Cascade Cyber Risk Management
Between Rule and Reality

Peter H.M.P. Roelofsma

1. Introduction: What is your cyber risk appetite?

In the whimsical yet insightful episode 'Threat Detected' of the classic cartoon 'Tom and Jerry', a seemingly simple chase between the cat and mouse duo unfolds into a complex narrative of cyber security challenges[1]. Tom, in his relentless pursuit, attempts to gain unauthorized access to Jerry's cell phone, only to be thwarted by an AI-based threat detection system with partially automated responses.

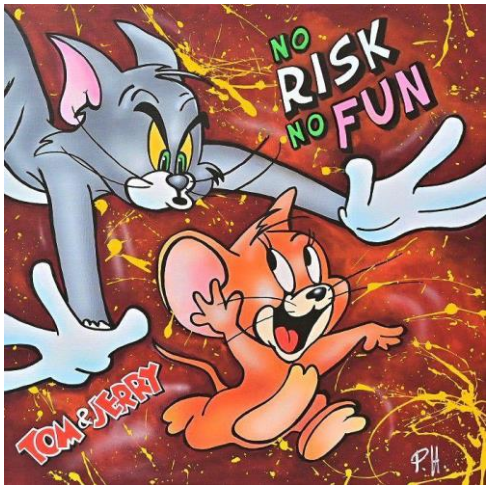

Figure 1. Jerry expressing an intense risk appetite

The enfolding scenario mirrors several cyber security dynamics, where malicious actors seek illegitimate access to sensitive information, and defensive systems must adapt to evolving threats. As the episode progresses, Jerry's use of IoT devices like the oven, water heater, and toaster to counter Tom's attacks highlights the interconnected nature of modern cyber environments. However, the AI support system becomes overwhelmed, leading to a cascade of unintended consequences, and the system starts attacking both Tom and Jerry. A rogue cable comes suddenly out of the wall as an unexpected entity and swallows them both and spews them out.

This chaotic turn of events underscores the potential for cascading failures in cyber security, where initial breaches can trigger a series of unpredictable and escalating disruptions, often exacerbated by non-linear feedback loops. Through this animated allegory, we explore the critical importance of robust, adaptive, and resilient cyber security measures in preventing and mitigating cascade effects in digital ecosystems.

The story also illustrated Tom and Jerry's 'No Risk, No Fun'- attitude with a high and escalating cyber risk appetite. This reflects their willingness to take on significant cyber risks in pursuit of their goals. A cyber risk appetite is the amount and type of risk that a person -or an organization- is willing to take in order to achieve its objectives. It involves balancing the potential benefits of taking risks against the potential negative consequences (Feng et al, 2019).

In the world of cybersecurity, new types of emotions have emerged, such as cyber shame and cyber paranoia. Cyber shame refers to the feelings of embarrassment and guilt that individuals or organizations experience after a cyber incident, particularly when it involves a breach of personal or sensitive information (Renault et al, 2021). Cyber paranoia, on the other hand, is

[1] See: The Tom and Jerry Show | Threat Detected | Boomerang UK

the excessive and irrational fear of being targeted by cyber threats, often leading to heightened anxiety and mistrust of digital environments (Mason et al, 2014).

While I want to avoid cyber shame and cyber paranoia, it's important to acknowledge that the world of cybersecurity is ever-evolving, with increasing variations in cyber risk landscape profiles. One of these is cascade cyber risk, which refers to the domino effect where a cyber-attack on one system leads to subsequent failures in interconnected systems in critical infrastructure (Paletti et al, 2021). The European Union Agency for Cybersecurity (ENISA 2023a) predicts that by 2030 cascade supply chain attacks will become the leading cyber threat facing organisations (ENISA, 2023a). The number of organisations impacted with such attacks has increased by more than 2600 percentage points over the past five years alone.

