) as well as creating Disaster Contingency Recovery Plan (DCRP) to outline procedures to follow when a disaster occurs (Cerullo & Cerullo, 2004).

Inspired by Covid-19 crisis, Grace et al. (2023) introduce continuity planning for cyber-physical infrastructure to maintain essential functions at existing or alternative workplaces thorough the crisis. The article discusses the interdependence of cyber-physical-social infrastructure in continuity planning for public health emergencies and suggests the need to expand business process/impact analysis to recognize dependencies and impacts on critical infrastructure that occur when other organizations' essential functions are impacted. Grace et al. (2023) particularly highlight the need for multiple-level redundancies to maintain continuity of operations and achieve organizational resilience.

Summary and Research Gaps

In the business and industrial context, highlighting the urgency of emergency management is clearer when using concepts like BCP or "mission-critical ecosystems," as any threats to digital and physical infrastructure, critical functions, or lacking critical teams and leadership are immediately recognized as crises requiring response. Existing studies, however, appear to focus on a limited set of infrastructures and not the expansive set of inter-organizational infrastructure components—ecosystems—that organizations depend on to maintain operations during a crisis. One of the gaps in the BCP framework is its inadequateness in addressing emerging risks such as new cyberthreats, climate change impacts and zero emission requirements assigned to organizations. This includes considerations such as prioritizing human centric approaches over reliance on automation, integrating climate risk management for sustainability, and incorporating social dynamics, as suggested by Industry 5.0.

Moreover, there is a gap where the mission-critical (eco)systems are not portrayed holistically, by considering all the ecosystems, and allowing the organizations to assess their weaknesses in a more thorough way. This article proposes that "Mission critical ecosystems encompass core technologies, physical infrastructures, the individuals, and teams who interact with the technologies, organizational and supply-chain environments that support critical (business) operations. A failure in one or more of these factors within this ecosystem can result in undesirable cascading risks and consequences for both business and society."

METHODOLOGY

Approach: Multi-Vocal Literature Review (MLR) Approach

This study is designed as qualitative research involves exploring research questions through collecting and analysing data using typical qualitative data collection methods. The study employed ***multi-vocal literature review (MLR) approach,*** especially because we want to include overarching themes laid down by strategic documents related to selected cases (e-health and energy). "MLR comprises all accessible writings on a common, often contemporary topic. The writings embody the views or voices of diverse sets of authors (academics, practitioners, journalists, policy canters, independent research and development firms, and others).

They reflect different purposes, perspectives, and information bases. They address various aspects of the topic and incorporate different research or non-research logics" (Garousi et al., 2019, p. 102).

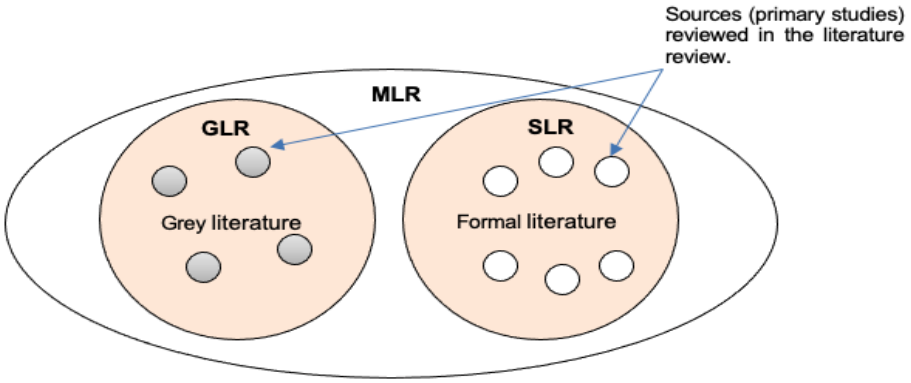

Figure 1 Venn diagram showing the relationship of SLR, GLR and MLR studies (Adapted from Garousi et al, 2019).

