Towards operationalizing cyber resilience - a socio-technical analytical framework

Anton Holmström[1], Simon Andersson[1] and Johan Wenngren[1]

[1]Computer Science, Electrical and Space Engineering, Luleå University of Technology, Sweden

Abstract

Cyber resilience has emerged as a complementary concept to cybersecurity, expanding the traditional predict-and-protect paradigm to include business continuity and adaptive capacities. However, much of the literature remains normative, emphasizing what organizations should do, rather than analyzing what cyber resilience looks like in practice. This paper presents a theoretical framework for analyzing cyber resilience in organizations. Drawing on resilience theory and socio-technical systems theory, the framework identifies four interdependent capabilities—anticipate, withstand, recover, and adapt—and uses the principle of joint optimization to examine how technical and social elements interact within and across these capabilities. The framework was developed using a concept analysis method and is designed to be applied to empirical data, such as interviews or case studies. Its key contribution is to enable structured analysis of how resilience manifests, and how different capabilities compensate for one another depending on the system's state. We argue that the organization is constantly evolving and changing, meaning that observations are of a temporary system state that has already begun to change. However, analyzing snapshots of the system's capabilities can help identify areas for improvement. Future research can apply the framework to understand the mechanisms underlying cyber resilience.

Keywords

cyber resilience, cybersecurity, socio-technical, business continuity

1. Introduction

Cyber resilience has emerged as a complementary concept to cybersecurity, offering a broader perspective on how organizations prepare for and respond to digital threats. With the rise of complex and persistent cyber threats, some limitations in traditional cybersecurity approaches have become visible. One such limitation is the tendency to assess risks only at a technical level, estimating, for example, a server's vulnerability without fully understanding the operational consequences of system failure [1]. As digital systems become more interconnected and embedded in everyday operations, there is a growing need for an approach that accounts not only for infrastructure and software but also for organizational behaviour, human decision-making, and the ability to adapt under pressure [2]. Cyber resilience responds to this need by expanding security beyond "predict and protect" to include how organizations withstand, recover from, and learn from disruptions [3]. In doing so, cyber resilience reflects a shift in how cybersecurity is conceptualized within modern organizations. By recognizing that adequate security is about building stronger technical defences and enabling socio-technical systems, where technology and people operate together, to remain functional in the face of uncertainty [4]. This reframing has contributed to the increasing use of the term across various contexts. Today, cyber resilience is prominently featured in policy documents, risk management strategies, and industry standards, signaling its growing relevance in fields ranging from national infrastructure protection to organizational IT governance [5].

11th International Workshop on Socio-Technical Perspectives in IS (STPIS'25)

*Anton Holmström

**Simon Andersson

**Johan Wenngren

†Originated the concept, led the project's overall development, and guided the research from inception through completion.

‡Contributed to refining the conceptual framework and provided ongoing support for both the methodological approach and manuscript preparation.

anton.holmstrom@ltu.se (A. Holmström); simon.andersson@ltu.se (S. Andersson); johan.wenngren@ltu.se (J. Wenngren)

0000-0002-0498-4858 (A. Holmström); 0000-0002-4057-9454 (S. Andersson); 0000-0003-3080-1354 (J. Wenngren)

Despite the growing attention to cyber resilience within politics, industry, and research, there remains a lack of structured, theory-informed approaches to analyze the behaviors and responses that promote resilience in organizations during cyber incidents. While many cyber resilience frameworks exist, most adopt a normative stance, defining what resilience should look like, rather than capturing how it is promoted in practice. This normativity often fails to recognize the ambiguity in resilience-related situations found in reality [6]. As Benoît Dupont et al. [7] argues, the issue with such normativity is further complicated by a lack of empirical research on how professionals and their organizations make sense of resilience and how they navigate conflicting demands in practice. This limits our understanding of how human and organizational factors practically promote or impair the resilience activities typically prescribed in the literature. There is a lack of ways to analyze resilience in practice, and this has resulted in a lack of empirical studies. To address this gap, we propose an analytical framework that captures how resilience emerges within socio-technical systems, rather than prescribing how it should function. The aim of this study is to take a first step towards operationalizing cyber resilience by developing a framework that supports empirical analysis of resilience in organizations. This framework focuses on four core capabilities and their socio-technical configurations. Therefore, this article explores the research question: *How can cyber resilience be analytically framed and assessed to reflect its emergent, socio-technical, and behavioral characteristics during cyber disruptions?*

2. Background

The concept of resilience, originating in physics and material science, describes how systems respond to external disturbances or stress. It was initially used to characterize the ability of materials to absorb energy and return to their original shape. Over time, the concept has been adopted across various disciplines—including ecology, psychology, engineering, economics, and, more recently, cybersecurity, each adapting the term to suit different system behaviors and contexts [8].