Cascade cyber incidents, where a cyber-attack on one system leads to subsequent failures in interconnected systems, have increasing significant impacts and implications on society's critical infrastructure. The SolarWinds attack, for instance, compromised numerous government and private sector systems by exploiting a software update (Kruti et al, 2023). The Ledger breach exposed sensitive customer data, leading to widespread phishing attacks (ENISA, 2023b). The Kaseya ransomware attack affected hundreds of businesses globally by targeting a remote management software (Oxford Analytica, 2021). The Viasat incident disrupted satellite internet services, impacting critical communications (Boschetti et al, 2021). Some cascades are intersectoral and lead from a failure in electricity to a failure in telecoms, to further failure in electricity, e.g. the 2003 Italian blackout (Buldyrev, 2010). Some are the result not from the evil outside the organization but result from insider threats (Al-Mhiqani, 2024) or from or insider mistakes, e.g. the CrowdStrike bug in 2024 (Kubota, 2024). The CrowdStrike cyber crash was not a malicious attack, but caused disruptions in various sectors due to a faulty content update. These incidents and many more highlight the vulnerabilities in interconnected systems and the far-reaching consequences of cascade cyber risk. How is your appetite for this type of risk?

Outline of this document.
Section 2 outlines the ten common components of cascade cyber risks. Section 3 explains the need for increased societal vigilance regarding this phenomenon. Section 4 discusses the 'Tower of Babel' effect in Cascade Cyber Risk Management. Section 5 identifies the five main misalignments between rules and realities in cascade cyber risk management that relate to this effect. Section 6 provides the theoretical and computational background for addressing these misalignments, detailing our innovative AI-based cascade cyber risk assessment method using computational shared mental modeling. This section also presents the initial results from the THUAS research group of the Risk Management & Cybersecurity lectorate. Section 7 describes the methodological approach for data collection foundational to the Cybersecurity Living Lab by the Risk Management and Cybersecurity lectorate, summarizing the main research directions of the Cybersecurity Living Lab. Section 9 outlines the narrative of change for the future of Cyber Cascade Risk Management. Section 10 includes an annex with a detailed description of the THUAS research program by the Risk Management and Cybersecurity research group.

2. Common components of cascade cyber risks

Recent literature has increasingly focused on cascade cyber risks (Gahdge et al, 2019; Daniel et al., 2022; Jaziery et al, 2023; Hill et all, 2023; Melnyk, 2021; Fayi, 2018; Toregas, et al 2019; Forscey et al., 2022; Colicchia et al, 2019; Boschetti et al., 2021; ENISA, 2023b;

Pescaroli et al., 2015; Paletti et al., 2021; Wallis et al., 2023; Panda et al. 2020; Pandey et al, 2020; Welburn et al., 2021; Torres et al., Zhang et al, 2017). Analysis of various cases and incidents reveals that these risks share ten key components, each contributing uniquely to the potential severity of cascade cyber incidents. While some components may overlap, each plays a distinct role in escalating the impact of cyber threats. Understanding these components is essential for organizations to develop robust cybersecurity strategies and enhance their resilience against cascading failures

2.1. Interconnected Systems

Interconnected systems influence each other, where the failure of one component can lead to the failure of others. This interdependence creates a network of risk that can escalate quickly. As systems become more integrated, the potential for systemic failures increases. Cascade cyber effects often originate from the interconnectedness of systems, driven by their interdependency and interoperability. This interdependence creates a network of risk that can escalate quickly. When one system fails, it can trigger failures in other connected systems, amplifying the impact of the initial disruption.

2.2. Shared Vulnerabilities

Interconnected systems may share common vulnerabilities, meaning that a single exploit can compromise multiple systems simultaneously. Identifying shared vulnerabilities is critical for organizations to implement comprehensive security measures. Organizations should collaborate to address these common risks. As demonstrated by the SolarWinds attack in 2020, a single vulnerability in a software provider can compromise multiple organizations. Misconfigurations in shared services, reveal how interconnected systems can amplify risks. Shared vulnerabilities in interconnected systems can lead to cascading effects, as a single exploit can compromise multiple systems simultaneously. Identifying and addressing these common vulnerabilities is crucial for organizations to implement comprehensive security measures and prevent widespread impacts.

2.3. Various Propagation Mechanisms

Risks can propagate through multiple pathways, including data flows, shared resources, and third-party services, making it challenging to predict the full extent of a risk event. Understanding these mechanisms is crucial for developing effective mitigation strategies. Organizations must map out their interdependencies to better anticipate potential propagation paths.