Data Collection Method from Academic and Grey Literature

This study uses documents as the main data sources, which then be coded and analysed to find patterns and themes, i.e. scientific literature, and grey literature (GL). The usage of grey literature in research have been discussed by scholars. The 1997 Luxembourg Convention defines the term as "*literature that is produced on all levels of government, academics, business, and industry in print and electronic formats, but which is not controlled by commercial publishers i.e., where publishing is not the primary activity of the producing body*" (Garousi et al., 2019; Kamei et al., 2021). Such literature is not obtainable through traditional publishing channels that typically require peer-review processes prior to publication to control publishable materials. Garousi et al. (2019) suggest three levels of GL. **The first tier** encompasses books, magazines, government reports and white papers with high outlet controls and high credibility such as reports, books, magazines government reports and white papers. **The second tier** has moderate outlet control and credibility such as annual reports, news articles, presentations, videos, question-answer sites, Wiki articles and so on. **The third tier** encompasses e.g., blogs, emails and tweets as low outlet control and credibility. Scholars argues on the importance of GL as it has the potential to understand the contextual contemporary information and provides valuable insights for research in fields where there are still received limited scholarly attention (Garousi et al., 2019).

The overall procedures conducted in this study is captured in Figure 2. In this study, scientific literature was used to map the components of "mission-critical (eco)systems". The search term "mission-critical" were applied in Scopus database and Google Scholar. Highly technical-oriented papers were filtered out. The selection focused on articles that tailor mission-critical term with organizational context. This procedure help deriving the mission critical ecosystem framework that integrates its component into a single framework (Figure 3). On the GL part, this study benefited from the government strategic documents publicly accessible, published between 2019-2023 by Norwegian Government or agencies that touch upon energy sectors, emergency preparedness, health preparedness and the green shift. Using the framework derived from the literature in Figure 3, I extracted emerging themes from the identified government reports that serves as vision for emergency management.

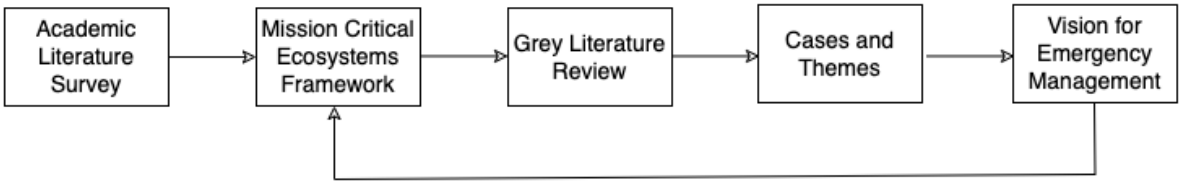

Figure 2 Procedure for deriving vision for emergency management

Data Analysis Method

The documents were coded thematically using a qualitative software Nvivo with simple criteria: renewable energy and health and societal security topics. However, whenever a new concept comes, it was treated as a new sub-theme during the analysis, which then was mapped into the broader theme. This framework was then used to map the government documents and strategies that dealing with more concrete e-Health and energy cases and to derive visions for future emergency management.

RESULTS

Figure 3 depicts a simplified MCEs framework derived from scientific literature, which subsequently utilized to map emerging themes within selected application areas and beyond. Figure 3(A) lists sources of instability both internally (on the right side) and externally (on the left side). The core circle captures various necessary applications, software, hardware, and various technologies and digital infrastructures needed to sustain the organizational operations. The second inner circle represents the "space", where these supporting technologies reside, while the third inner circle (mission-critical users) comprises the core teams and human resources interacting with the technologies, ensuring seamless operation of the organizations. The fourth inner circle represents the criticality of organizational layer where the leadership, organizational cultures (safety, security, and risk cultures). The outermost circle portrays the supply-chain of goods (e.g., raw materials, equipment, critical components of industries), services (consultancies, software as a service, expertise for hire), and digital supply chain (e.g., digital technologies, data analytics, predictive analytics, Internet of things (IoT)-based services). While in Figure 3A the whole landscape of the MCEs seems disjointed, in reality there are dependencies among these factors as has been simplified in Figure 3B.

Externally (left side of Figure 3), there are known and unknown factors that affect businesses´ resilience such as:

- extreme events (e.g., snowstorm, floods, terrorist actions, landslide, pandemic)
- risks, threats and cyberthreats (e.g., black-swan events, cyberattacks, cybercrime and extortion)
- new demands for customers (e.g., preferences, desired services, sophistication levels, platforms)
- contemporary trends (e.g., industry 4.0, industry 5.0, sustainability, green deals demand, new competencies)
- new national and international strategies (e.g., stronger privacy laws, new highlights in governments´ regulations, artificial intelligence act, and so on)