2.1. Cyber Resilience

Holling [9], a foundational researcher in ecology, outlines two distinct interpretations of resilience. The first, often referred to as engineering resilience, emphasizes stability and the capacity of a system to resist change and quickly return to an equilibrium state following a disruption. This interpretation has influenced engineering and economic theory, where performance is measured regarding efficiency, control, and recovery time. The second interpretation, ecological resilience, concerns how systems behave far from equilibrium. It highlights the ability to absorb shocks without losing functional integrity, even when facing disturbances that may fundamentally alter the system's structure or behavior. Instead of returning to a previous state, a resilient system may reorganize into a new, stable state that still fulfills essential functions. Ecological resilience is based on the idea that variability, redundancy, and diversity promote a system's ability to survive disruptions and adapt over time. However, applying this thinking to organizations, which usually prioritize efficiency and control, suggests that organizations are limited in their ability to tolerate variation and transformation. Therefore, strategies that maximize short-term results, like lean processes and cost-savings, may inadvertently reduce the long-term resilience by eliminating room and diversity that promote adaptability [3]. These two views reflect fundamentally different assumptions about how systems behave under stress. While engineering resilience aims for preservation and control, ecological resilience embraces uncertainty, adaptation, and transformation. Despite being based in ecological systems, Holling's [9] work provides valuable insights into guiding decision-makers in highly coupled areas like critical infrastructures, organizations, and digital environments, where resilience must balance efficiency and adaptability to thrive. As cyber attacks become increasingly unpredictable, with potential complicated and sometimes complex consequences, the ecological view of resilience offers a more suitable foundation for understanding how organizations survive and evolve through disruptions.

Organizational cyber resilience ought to be viewed through the lens of ecological systems, as this provides a more realistic and flexible conceptual foundation for cyber resilience than the engineering

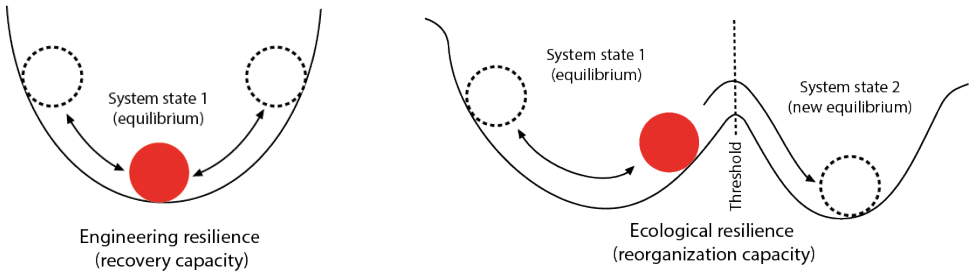

Figure 1: Engineering and Ecological Systems, adapted from [10]

model. While engineering resilience builds on the idea of a closed system perspective with clear boundaries and predictable ways of recovery, an organization is an open system continuously being shaped by its interaction with the environment. An organization's survival depends on its relation to external and internal actors and conditions [11]. This has important implications for how we approach resilience. Instead of understanding resilience as just a return to a previous state, resilience must be understood as something that emerges over time, shaped by uncertainty, adaptation, and learning. Much of the existing literature on cyber resilience, however, remains normative—focused on what resilient organizations should look like, rather than how resilience is actually achieved in practice. As Duchek [12, p. 223] notes, "we do not really know how resilience may be achieved in practice," which makes it challenging to design for. This highlights a central limitation of engineering-based models: they assume that resilience can be planned and built into systems in advance. But in organizational contexts, resilience is not simply a property of design; it is a situated, ongoing process that unfolds in action [3]. Because engineering models rely on predictability and control, they struggle to account for the ambiguity, improvisation, and social dynamics that shape how resilience is enacted during actual disruptions. This further supports the view that an ecological perspective offers a more suitable basis for understanding how cyber resilience is enacted in organizational settings. With this foundation in place, we can now begin to consider how resilience relates to and differs from core cybersecurity practices.