2.4. Feedback Loops

Feedback loops can exacerbate risks, where the effects of a failure may lead to further failures, creating a cycle of cascading impacts. These loops can hinder recovery efforts and prolong the duration of an incident. Recognizing feedback mechanisms is vital in cascade cyber risk management for enhancing resilience in interconnected systems Feedback loops can exacerbate cyber risks by creating a cycle where initial failures lead to further failures, resulting an cascading impacts that hinder recovery efforts and prolong incidents.

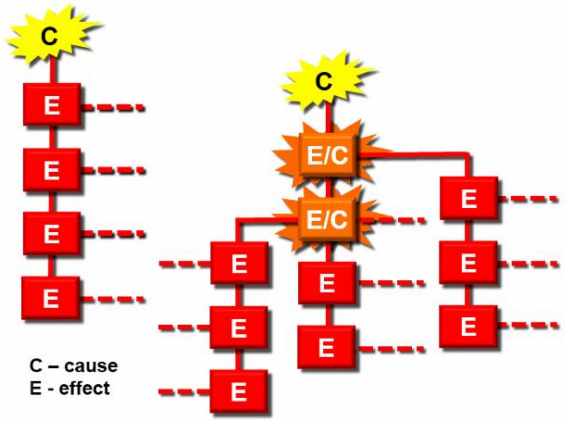

Figure 2. At the left: a linear or domino effect. Cascade risks -at the right- are often non-linear.

2.5. Non-linear Effects

The relationship between system components is often non-linear (see: Figure 2), meaning small failures can lead to disproportionately large impacts, complicating risk assessment and management. Non-linear interactions can amplify risks, leading to unexpected and severe consequences. Effective modeling techniques are essential to understand these dynamics. Non-linear relationships between system components can cause small failures to escalate into disproportionately large impacts, complicating risk assessment and management, and necessitating effective modeling techniques to understand and mitigate these dynamics.

2.6. Delayed Effects

The impacts of a cybersecurity incident may not be immediately apparent, leading to delayed responses that can worsen the situation. Organizations may need to implement more sensitive monitoring systems to detect issues early and respond more effectively. Understanding potential delays is essential for planning incident response strategies. Delayed recognition of cybersecurity incidents can exacerbate cascade risks by hindering timely responses, necessitating the implementation of sensitive monitoring systems to detect issues early and enhance incident response strategies.

2.7. Dependency on Trust

Trust in other components or systems can lead organizations to overlook potential vulnerabilities, increasing the likelihood of cascading failures. Building a culture of skepticism where potential risks are regularly assessed can help organizations mitigate this dependency. Trust must be continuously evaluated in interconnected environments. Dependency on trust in other components or systems can cause organizations to overlook vulnerabilities, increasing the risk of cascading failures, highlighting the need for continuous evaluation and a culture of regular risk assessment.

2.8. Complexity

The complexity of interconnected systems can obscure potential vulnerabilities and make it difficult to identify and address risks effectively. As systems evolve, complexity increases. The complexity of interconnected systems can obscure vulnerabilities and hinder effective risk identification and management, with increasing complexity amplifying these challenges.

2.9. Dynamic Nature

The interconnectedness of systems changes over time, with new integrations and dependencies forming, which can alter the risk landscape. Continuous monitoring and adaptive governance frameworks are necessary to respond to these evolving risks. Organizations must remain agile to address new challenges as they arise. The dynamic nature of interconnected systems, with evolving integrations and dependencies, can alter the risk landscape, necessitating continuous monitoring and adaptive governance to effectively manage emerging risks.

2.10. Invisibility of Risks

Cascade cyber risks may remain hidden until they manifest, making proactive risk management challenging. Organizations should adopt proactive risk assessment techniques to identify potential vulnerabilities before they lead to incidents. Increased transparency can help in recognizing and addressing these invisible risks. The invisibility of cascade cyber risks, which may remain hidden until they manifest, complicates proactive risk management, necessitating the adoption of proactive risk assessment techniques and increased transparency to identify and address potential vulnerabilities.