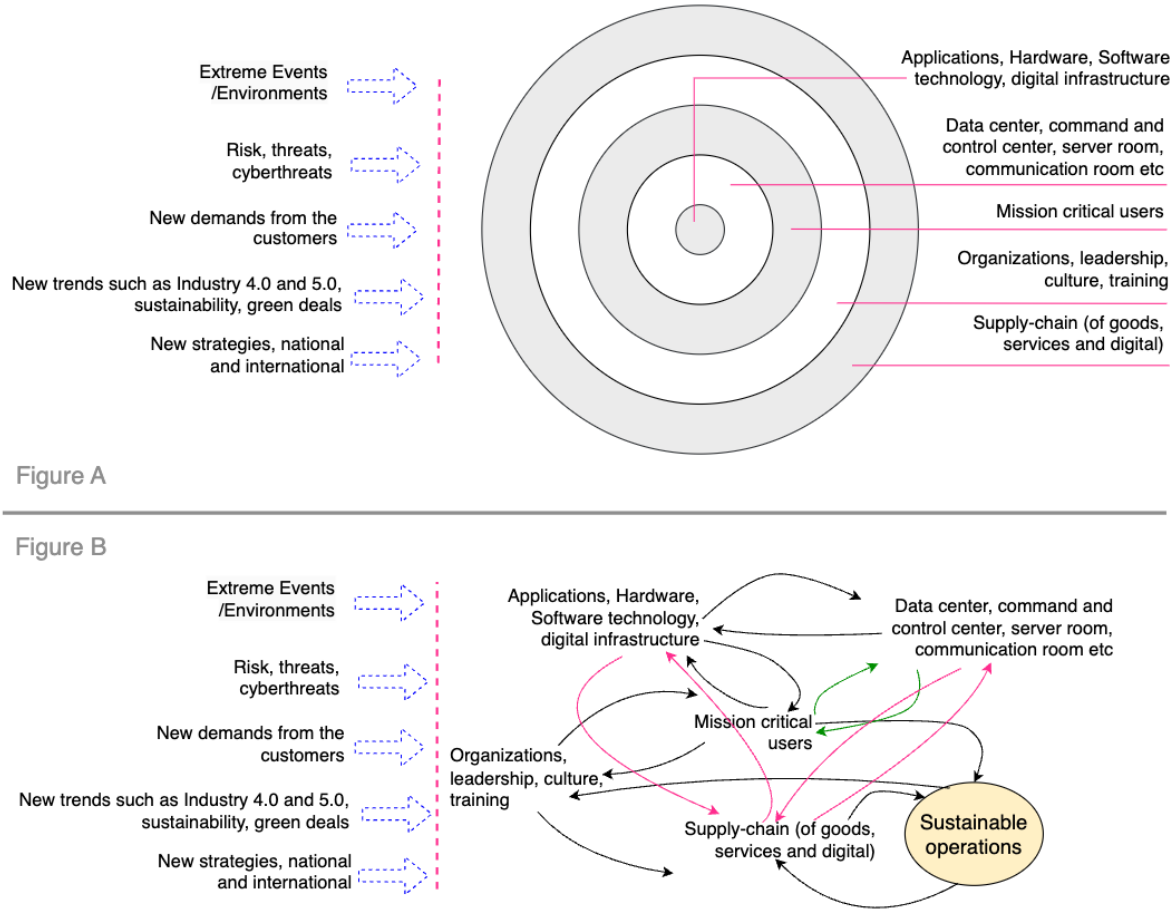

Figure 3 A Framework to untangle the mission-critical ecosystems.

We applied this MCEs as thematic analysis framework into two selected cases, i.e., challenges in renewable energy and e-health sectors that affect societal security. The following trends are identified and reemphasized:

Applying the MCE Framework for the e-Health Case

As our focus is to identify the e-health themes, the following issues within the MCEs framework were identified:

- **Digital and critical infrastructure**: Themes such as digital infrastructure, information security, managing security breaches, secure communication, security-privacy consequences, risk assessment and management, and secure IT operation with access control have repeatedly emphasized (DEH, 2023; Meld.St.5, 2023; NORMEN, 2018, 2022a, 2022b, 2023). The ICT solution is a backbone of the eHealth service. Organizations should capable of assessing the risks and consequences regarding the unavailability of the service (NORMEN, 2021).
- **Facility:** The inclusion of e-health initiatives in health preparedness aims to enhance monitoring, detection, and analysis of e-health digital threats and vulnerabilities, the relevance of Computer Emergency Response Teams (CERTs), and required facilities for conducting these activities (Meld.St.5, 2023).
- **Critical users:** There are lacking competence and knowledge in some sectors including basic research in the development of pharmaceutical, diagnostics and vaccines, medical technical equipment, and digital health.