An organization can have cybersecurity without being cyber resilient, but it cannot be cyber resilient without cybersecurity [3]. Cyber resilience builds on the foundational cybersecurity routines, but extends further by including contingency planning, adaptive capacity, and system-level robustness [6]. However, with the increasing complexity and unpredictability of cyber threats, more than preventative controls are required. Resilience becomes decisive when traditional risk management fails to predict or mitigate disruptions. In such situations, resilience takes over from risk management and works as a continuous cycle of prediction, reaction, and adaptation [3]. Instead of only trying to prevent intrusion, resilient organizations can absorb and work through the attacks, minimizing the operational impact of an attack. Despite this extended scope, the concept of cyber resilience has been criticized for its vagueness and lack of operational clarity [13]. Scholars note that the term is widely used but inconsistently defined, undermining its value for research and practice [14]. This ambiguity makes it difficult to design for resilience, assess its presence, or integrate it meaningfully into organizational strategy. To move beyond this challenge, it is necessary to unpack what resilience does, rather than what it is. One way to do this is to consider resilience as a set of capabilities that unfold over time—some of which can be planned for in advance, while others emerge in response to disruption.

Resilience can be understood to operate across two dimensions: planned and adaptive resilience [15]. Planned resilience is about preparedness, actions taken before a disruption occurs. These can be risk management, crisis exercises, or technical controls. These actions create the foundation for the system's robustness and its ability to identify and manage potential risks in an early stage. On the other hand, adaptive resilience is about developing new abilities during or after a disruption. This dimension is activated when something unexpected happens, requiring actions that were not accounted for in prior plans. Flexibility, improvisation, and organizational learning are central aspects here [15]. These two dimensions are interdependent. Planned resilience enables adaptive resilience, and better

preparedness results in a greater ability to act flexibly in crisis. Further, the results from the adaptive efforts are valuable input for future planning: What did we learn, and how can it be incorporated into the organization's preparedness? Resilience occurs when planned and adaptive capabilities collaborate. When the planned actions are not enough, the adaptive elements—such as incident response and improvised problem solving—need to take over and assume greater responsibility [16].

2.2. Cyber Resilience Capabilities

To explore how resilience may be understood and analyzed, it is helpful to consider four core capabilities: *anticipate*, *withstand*, *recover*, and *adapt*. These capabilities are not drawn from a single unified definition but recur across literature on cyber resilience, system resilience, and crisis response [17, 18, 19, 20]. Rather than presenting a new theory, this paper builds on and integrates existing ideas to support a more structured understanding of cyber resilience. In this paper, cyber resilience is defined as the capacity of a system, in this case, the organization, to continuously deliver its intended outcomes by anticipating, withstanding, recovering from, and adapting to adverse cyber events [21, 7, 17]. While these capabilities may take different forms depending on context, they offer a conceptual structure for analyzing how resilience is promoted and enacted over time.

- **Anticipate** refers to the organization's ability to recognize and prepare for potential disruptions. This might involve formal activities such as risk assessments, scenario planning, or technical monitoring, but also includes informal practices like cultivating situational awareness, encouraging knowledge sharing, or drawing on intuition based on experience.
- **Withstand** is the ability to absorb and contain the effects of disruption without losing core functionality. It includes technical protections and social and organizational factors such as team cohesion, trusted leadership, and the ability to make decisions under stress.
- **Recover** focuses on restoring function after a disruption. This may involve structured processes such as incident response, system restoration, and more improvised efforts like sensemaking, re-prioritization, and mobilizing internal networks to stabilize operations.
- **Adapt** is about making longer-term changes based on lessons learned. It can include refining processes, updating policies, restructuring systems, or shifting organizational norms. Adaptation may be incremental or transformational, often based on insights gained during recovery.

2.3. Socio-Technical Systems Theory and Joint Optimization

Organizations are best understood as socio-technical systems, meaning they are composed of both technical and social elements that interact to shape system behaviour [22]. A socio-technical system (STS) consists of two interdependent elements: the technical and the social. The technical element includes infrastructures, supporting artefacts, and digital systems, while the social element comprises people, roles, norms, and work practices. These elements are interconnected and should not be viewed as separate or isolated; they function as part of a larger whole [23]. STS are made up of humans using technology to carry out tasks within an organization to achieve defined objectives [24]. The social dimension aims to design work environments and organizational structures considering people's psychological needs. It is not just about doing the job efficiently, but about people: doing meaningful work, feeling a sense of belonging to the group or organization, and feeling responsible for what they do. The purpose of the technical dimension is to provide the organization with technologies enabling it to achieve its goals [25]. Understanding the technical and social differences is central to how we think about cyber resilience. Resilience is not something that resides in a technical solution or an individual. Instead, it emerges from how social and technical elements work together to respond to disruption [4]. In this sense, resilience is an emergent property, a characteristic of the whole system that none of the parts have when taken separately. Cyber resilience, then, is not simply about having the right defences; it is about how the system as a whole anticipates, withstands, recovers, and adapts to disruptions. To support this kind of system-wide resilience, it is not enough to develop the technical and social components in isolation. They need to be designed and managed together.