3. Need for increased vigilance: towards an integrated approach

The interaction effects that occur when vulnerabilities are shared in the context of this set of cascade risks components put an high demand on developing and maintaining shared situation awareness in organisations and society. New risk assessment techniques are needed so as to predict potential future implications of cascade cyber risk. The increased invisibility due to the increase of technology has put society and its critical infrastructure with a need for increased societal resilience to such cascading events (Pescaroli et al, 2015). This holds not only for threats from outside but also for insider threats and -mistakes (Al-Mhiqani, 2024; Ivan, 2024).

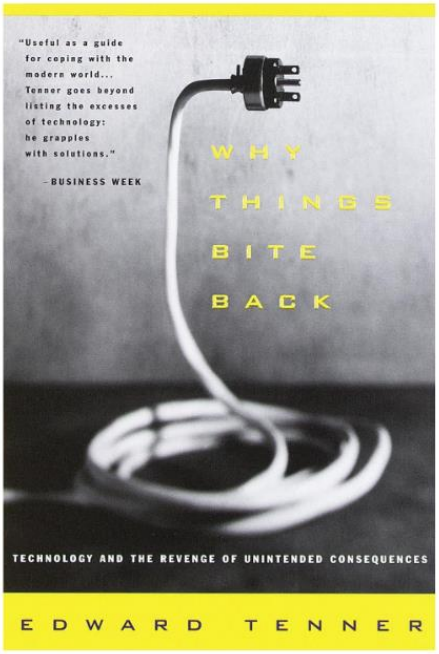

Figure 3. Increasing innovation requires increasing shared vigilance

Edward Tennner (1996) in his book *Why things bite back* argues that technological advances often transform rather than eradicate risk, leading to unforeseen negative consequences that demand increased vigilance and innovative risk assessment to protect society from these chronic and subtle problems. Humans find it complex to imagine the multiple interactions of vulnerabilities that accompany technological innovation. Technological advances often lead to unintended and unforeseen negative consequences. While technology can solve catastrophic risks, it frequently creates more subtle, chronic problems that are harder to predict and solve. Tenner highlights the concept of ‘revenge effects’, where attempts to manage the environment with technology result in unpredictable outcomes. He criticizes regulatory policies for failing to account for such countervailing risks.

"Why Things Bite Back," has been referenced in discussions surrounding technology and cyber risk management. His insights into the unintended consequences of technological innovations, encapsulated in concepts such as the "revenge effect," are particularly relevant in the context of cybersecurity, where new technologies can introduce unforeseen vulnerabilities. Vlijmen (2023) mentions that Tenner's ideas are invoked to illustrate the complexities and complications that arise from rigorous technological interventions. The author notes that Tenner's work elevates the discussion of problem preservation, highlighting how interventions can lead to chronic issues akin to a disease. McDonald et al. (2022) refer to Tenner's notion of technologies that "bite back" in the emphasizing that there is no straightforward solution to the complexities introduced by these innovations. This aligns with the broader implications of Tenner's work, suggesting that the integration of new technologies in any field, including cybersecurity, must be approached with caution and awareness of potential negative outcomes. Ultimately, Tenner calls for sustained vigilance in protecting ourselves from the chronic and subtle problems caused by the increase of technological innovation.

The ongoing relevance of vigilance is increasingly relevant today (see also: Vaughn et al., 2024, Grobler, 2021; Ray, 2013; Liu, 2023).

This heightened vigilance is also evident in the call for integrated approaches to cascade cyber risk management. For example, Jazairy (2024) examined the impact of cascade cyber risk management strategies on integration decisions for cybersecurity with suppliers, customers, and internal processes, aiming to enhance cascade cyber resilience and robustness. Mizrak (2023) highlights the importance of integrating cybersecurity risk management into strategic management, emphasizing the need to align cybersecurity efforts with broader organizational strategies to protect digital assets and infrastructure against evolving cyber threats. Marotta et ak (2018) advocate for a holistic approach to cyber risk management, integrating proactive techniques within the enterprise risk management (ERM) framework. This collaboration across disciplines is essential for addressing the complexities of cyber risks, as highlighted by Panda et al. (2020) who emphasize the need for a solid understanding of disaster risks to improve mitigation efforts. Melaku (2023) suggests incorporating a dynamic and adaptive cybersecurity governance framework to provide strategic direction, ensuring that security risks are managed appropriately and organizational resources are optimized.