The health sector should be prepared against crisis and catastrophes (*Veikart Helsenæringen*, 2023), and ICT security competence to understand threats and risk control (Meld.St.5, 2023).

- **Organization, leadership, and culture:** The themes touch upon the issues of strengthening system for health preparedness, resilient health preparedness, and understanding of risk and vulnerability. Health organizations should cooperate on societal security based on systematic risk management. Prevention and preparedness must be prioritized (Meld.St.5, 2023). In eHealth, the organizations should comply with the requirements for information security (NORMEN, 2022a).
- **Supply chain**: Sometimes health organizations act as data controller by collecting health data, which may be processed further by the third-party data processors on behalf of the data controller. Data controller organizations sometimes act both as data controller and data processor. In other instances, suppliers come as data processors in the cloud services or operational services, maintenance (physical service) and remote access, or even outsourcing the ICT functions. These suppliers should adhere to the existing requirements to avoid potential data breaches (NORMEN, 2022a)
- **External issues:** Examples of themes include feared threats and risk scenarios involving digital infrastructure in e-health including human errors, accidents, technical failures, and extreme weather are highlighted. The risks are annually assessed by relevant national agencies such as policy security service, intelligence services, national security authority and Health-CERTs. Relevant risks, threats and vulnerabilities that will harm the availability, confidentiality and integrity of personal information should be understood (NORMEN, 2022b). There are also concerns on software dependency, dependencies related to the supply chain and digital infrastructure, as well as the development of artificial intelligence, and its consequences (Meld.St.5, 2023).

Applying the MCE Framework for Power Sector Scenario: "New" Renewable Energy and Battery

The themes derived from energy case are coded and aligned the MCEs framework, for instance, automation and digitalization, which significantly contribute to increased power consumption (Motvind-Norge, 2019), alongside the electrification of the transport systems. The following themes were identified:

- **Technology and digital and critical infrastructure**: The energy storage system such as battery is a key for keeping excessive energy production originated from use of renewable energy such as wind power (Motvind-Norge, 2019). Such energy source development has changed the risk picture from the societal security perspective (NOU, 2023b). The energy white-paper document (NOU, 2023a) indicates the emergency management work should include the understanding of the new incident risks caused by such power sources and how to manage them (NOU, 2023b).
- **Facility:** Many energy companies active promoting the energy-intensive data center and the energy usage will increase, thus this development is a part of the calculated future energy needs (NOU, 2023a)
- **Critical users**: The theme stresses the shortage of personnel with practical risk management skills, hindering the effective implementation of risk analysis and measures in practice (Johnsen & Lysgaard, 2022). This knowledge gap can impede the procurement of ICT systems, particularly in assessing their security risks. There is a pressing need for clearer roles for policymakers and other stakeholders to enhance the resilience of critical infrastructure and systems (NOU, 2023a)
- **Organization, leadership, and culture**: the themes point out the need for a better coordination and cooperation among relevant organizations such as Power supply Emergency Preparedness Organizations (KBO). Culture for sharing information is also need improvement (NOU, 2023a, 2023b).
- **Physical and digital supply chain:** the transition to e.g., wind power or battery, triggers higher demand for raw materials, minerals, and metals. Thus, industries are more dependent on a number of goods such as aluminum, cobalt, copper, steel, zinc and lithium (Motvind-Norge, 2019). The supply chain also involves complex arrangement of suppliers involved in infrastructure construction. The digital supply chain receives high attention due to its role as a gateway for cyberattacks, with statistics indicating a rising trend in attacks among suppliers, leading to digital disasters. It encompasses the delivery structure between businesses, involving digital services, software, or hardware in each delivery (DSB, 2020). Thus, ICT security risk management of the supply chain is especially important in many sectors, especially energy (Johnsen & Lysgaard, 2022). Understanding the supply chain is becoming relevant and crucial to safeguard mission-critical core of the business.
- **External issues**: There is high fluctuation of electricity supply from "new" energy such as wind power. In certain European countries, dual wind power sources, offshore and onshore, are common, but they present challenges such as construction and funding. The potential of onshore energy for power balance is recognized, yet barriers have caused delays, due to environmental concerns and local conflicts, such as community acceptance of onshore wind facilities. Harsh environments can heighten the risk of infrastructure damage

(NOU, 2023a). Likewise, on the offshore part, the risks of marine ecosystem damage and other ocean-related interests can be affected negatively. These are an example as well how the mission-critical business core can affect societal security, especially with the societal conflict risks, and vulnerable physical infrastructure.