Joint optimization is a central principle of socio-technical systems theory. It suggests that a system's social and technical parts must be co-developed to create sustainable system performance. If an organization aims to improve functions or efficiency through isolated changes in technology or social factors, it will create an imbalance. Technology and humans affect each other, and it is in the interaction between these that the actual functioning of the system is shaped. Therefore, it is suggested that a system cannot be understood or enhanced if the interdependent relationship of the components is ignored [22]. Technology shapes how people work, while people's behaviours, habits, and needs influence technology. For example, suppose an organization introduces an advanced cybersecurity software without considering how the business operates or providing support to understand it, there is a risk that it will be used incorrectly or not at all. Similarly, a strong security culture is insufficient if the technical measures that support secure behaviour are missing. For the system to work, technology and human factors must evolve in tandem and with each other [26]. Joint optimization means designing and managing a system's social and technical elements in parallel, so they support each other and work together to achieve overall system performance.

3. Research Approach

The research approach is based on Näsi [27]'s concept analysis model, as presented in Nuopponen [28], which outlines four interrelated phases. First, a knowledge foundation is established through a literature review. Second, relevant concepts are distinguished from related or overlapping terms (external analysis). Third, the internal structure and relationships of the selected concepts are examined (internal analysis). Finally, conclusions are drawn in the form of a structured framework intended to support empirical analysis. The process began with a review of the literature on cyber resilience. We noted that most contributions are normative in nature and offer limited solutions for analyzing what organizations do in practice. To address this, we traced the conceptual roots of cyber resilience in resilience theory, identifying two main perspectives: engineering and ecological. We chose the ecological perspective as our main perspective to frame resilience as a dynamic property of open systems. We then returned to the cyber resilience literature and identified four commonly cited capabilities: anticipate, withstand, recover, and adapt. These capabilities form the foundation of the framework. To analyze how these capabilities manifest in practice, we introduced snapshots, temporary representations of the system's state before, during, or after a disruption. Each snapshot allows for examination of which capabilities were active and how they interacted. Finally, we applied socio-technical systems theory to assess the alignment between technical and social components within each capability. The principle of joint optimization was used to identify potential imbalances. The outcome is an analytical framework intended for use in empirical case studies.

4. Results

The analytical framework brings together two perspectives: organization as a socio-technical system and resilience as an emergent property of that system. In this framework, the organization is understood as an open, dynamic system that consists of independent social and technical components. Drawing on the ecological systems thinking, resilience is conceptualized not as returning to a fixed equilibrium, but as the system's ability to remain functional within or across different states of stability or "basins of attraction" [9]. Stability in the system is maintained through the ability to predict, absorb, and respond to disruptions. However, when a disruption exceeds the system's ability to absorb, recovery and adaptation become necessary to establish a new form of stability. Thus, resilience is not a fixed property gained from a technical tool (document templates, software, etc., intended to support an activity [29]) or plan but a system-level behavior that evolves over time [3]. This dynamic understanding of the system's behavior is the foundation for how the analytical framework is applied different moments in time, where every capability has different roles before, during, and after an incident.

To capture how resilience is manifested over time, the framework uses the concept of "snapshots",

discrete analytical moments. To analyze an incident includes identifying what the organization did before, during, and after the disruption. At each stage, different resilience capabilities may be utilized or emphasized; different states are shown in Figure 2. For example, in a stable state, its anticipatory capabilities, such as risk assessment, crisis management plans, or protective actions, are likely to be visible before a disruption. These are aimed at preserving a desired state. Other capabilities emerge when the situation changes, such as during an attack. Withstand and recover become more central as the organization works to contain the disruption and restore core functionality. By breaking the timeline of an incident into analytical moments, we can observe how resilience is not constant, but shifts depending on the system's state and the nature of the threat. This structure supports a nuanced analysis of how these capabilities work in practice and provides a foundation to examine the socio-technical balance within each capability.