There is consensus that cybersecurity risk management should not be viewed as a standalone function; rather, it must be an integral part of the business strategy in the DNA of every organisation across the entire supply chain. Cyber threats do not respect organizational boundaries; a vulnerability in one area can compromise the entire network. Therefore, organizations must collaborate with suppliers, partners, and other stakeholders to ensure a unified response to cascade cyber risks. For a cyber cascade strategy to be effective, it must be embedded in the organizational cultures of the supply chain.

In the realm of cascade cyber risk management, communication is increasingly important and language confusion can significantly hinder effective communication. The next session addresses this and the issue of the so-called ‘Tower of Babel effect.’

5. The ‘Tower of Babel’ effect in cascade cyber risk management

The interconnectedness of systems in cascade cyber risks necessitates a common language and narrative that articulates the organization’s approach to cybersecurity, promoting transparency and cooperation across the supply chain. Increased vigilance and integrated approaches, coupled with effective communication and a shared language among IT, legal, business, and risk management professionals, have become increasingly relevant.

Figure 4. Bruegel’s Tower of Babel

Despite the critical need for a unified approach to cybersecurity, a common language surrounding cascade cybersecurity is often lacking. This absence creates significant barriers to effective communication about cyber risks and mitigation strategies. Without alignment and a shared language, employees at all levels struggle to understand and engage with cybersecurity concepts, leading to misalignments and vulnerabilities. This so called ‘Tower of Babel’ effect in cascade cyber risk management describes the challenges and inefficiencies caused by the use of diverse and often incompatible terminologies, directives,

frameworks, and methodologies among different stakeholders. This fragmentation can result in miscommunication, inconsistent risk assessments, and disjointed mitigation efforts, undermining organizations' ability to effectively manage and respond to cybersecurity threats (Dijkstra, et al 2024; ENISA, 2023b; Roesch, 2023; Cains et al, 2021; Hoppe et al, 2021).

5.1 Need for a common language

Establishing a common language is essential to overcoming the 'Tower of Babel effect', facilitating better understanding and engagement across within and across organizations. The Tower of Babel concept highlights the importance of s communication, shared frameworks, and directives to ensure cohesive and effective cascade risk management across all levels. The Tower of Babel effect can occur in separate organizations, and in cascade cyber risk management, individual confusion can multiply easily as the chain is only as strong as its weakest link. ENISA (2023b) mentions in their report on 'Supply Chain Best Practices' that