Societal Security and Cybersecurity in relation to eHealth and Energy Scenario

A strategic document called "Risk 2023" advices businesses to have better visions on security work in a larger context, and take measures to protect themselves against espionage, sabotage, terror, and complex threats (NSM, 2023). Kvadsheim et al. (2023) pinpoint that the security quality is closely connected the preparedness. Energy-related organizations need to establish preparedness plan (how to respond), structure (role and responsibilities), training (to test if the preparedness plan works), evaluation and learning. The Norwegian *Total-preparedness* strategy justifies the preparedness and management in energy supply and recommends measures to handle unwanted threats (NOU, 2023a), including digital security and preparedness for digital response (NOU, 2023b).

The *total-preparedness* strategy covers also health preparedness, aimed at safeguarding lives and well-being by ensuring continual provision of medical treatment, nursing, and care for individuals affected by crises, including major natural disasters, terrorist attacks, war, and pandemics and typically causing death or severely injured victims (NOU, 2023b). This health preparedness highlights the importance of services in emergency medicine, emergency room, municipal health service and specialist health services. Swine-flu pandemic 2009 and Covid-19 pandemic are examples of the importance of good infection controls as public health measure. Overall, the *total-preparedness* strategy underlines improved risk analysis and management for better health preparedness, including the protection of critical infrastructure to maintain seamless electronic communication services in crisis events. Battery has been mentioned as an important energy storage, to back up the energy sources for critical infrastructure during the power outage.

DISCUSSIONS AND REFLECTIONS

The identified trends or issues highlighted in the previous sections indicate that organizations are often vulnerable, facing both new and interrelated threats that may go unnoticed without a comprehensive analysis of the overall ecosystems. The listed trends in the previous section, derived mainly from the Norwegian experience, specifically in e-health and energy sectors, may not align with other countries' experiences. For example, differences in the adoption of electric cars, levels of digitalization for critical infrastructure systems, reliance on electricity in daily life, and dependence on renewable energy sources vary among nations. In fact, Norwegians build their preparedness system based on trust, a societal value that highly appreciated in their society, may not be applicable to countries with more fragmented social structures and higher level of distrust. However, certain general topics consistently emerge, and generally applicable in building emergency management:

- The strategic documents emphasize the significance of ***the preparedness stage*** in emergency management. A well-crafted preparedness plan, outlining response procedures, organizational structure, role delineation, training protocols, and continuous evaluation, is crucial for an effective crisis response. Systematic research on building excellent preparedness plans across diverse and emerging scenarios could be a relevant research agenda.
- The ability to conduct thorough ***risk assessments*** is pivotal in creating realistic preparedness plans that account for new threats and are regularly updated. Research on risk analysis, risk perceptions, systemic risks analysis, intertwined risks, and cascading risks within the emergency management and response domain could contribute significantly to the field.
- Examining ***organizational ecosystems*** is crucial in establishing emergency plans and conducting risk analyses. The proposed mission-critical framework, focusing on each component or layer, aids in understanding threats and defining preparedness plans.
- ***Digital transformation*** is inevitable in various sectors, including emergency management. However, limited studies exist on digitalization within this domain, including potential "digital disasters." Research on the implications of digital disasters and their relevance to emergency management is needed.
- The increasing connection between ***cybersecurity and emergency management*** is noteworthy. Understanding digital risks, security, and privacy protection becomes integral to post-digital transformation. Research should explore events that resemble cybersecurity incidents but trigger emergency management responses, such as a cyberattack on a transport control system causing citywide traffic chaos.
- Resources with skills in risk analysis, cybersecurity, and ICT supply chain security are limited. Research on ***human resources in the digitalization era*** within emergency management, focusing on capabilities, competencies, and training ideas to address gaps, is essential.

To sum up, this study provides valuable lessons that can guide efforts to derive new research areas in the emergency management domain that put business and industries into the picture, particularly when examining individual scenarios like those are relevant for the e-health and energy as critical services. Moreover, to repeat that we have proposed the definition MCEs as an integration, and interconnectedness between the critical *internal arrangement* of organizations (actors, knowledge, digital platforms, critical facilities, supply chain) with *external stressors* that pressing organizations to adapt, respond or change to fulfill their goals (e.g., protect essential service functions, core businesses) which sometimes require interactions with external stakeholders. By applying this framework during the analysis stage, several pressing issues on each category of component in mission critical ecosystems have been identified. The implication for research among other things is how to identify detailed components of mission critical ecosystems, and how to detail the green transition within industrial mission critical ecosystems. There is a newer model in the BCP literature such as Eco-centric BCP that build on four pillars: 1) reduction in emission from industry; 2) sustainable use and reuse of ecosystem services; 3) legislation-and implementation, and 4) sustainable energy usage and consumption. In the Eco-centric BCP Model, environmental aspects are highly dominant and translated as e.g., environmental norms, waste production and reduction, emission treatment, certification for sustainable indexing, circular economy, and emission management. This can be explored as further study encompassing their relevance for mission critical ecosystems, and how organizations move forward with the eco-centric BCP (Mukherjee et al., 2020).