Within each capability, the framework allows for analysis on the degree of alignment between the social and technical components using the principle of joint optimization. Joint optimization does not mean that we are aiming for a consistent 50/50 distribution of social and technical components, but rather to find a state where the social and technical elements are mutually supportive and proportionate to the needs of the situation [22]. To clarify, some situations might refer to balance as a highly technical solution supported by a minimal social component, such as training or understanding how to operate it. Other situations might require a social component to dominate, while the technical tool is supportive. Imbalance occurs when one dimension is overdeveloped or overloaded without sufficient support from the other [26]. For instance, an organization is recovering from an ongoing cyberattack and has deployed an advanced backup system to restore data. However, if staff are unsure how to access or activate the system under pressure, or if communication between IT and operational teams is unclear, the recovery process may stall. In this case, the technical component is strong. Still, the lack of social support, such as training, clear roles, or communication routines, creates an imbalance that weakens the overall recovery capability. This places pressure on one part of the system, weakening the overall capability. By identifying these imbalances in the different phases of an incident, the analysis can show where resilience is constrained not by a lack of effort but by a lack of integration. Joint optimization is, therefore, not the result but a diagnostic measure for evaluating the effectiveness and coherence of each capability within the socio-technical system.

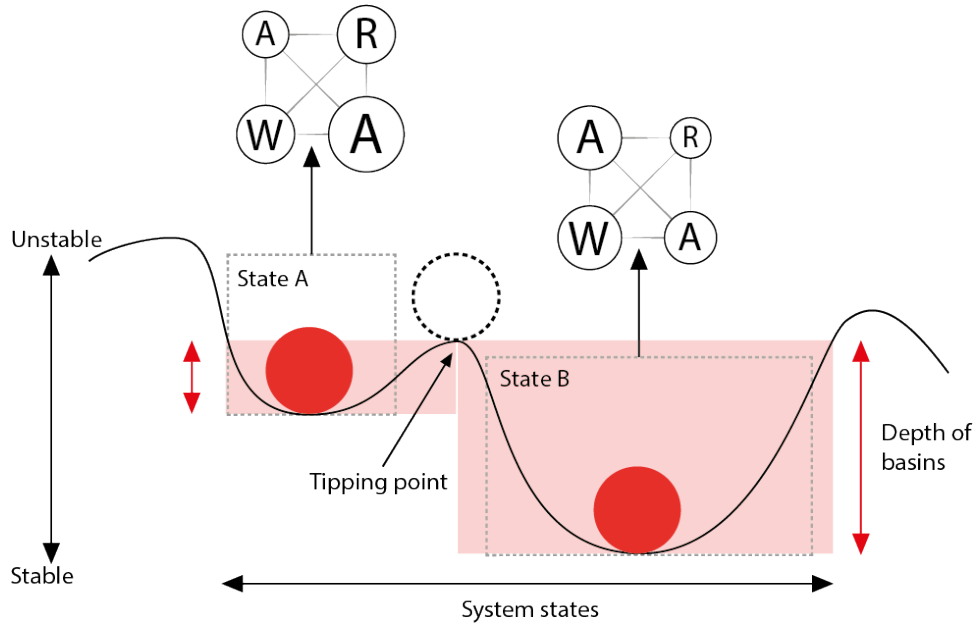

Figure 2: Engineering and Ecological Systems, adapted from [30]

5. Discussion

To illustrate cyber resilience, we utilize the basin of attraction model (see figure 2). The basin of attraction stems from ecological resilience theory and is commonly used to visualize how systems respond to disturbances [31]. In this analogy, the ball represents the organization and its position in the current operational state, and the basin walls symbolize the organization's resistance to change. The steepness of the basin walls illustrates an organization's ability to absorb disruption. With a shallow basin, even a moderate disruption could affect the organization, and disturbances can affect and unbalance its current state. From this perspective, resilience is not only about resisting change but also about the system's ability to maintain a position and adapt and change into a new position when facing a disruptive change [3].