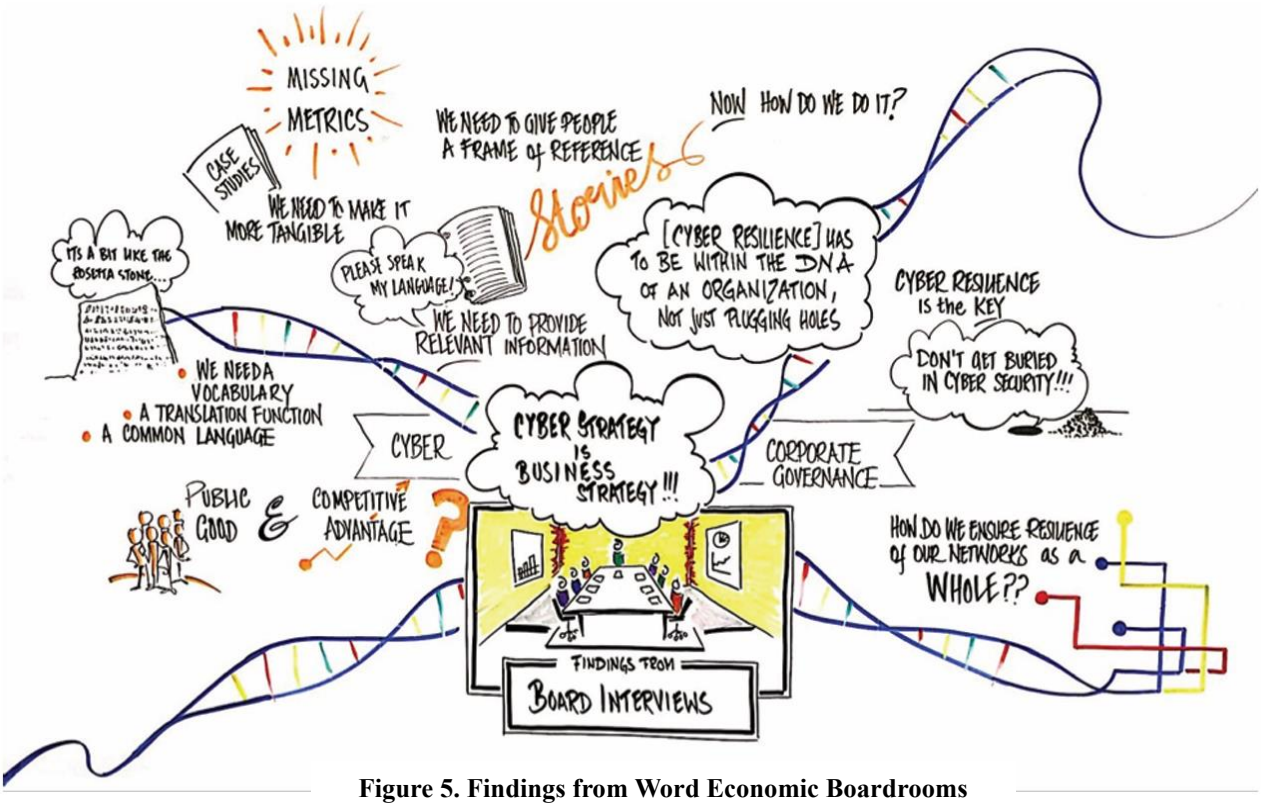

Figure 5. Findings from Word Economic Boardrooms interviews: 'We need a story and a common language'.

misalignment and terminology differences can significantly impact and challenge overall cascade security and resilience.

5.2 The role of leaders and boards

Organisational Leaders and boards bear the responsibility to verify this common organizational language: to simplify complex concepts and use terminology that resonates with all employees, regardless of their technical expertise. This approach not only enhances situational awareness but also empowers employees to contribute meaningfully to the organization's cascade cyber resilience efforts. As organizations navigate the complexities of the digital landscape, integrating cybersecurity into the overall business strategy has become

paramount. By aligning cybersecurity efforts with broader organizational strategies, leaders can ensure that cybersecurity is embedded in the organizational culture and that a common language and narrative will be established and verified (World Economic Forum, 2017).

5.3 The Need for a Common Story

A common story is essential for aligning these efforts toward cascade cyber resilience. This narrative should clearly communicate the organization's vision, priorities, and strategies for addressing cyber threats. By fostering a shared understanding of the risks involved and the collective responsibility for mitigating them, organizations can enhance collaboration among teams and departments. This common story also serves as a foundation for developing effective policies and procedures, ensuring that all stakeholders are on the same page. The leaders and the boards are also responsible for making and telling this common story (World Economic Forum, 2017).

To effectively address this issue, it is essential to identify and catalog the various misalignments and confusions present in cascade risk management. The following section provides a description of five misalignments for cascade cyber risk management.

6. Misalignment between rules and realities in cascade cyber risks

The problem of confusion and misalignment pops up in various domains in the field of cascade cybersecurity. At least five areas can be identified that have a need for a more alignment in this field.

6.1 Rule based versus Risk Based Management in NL and EU

Cyber risk management in the Netherlands and the EU heavily relies on a variety of risk frameworks, leading to confusion due to differing terminologies and definitions. For instance, the term 'risk' can have multiple interpretations, complicating the alignment of cybersecurity measures. Additionally, there can be confusion about what constitutes 'risk appetite' and the level of resilience needed. According to Dijkstra et al. (2024), organizations are still grappling with their cyber risk identity and appetite. The plethora of directives and frameworks, such as NIST, ISO, and ITSRM2, further exacerbates this confusion, often resulting in a checkbox mentality where risk managers focus on forms of rule compliance rather than analysis of actual risks. Dijkstra and Veen suggest adopting a risk-based approach and sharing a cyber risk management roadmap to better align these frameworks with real-world risks.
Alignment is necessary for effective cyber risk management requires coordinated communication across different organizational levels, from CERT/CSIRT teams to senior management, risk owners, supervising bodies, and national cybersecurity authorities. However, there is often a misalignment in information gathering across management teams, leading to isolated efforts and ineffective risk management (Marotta et al, 2018; Talesh, 2018; Kure et al., 2022). The European Union Agency for Cybersecurity (ENISA, 2024) highlights the importance of coordinated communication for shared situational awareness, which is currently underdeveloped.