CONCLUSION AND FUTURE WORK

This article argues for the necessity of adopting a less siloed approach to emergency management. As technology plays an increasingly integral role in emergency response, the distinction between emergency management and cybersecurity becomes more challenging. Various technologies are now utilized in emergency response activities, encompassing tasks such as data collection, exchange, and storage. The proposed mission-critical framework serves to map and comprehend the emergency management landscape from an organizational standpoint. This study relies on a single-country case and a few industrial or business scenarios, however, it sheds light on diverse and promising research directions. Moving forward, it is essential to explore additional scenarios, examine deeper into case studies and leverage the mission-critical ecosystem as a framework for enhancing emergency management preparedness and response.

REFERENCES

Ali, A., & Ware, A. (2021). Effective Performance Metrics for Multimedia Mission-critical Communication Systems. *Annals of Emerging Technologies in Computing (AETiC)*, *5*(2), 1-14.

Austin, R., & Larkey, P. (1992). The unintended consequences of micromanagement: the case of procuring mission critical computer resources. *Policy Sciences*, 3-28.

Bernardini, G., Paganelli, F., Manetti, M., Fantechi, A., & Iadanza, E. (2013). SYRMA: a tool for a system approach to risk management in mission critical systems. *International Journal of Business Information Systems*, *13*(1), 21-44.

Boh, W., Constantinides, P., Padmanabhan, B., & Viswanathan, S. (2023). Building digital resilience against major shocks. *MIS Quarterly*, *47*(1), 343-360.

Breznitz, D., Ornston, D., & Samford, S. (2018). Mission critical: the ends, means, and design of innovation agencies. *Industrial and Corporate Change*, *27*(5), 883-896.

Cao, J., Zhao, J., Zhu, X., Jiang, Y., & Wei, Z. (2021). Toward a green secure relay system for mission-critical IoT: Hybrid duplex relay selection and resource allocation in the finite block length regime. *IEEE Transactions on Green Communications and Networking*, *5*(4), 1869-1879.

Cerullo, V., & Cerullo, M. J. (2004). Business Continuity Planning: A Comprehensive Approach. *Information Systems Management*, *21*(3), 70-78. https://doi.org/10.1201/1078/44432.21.3.20040601/82480.11

CISA. (2024). *Emergency Services Sector Continuity Planning Suite*. . USA: Cybersecurity and Infrastructure Security Agency Retrieved from https://www.cisa.gov/emergency-services-sector-continuity-planning-suite

Curtis, P. M. (2021). *Maintaining Mission Critical Systems in a 24/7 Environment*. John Wiley & Sons, Inc.

Dahl, I. R., Tveiten, B. W., & Cowan, E. (2022). The Case for Policy in Developing Offshore Wind: Lessons from Norway. *Energies*, *15*(4), 1569.

DEH. (2023). *National e-Health Strategy*. Norway: Directorate of e-Health

DSB. (2020). *Risikostyring i digitale verdikjeder*. Norway: Direktoratet for samfunnsikkerhet og beredskap

A Green Deal Industrial Plan for the Net-Zero Age, (2023).

FEMA. (2018). *Continuity Guidance Circular*. USA: Federal Emergecy Management Agency - National Continuity Programs Retrieved from https://www.fema.gov/sites/default/files/2020-07/Continuity-Guidance-Circular_031218.pdf

FEMA. (2019). *Business Process Analysis and Business Impact Analysis User Guide*. USA: Federal Emergency Management Agency Retrieved from https://www.fema.gov/sites/default/files/2020-07/fema_BPA-BIA-Users-Guide_070119.pdf

FEMA. (2020). *Continuity of Operations Plan Template for Federal Departments and Agencies*. Washington DC, USA: Federal Emergecy Management Agency - National Continuity Programs Retrieved from https://www.fema.gov/sites/default/files/2020-10/fema_planning-template-federal-departments-agencies_october-2020_0.pdf

FEMA. (2021). *Developing and Maintaining Emergency Operations Plans Comprehensive Preparedness Guide (CPG) 101 Version 3.0*. USA: Federal Emergecy Management Agency - National Continuity Programs Retrieved from https://www.fema.gov/sites/default/files/2020-07/Continuity-Guidance-Circular_031218.pdf

Figenbaum, E. (2023). The contribution of research and knowledge accumulation in the development of the Norwegian battery electric vehicle market. *Transportation Research Procedia*, *72*, 4127-4134.