Working with cyber resilience requires shifting between an open and a closed system perspective. An open system perspective views the organization as dynamic, constantly interacting with and shaped by its environment. It acknowledges the organization's system-of-systems nature, where internal subsystems are interlinked and influenced by external factors such as political, economic, ecological, societal, and technological. In contrast, a closed system perspective treats the system as temporarily bounded and stable, enabling analysis and targeted intervention [9]. We must accept that the system is constantly in flux to get closer to operationalizing cyber resilience. Any observation or assessment is a temporary system state that has already begun to shift. However, without these analytical snapshots, it would be impossible to identify what capabilities are active, how they interact, and what can be strengthened or redesigned. Whenever the system is affected by internal or external factors, there will be a shift in its state and balance; this shift triggers a response among the four resilience capabilities. The capabilities, anticipate, withstand, recover, and adapt are not independent silos. They form a holarchical structure, where each capability supports the others but may carry different weights depending on the system's state. If one capability is weak or underdeveloped, another must compensate. For instance, when anticipation fails to detect a threat, the pressure to withstand or recover from that disruption increases. This interdependence and compensating relationship mean resilience is not evenly distributed but dynamically negotiated across capabilities. Different capabilities take on greater responsibility as the system shifts from stability to disruption and possibly reconfiguration. In the early phases, anticipation may dominate; during a crisis, withstand and recover become central; and in the aftermath, adapt carries the load. These shifts are not linear. Instead, feedback loops between the system's changing state and the activation of capabilities shape how resilience is enacted in practice. Understanding this internal logic is key to analyzing how resilience is sustained or strained over time. Much of the complexity lies in the transition between the feedback loops. Understanding how organizations move between anticipating, withstanding, recovering, and adapting, and how one capability feeds into or compensates for another, offers a promising direction for further research.

6. Illustrating the use of the framework

In each case, the analysis considers what was done and how these actions were supported technically and socially. If a technical backup system was in place but no one knew how to activate it, this would indicate an imbalance under the *recover* capability. Conversely, if recovery efforts were coordinated effectively between IT and operational staff, it might suggest a high degree of joint optimization. This way, the framework supports a structured, socio-technical interpretation of resilience-in-practice without reducing it to checklists or static maturity models.

To demonstrate how the framework can be applied, Table 1 presents an example based on a hypothetical incident. The example shows how observed or reported actions during different phases of an incident can be categorized under the four core capabilities. Each entry is then assessed based on whether it reflects a technical, social, or socio-technical response, followed by an interpretation of how well joint optimization is achieved. This allows for a structured analysis of strengths and imbalances in how resilience is enacted across the socio-technical system.

Table 1
Example of socio-technical analysis of resilience capabilities

Capability	Observed action or quote	Type	Joint Optimization	Analytical reflection
Anticipate	"We conducted a technical risk assessment of our IT systems."	Technical	Imbalance	Risk assessment focused on system vulnerabilities, but excluded end-user perspectives. Potential blind spots.
Withstand	"We had redundant servers, but staff were unsure how to switch between them."	Both (weak social)	Imbalance	Technical infrastructure was in place, but operational knowledge was lacking. Highlights dependence on social readiness.
Recover	"After the attack, we activated our incident response plan and convened the crisis team."	Both	Balanced	Recovery involved both planned technical responses and coordinated social action. Illustrates effective integration.
Adapt	"We held a debriefing, but no formal changes were made."	Social	Imbalance	Reflection occurred, but insights were not translated into structural or technical adaptations. Learning remained superficial.

Using the analytical framework, we expect to gain a better understanding of the activities in the four capabilities enabling cyber resilience in organizations, taking one step towards operationalization. This includes evaluating the relationship between the capabilities and whether they are supported by a socio-technical balance of people and technology, or if resilience is constrained by misalignment.

7. Conclusion and Future Directions

This paper set out to address a gap in the cyber resilience literature. While the concept has gained widespread attention, it is often treated normatively, with limited tools for analyzing what organizations do to be resilient in practice. Our motivation has shifted focus from what resilience should look like to how it is enacted within organizations. We address the research question: *How can cyber resilience be analytically framed and assessed to reflect its emergent, socio-technical, and behavioral characteristics during cyber disruptions?* by developing an analytical framework grounded in resilience theory and socio-technical systems thinking. The framework identifies four core capabilities: anticipate, withstand, recover, and adapt, and provides a structure for analyzing how these capabilities are activated across different system states. By incorporating the principle of joint optimization, the framework also highlights how technical and social components shape the effectiveness of each capability.

Future research could apply this framework to empirical case material to further assess its usefulness and refine its components. Doing so could support a deeper understanding of how cyber resilience is operationalized within real-world contexts. We hope this framework will support researchers and practitioners alike in making cyber resilience more observable and actionable.

Declaration on Generative AI

While preparing this work, the author(s) used ChatGPT and Grammarly to check grammar and spelling. After using these tools, the author(s) reviewed and edited the content as needed and take full responsibility for the publication's content.