6.2 Usability versus Cybersecurity

A significant misalignment exists between cybersecurity measures and usability, creating tension between security and user convenience. Users often find complex authentication processes burdensome or even annoying or stressful, leading to frustration and potential security lapses. Research by Furnell (2024) highlights the challenges of making cybersecurity

usable without compromising security. Reuter et al. (2022) emphasize the need for transparency and tailorability in security measures to enhance user acceptance and effectiveness. Grobler et al. (2021) advocate for a human-centric approach to cybersecurity, focusing on user behavior and cognitive perceptions to bridge the gap between security and usability. Alignment here is also necessary. Discrepancies between usability and security can be a source of vulnerabilities for systemic risks.

6.3 Academic Education versus Industry Needs

There is a notable disconnect between cybersecurity education and industry requirements. Current educational programs often fail to equip students with the practical skills needed in the workforce. Yusuf (2024) argues that cybersecurity curricula need to be updated to reflect industry demands, ensuring graduates are job-ready from day one. AlDaajeh et al. (2022; 2024) propose aligning educational programs with national cybersecurity strategies to close the skills gap. Towhidi and Pridmore (2023) suggest a model for designing courses that meet industry needs, emphasizing the importance of practical, hands-on experience. It is crucial to solve this discrepancy in the field. Alignment here is needed. There is a shortage of cascade cyber risk personnel and they should be adequately equipped to perform their mission.

6.4 Misalignments in the Supply Chain Risk Management

ENISA (2023b) identified four categories of frequently occurring organizational misalignments related to supply chain risk management. They highlighted several knowledge gaps and related them to a supply chain risk management cycle. These gaps were categorized into four subsequent areas with ‘to do’ steps, emphasizing the misalignments between theoretical rules and practical realities:

a) Supply Chain Risk Management:
• Understand the supply chain; identify suppliers and providers.
• Understand the potential risks for the organization and for end customers.
Misalignment: Often, organizations fail to fully map their supply chain, leading to gaps in risk identification and management (Sijan et al, 2024).

b) Supply Chain Relationship Management:
• Manage the supply chain; have policies and agreements in place; have cybersecurity requirements defined.
• Monitor supplier and service provider performance; manage changes.
Misalignment: Policies and agreements may exist on paper, but their implementation and enforcement are frequently inconsistent, leaving vulnerabilities unaddressed.

c) Vulnerability Handling:
• Manage vulnerabilities; know your assets; understand risks of vulnerabilities.
• Monitor vulnerabilities; patch vulnerabilities; have a defined maintenance policy.
Misalignment: Despite having vulnerability management processes, many organizations struggle with timely patching and asset management, leading to exploitable gaps.

d) Quality of Products and Services:
• Provide secure products and services; protect the infrastructure; have secure processes in place.
• Implement technical measures; create transparency in the supply chain; measure the quality of products and services.
Misalignment: The quality and security of products and services often fall short of standards due to inadequate technical measures and lack of transparency in the supply chain.

6.5 Misalignment of theoretical frameworks and empirical based scientific research

Hubbard (2020) and Cremer et al. (2022) argue that traditional risk management methods and frameworks fail primarily due to their reliance on qualitative assessments and lack of quantitative empirical evidence. Quantitative empirical approaches are needed to adapt to the dynamic nature of cascade cyber threats, where these shortcomings are particularly pronounced (Colicchia et al, 2019; Pandey et al, 2020; Welburn et al, 2021). Cascade cyber risk research often relies on ex post facto data, collected after an incident has occurred. What is needed is comprehensive data collection throughout the supply chain—before, during, and after cyber incidents).

There is also a misalignment in the understanding of what constitutes data. For scientific purposes, quantitative data should be measurable, repeatable, and accessible. Addressing these misalignments between theoretical frameworks and empirical data collection requires a concerted effort to continuously evaluate and improve cybersecurity practices based on empirical systemic data.