Garousi, V., Felderer, M., & Mäntylä, M. V. (2019). Guidelines for including grey literature and conducting multivocal literature reviews in software engineering. *Information and software technology*, *106*, 101-121.

Grace, R., Gautam, S., & Tapia, A. (2023). Continuity planning for public health crises: Designing workplace redundancies for organizational resilience. *Journal of emergency management (Weston, Mass.)*, *21*(6), 523-537.

Hannah, S. T., Uhl-Bien, M., Avolio, B. J., & Cavarretta, F. L. (2009). A framework for examining leadership in extreme contexts. *The Leadership Quarterly*, *20*(6), 897-919.

Hansen, L., & Nissenbaum, H. (2009). Digital disaster, cyber security, and the Copenhagen School. *International studies quarterly*, *53*(4), 1155-1175.

Hebert, P., Clare, G., Jayadas, A., & Balasubramanian, M. (2018). Tunable White Light System for Mission-Critical Control Room and Anti-Fatigue Room for Shift Workers: A Case Study. 2018 IEEE PES Asia-Pacific Power and Energy Engineering Conference (APPEEC),

Innovasjon-Norge. (2023). Tall om batterier.

Johnsen, I.-K., & Lysgaard, V. (2022). *Risikostyring av IKT-sikkerhet i leverandørkjeder* Oslo, Norway: Norges vassdrags- og energidirektorat

Johnson, D. (1999). Secure Access to Mission-Critical Applications. *Inf. Secur. J. A Glob. Perspect.*, *8*(1), 54-63.
Kamei, F., Pinto, G., Wiese, I., Ribeiro, M., & Soares, S. (2021). *What Evidence We Would Miss If We Do Not Use Grey Literature?* Proceedings of the 15th ACM / IEEE International Symposium on Empirical Software Engineering and Measurement (ESEM), Bari, Italy. https://doi.org/10.1145/3475716.3475777
Krivý, M. (2023). Digital ecosystem: The journey of a metaphor. *Digital Geography and Society*, *5*, 100057. https://doi.org/https://doi.org/10.1016/j.diggeo.2023.100057
Kvadsheim, H. D., Øvergaard, B. N., & Barstad, L. (2023). *IKT-sikkerhetstilstanden i kraftforsyningen 2023* Oslo, Norway: Norges vassdrags- og energidirektorat
LeSaint, J., Reed, M., & Popick, P. (2015). System security engineering vulnerability assessments for mission-critical systems and functions. 2015 Annual IEEE Systems Conference (SysCon) Proceedings,
Magutshwa, S. (2022). Rethinking the improvisation of digital health technology: A niche construction perspective. *Australasian Journal of Disaster and Trauma Studies*, *26*(Special Issue on Information Systems).
Magutshwa, S., & Radianti, J. (2021). A Qualitative Risk Identification Framework for Cyber-Physical-Social Systems. Proceedings of the 18th Information Systems for Crisis Response and Management Conference Blacksburg, VA, USA
Magutshwa, S., & Radianti, J. (2022). Is this Digital Resilience? Insights from Adaptation and Exaptation of a Cyber-Physical-Social System.
Mars, M. M., Bronstein, J. L., & Lusch, R. F. (2012). The value of a metaphor: Organizations and ecosystems. *Organizational Dynamics*, *41*(4), 271-280.
Mattos, D. I., Dakkak, A., Bosch, J., & Olsson, H. H. (2020). Experimentation for business-to-business mission-critical systems: A case study. Proceedings of the International Conference on Software and System Processes,
Meld.St.5. (2023). *En motstandsdyktig helseberedskap Fra pandemi til krig i Europa. Meld. St. 5 (2023–2024), Melding til Stortinget*. Helse-og-omsorgsdepatementet
Microsoft. (2023). Mission-critical workloads. *Azure*.
Motvind-Norge. (2019). *Energipolitikk på naturens premisser – til beste for klima, naturmangfold, mennesker og næringsliv*.
Mukherjee, M., Chatterjee, R., Khanna, B. K., Dhillon, P. P. S., Kumar, A., Bajwa, S., Prakash, A., & Shaw, R. (2020). Ecosystem-centric business continuity planning (eco-centric BCP): A post COVID19 new normal. *Progress in Disaster Science*, *7*, 100117. https://doi.org/https://doi.org/10.1016/j.pdisas.2020.100117
NORMEN. (2018). *Tiltak for å hindre ondsinnet programvare (faktaark 19)* Norway: Directorate for e-Health
NORMEN. (2021). *Nødprosedyrer ved bortfall av IKT (faktaark 11) , versjon 3.0*. Norway: Direktoratet for e-helse
NORMEN. (2022a). *Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren Versjon 6.1* Norway: Direktoratet for e-Helse
NORMEN. (2022b). *Veileder om risikostyring for informasjonssikkerhet og personvern* Norway: **Direktoratet for e-helse**
NORMEN. (2023). *Informasjonssikkerhet og personvern for leverandører til helse- og omsorgssektoren* Norway: Direktoratet for e-Helse
NOU. (2023a). *Mer av alt - raskere: energikommisjonens rapport*. Norway: Norges offenlige utredninger
NOU. (2023b). *Når det er alvor: Rustet for en usikker fremtid*. Norway: Norges offenlige utredninger
NSM. (2023). *Risiko 2023: Økt uforutsigbarhet krever høyere beredskap*. Norway: Nasjonal sikkerhetsmyndighet
Pavlikakis, G. E., & Tsihrintzis, V. A. (2000). Ecosystem Management: A Review of a New Concept and Methodology. *Water Resources Management*, *14*(4), 257-283. https://doi.org/10.1023/A:1008139011867
Pickett, S. T. A., & Cadenasso, M. L. (2002). The Ecosystem as a Multidimensional Concept: Meaning, Model, and Metaphor. *Ecosystems*, *5*(1), 1-10. https://doi.org/10.1007/s10021-001-0051-y
Reid, M. B. (2021). Business continuity plan. In *Encyclopedia of Security and Emergency Management* (pp. 52-57). Springer.
Rucks, A. C., Ginter, P. M., Duncan, W. J., & Lesinger, C. (2011). A continuity of operations planning template: Translating public policy into an effective plan. *Journal of Homeland Security and Emergency Management*, *8*(1), 000010220215477355177 5.
Schulz, F., & Rode, J. (2022). Public charging infrastructure and electric vehicles in Norway. *Energy Policy*, *160*, 112660.