References

[1] A. Holmström, Managing a Ransomware Attack: The Resilience of a Swedish Municipality – A Case Study:, in: Proceedings of the 11th International Conference on Information Systems Security and Privacy, SCITEPRESS - Science and Technology Publications, Porto, Portugal, 2025, pp. 199–208. URL: https://www.scitepress.org/DigitalLibrary/Link.aspx?doi=10.5220/0013110900003899. doi:10.5220/0013110900003899.

[2] Kjell Hausken, K. Hausken, Cyber Resilience in Firms, Organizations and Societies 11 (2020) 100204. doi:10.1016/j.iot.2020.100204, mAG ID: 3024755729.

[3] Benoît Dupont, The Cyber-Resilience of Financial Institutions: Significance and Applicability, Journal of Cybersecurity (2019). doi:10.1093/cybsec/tyz013, 24 citations (Crossref) [2023-04-24].

[4] M. Dunn Cavelty, C. Eriksen, B. Scharte, Making cyber security more resilient: adding social considerations to technological fixes, Journal of Risk Research 26 (2023) 801–814. URL: https://www.tandfonline.com/doi/full/10.1080/13669877.2023.2208146. doi:10.1080/13669877.2023.2208146.

[5] R. Azmi, W. Tibben, K. T. Win, Review of cybersecurity frameworks: context and shared concepts, Journal of Cyber Policy 3 (2018) 258–283. URL: https://doi.org/10.1080/23738871.2018.1520271. doi:10.1080/23738871.2018.1520271, publisher: Routledge _eprint: https://doi.org/10.1080/23738871.2018.1520271.

[6] S. M. Alhidaifi, M. R. Asghar, I. S. Ansari, A Survey on Cyber Resilience: Key Strategies, Research Challenges, and Future Directions, ACM Computing Surveys 56 (2024) 1–48. URL: https://dl.acm.org/doi/10.1145/3649218. doi:10.1145/3649218.

[7] Benoît Dupont, Clifford Shearing, Marilyne Bernier, Rutger Leukfeldt, The tensions of cyber-resilience: From sensemaking to practice, Computers & security 132 (2023) 103372–103372. doi:10.1016/j.cose.2023.103372, mAG ID: 4382602104 S2ID: fb1f88184ba2063a79e7d34d32d146dfe4c528b7.

[8] V. Tzavara, S. Vassiliadis, Tracing the evolution of cyber resilience: a historical and conceptual review, International Journal of Information Security 23 (2024) 1695–1719. URL: https://link.springer.com/10.1007/s10207-023-00811-x. doi:10.1007/s10207-023-00811-x.

[9] C. S. Holling, Engineering resilience versus ecological resilience, Engineering within ecological constraints 31 (1996) 32.

[10] M. C. Thoms, H. Piégay, M. Parsons, What do you mean, 'resilient geomorphic systems'?, Geomorphology 305 (2018) 8–19. URL: https://www.sciencedirect.com/science/article/pii/S0169555X1730212X. doi:https://doi.org/10.1016/j.geomorph.2017.09.003.

[11] M. N. Bastedo, Open systems theory, Encyclopedia of educational leadership and administration (2004) 20–24.

[12] S. Duchek, Organizational resilience: a capability-based conceptualization, Business Research 13 (2020) 215–246. URL: https://link.springer.com/10.1007/s40685-019-0085-7. doi:10.1007/s40685-019-0085-7.

[13] J. Hillmann, E. Guenther, Organizational Resilience: A Valuable Construct for Management Research?, International Journal of Management Reviews 23 (2021) 7–44. doi:10.1111/ijmr.12239.

[14] T. Prior, J. Hagmann, Measuring resilience: methodological and political challenges of a trend security concept, Journal of Risk Research 17 (2014) 281–298. URL: http://www.tandfonline.com/doi/abs/10.1080/13669877.2013.808686. doi:10.1080/13669877.2013.808686.

[15] B. Walker, V. Nilakant, R. Baird, Promoting Organisational Resilience through Sustaining Engagement in a Disruptive Environment: What are the implications for HRM? (2014).

[16] E. Barasa, R. Mbau, L. Gilson, What Is Resilience and How Can It Be Nurtured? A Systematic Review of Empirical Literature on Organizational Resilience, International Journal of Health Policy and Management 7 (2018) 491–503. URL: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6015506/.

[17] I. Linkov, A. Ligo, K. Stoddard, B. Perez, A. Strelzoffx, E. Bellini, A. Kott, Cyber Efficiency and Cyber Resilience, Communications of the ACM 66 (2023) 33–37. URL: https://dl.acm.org/doi/10.1145/3549073. doi:10.1145/3549073.

[18] S. Hosseini, K. Barker, J. E. Ramirez-Marquez, A review of definitions and measures of system resilience, Reliability Engineering & System Safety 145 (2016) 47–61. URL: https://www.sciencedirect.com/science/article/pii/S0951832015002483. doi:10.1016/j.ress.2015.08.006.

[19] T. Williams, D. Gruber, K. Sutcliffe, D. Shepherd, E. Y. Zhao, Organizational Response to Adversity: Fusing Crisis Management and Resilience Research Streams, The Academy of Management Annals 11 (2017). doi:10.5465/annals.2015.0134.

[20] T. Panagiotis, R. Holfeldt, M. Koraeus, B. Uckan, R. Gavrila, G. Makrodimitris, Report on cyber-crisis cooperation and management., Technical Report, Publications Office, LU, 2014. URL: https://data.europa.eu/doi/10.2824/34669.

[21] F. Björck, M. Henkel, J. Stirna, J. Zdravkovic, Cyber Resilience – Fundamentals for a Definition, Advances in Intelligent Systems and Computing 353 (2015) 311–316. doi:10.1007/978-3-319-16486-1_31.

[22] G. Baxter, I. Sommerville, Socio-technical systems: From design methods to systems engineering, Interacting with Computers 23 (2011) 4–17. URL: https://academic.oup.com/iwc/article-lookup/doi/10.1016/j.intcom.2010.07.003. doi:10.1016/j.intcom.2010.07.003.

[23] B. Whitworth, A Brief Introduction to Sociotechnical Systems:, in: M. Khosrow-Pour, D.B.A. (Ed.), Encyclopedia of Information Science and Technology, Second Edition, IGI Global, 2009, pp. 394–400. URL: http://services.igi-global.com/resolvedoi/resolve.aspx?doi=10.4018/978-1-60566-026-4.ch066. doi:10.4018/978-1-60566-026-4.ch066.

[24] R. P. Bostrom, J. S. Heinen, MIS Problems and Failures: A Socio-Technical Perspective. Part I: The Causes, MIS Quarterly 1 (1977) 17–32. URL: https://www.jstor.org/stable/248710. doi:10.2307/248710, publisher: Management Information Systems Research Center, University of Minnesota.

[25] S. H. Appelbaum, Socio-technical systems theory: an intervention strategy for organizational development, Management Decision 35 (1997) 452–463. URL: https://doi.org/10.1108/00251749710173823. doi:10.1108/00251749710173823, publisher: MCB UP Ltd.

[26] M. Malatji, S. Von Solms, A. Marnewick, Socio-technical systems cybersecurity framework, Information & Computer Security 27 (2019) 233–272. URL: https://www.emerald.com/insight/content/doi/10.1108/ICS-03-2018-0031/full/html. doi:10.1108/ICS-03-2018-0031.

[27] J. Näsi, Ajatuksia käsiteanalyysista ja sen käytöstä yrityksen taloustieteessä, Yrityksen taloustieteen ja yksityisoikeuden laitoksen julkaisuja: Tutkielmia ja raportteja, Tampereen yliopisto, 1980. URL: https://books.google.se/books?id=eX1cAAAACAAJ.

[28] A. Nuopponen, Methods of concept analysis-tools for systematic concept analysis (part 3 of 3), LSP Journal-Language for special purposes, professional communication, knowledge management and cognition 2 (2011).

[29] S. Andersson, E. Bergström, M. Lundgren, K. Bernsmed, G. Bour, Information security risk management tools in the air traffic management domain: what are practitioners' needs?, Information Security Journal: A Global Perspective (2025) 1–18.

[30] H. Fujita, S. Yoshida, K. Suzuki, H. Toju, Alternative stable states of microbiome structure and soil ecosystem functions, Environmental Microbiome 20 (2025) 28. URL: https://doi.org/10.1186/s40793-025-00688-4. doi:10.1186/s40793-025-00688-4.

[31] D. Briske, A. Illius, J. Anderies, Nonequilibrium Ecology and Resilience Theory, 2017, pp. 197–227. doi:10.1007/978-3-319-46709-2_6.