Skjærseth, J. B., & Rosendal, K. (2023). Implementing the EU renewable energy directive in Norway: from Tailwind to Headwind. *Environmental Politics*, *32*(2), 316-337.

Thorne, R., Aguilar Lopez, F., Figenbaum, E., Fridstrøm, L., & Müller, D. B. (2021). Estimating stocks and flows of electric passenger vehicle batteries in the Norwegian fleet from 2011 to 2030. *Journal of Industrial Ecology*, *25*(6), 1529-1542.

Thorne, R. J., Hovi, I. B., Figenbaum, E., Pinchasik, D. R., Amundsen, A. H., & Hagman, R. (2021). Facilitating adoption of electric buses through policy: Learnings from a trial in Norway. *Energy Policy*, *155*, 112310.

Van der Meulen, N. (2013). Diginotar: Dissecting the first dutch digital disaster. *Journal of strategic security*, *6*(2), 46-58.

Veikart Helsenæringen. (2023). Norway: Helse- og omsorgsdepartementet

Veisten, K., Wangsness, P. B., Farstad, E., & Ydersbond, I. M. (2024). Will people prefer future travel with battery-powered airplanes? *Transportation Research Part D: Transport and Environment*, *126*, 104013.

Weger, K., Matsuyama, L., Zimmermann, R., Mesmer, B., Van Bossuyt, D., Semmens, R., & Eaton, C. (2023). Insight into user acceptance and adoption of autonomous systems in mission critical environments. *International Journal of Human–Computer Interaction*, *39*(7), 1423-1437.

Yip, J., Ernst, C., & Campbell, M. (2009). Boundary spanning leadership: Mission critical perspectives from the executive suite. *Center for Creative Leadership Organizational Leadership White Paper*.

Zuo, Y. (2013). Modeling service migration and relocation in mission-critical systems. Critical Infrastructure Protection VII: 7th IFIP WG 11.10 International Conference, ICCIP 2013, Washington, DC, USA, March 18-20, 2013, Revised Selected Papers 7,