For example, it is crucial to predict, based on data, which companies within a supply chain are likely to be attacked when a supplier within the chain is compromised. This predictive capability would allow for better preparation and response strategies, enhancing the overall resilience of the supply chain against cascade cyber threats. The literature consistently emphasizes that effective cascade cyber risk management should be based on empirical data. The current body of research reveals a dearth of empirical evidence in cybersecurity risk management, highlighting the need for further studies to inform best practices and enhance organizational resilience against cyber threats.

In summary, the current state of cascade cyber risk management highlights several key issues: 1) the need for increased vigilance against cascade threats, 2) confusion and misalignment across multiple domains in this field, and 3) a lack of empirical data.

Sections 7 and 8 will address these challenges by providing solutions for the five identified misalignments. In Section 7, we introduce the theory of the computational shared mental model, which facilitates AI-based risk assessments of cascade risks. Section 8 outlines the research methodology of the Living Lab approach, enabling comprehensive data collection for cascade cyber risks.

7. Computational shared mental models for cascade cyber risk management

One way to address the misalignment and the concomitant ‘Tower of Babel’ effect is by using the theory of shared mental models. The mental model approach has been applied to the field of cybersecurity for over a decade (Murimi, 2023), and the need for such adaptive dynamic modeling has been highlighted by several researchers (see also: Melaku, 2023). A computational approach suitable for modeling mental processes involving internal mental models was developed by Treur (2020). Recently, Roelofsma et al. (2024) applied this approach to shared cyber risk management. What follows is a brief description of the shared mental models approach and how it is being applied to computational cascade risk management.

7.1 Shared Mental Models

Kenneth Craik (1943) introduced the concept of mental models, describing them as an organism’s internal representations of the external world that help the organism navigate their environment. He emphasized that these models allow individuals to simulate various

scenarios and pathways, use past experiences to inform present decisions, and respond more effectively to challenges.

Mental models are not static; they are dynamic and can evolve over time. They consist of relational structures that mirror real-world processes. This understanding leads to the idea that mental models can be represented in network forms, where relationships between elements can be studied in terms of network connections that can change over time.

Research indicates that mental models play a crucial role in various cognitive processes, such as planning, reasoning, and adaptation through learning and forgetting. A shared team mental model is vital for high-performing teams, enhancing their ability to coordinate and execute complex tasks. These models help align individual understandings among team members, ultimately improving collaboration and efficiency.

7.2 Organizational Learning

From a socio-cognitive perspective, learning begins with individuals who adjust their mental models in response to new experiences. This adjustment can be shared with others, e.g. through discussions, gaming, or other social interaction leading to collective learning. Once established, this learning becomes embedded in organizational routines, allowing it to persist even after individuals leave.

Organizational learning is not merely a collection of individual learnings; it is a dynamic process that involves multiple levels—individual, team, and organization, society. Feedback loops enable the organization to learn from individuals and vice versa, enhancing overall adaptability.

Recent computational modeling approaches have been developed to analyze these learning processes, considering factors like organizational culture and leadership. These models contribute to understanding how organizations can foster an environment of continuous learning and adaptation (Canbaloğlu et al, 2022; 2024).

7.3 Network Modeling of Complex and Dynamic Systems

The complexity of mental models and organizational learning presents challenges for computational modeling. However, higher-order adaptive dynamical systems can be utilized to create effective models. These systems can be represented as networks that capture relationships between states and their dynamics.

Adaptive network models allow for changes in both the network's states and its characteristics, enabling more realistic representations of learning and forgetting processes. This adaptive network perspective supports better understanding and modeling of how organizations learn and adapt over time (Treur, 2020; Roelofsma, et al 2024).

The interplay between shared mental models and organizational learning is crucial for effective teamwork and adaptability in complex dynamic organizational environments. Understanding and modeling these concepts can enhance both individual and collective performance within organizations.

7.4 Network Oriented Modeling and cascade risk assessment

The method of adaptive network-oriented modeling described by Mestour et al. (2024) addresses cascade cyber risk management by simulating and analyzing cascade cyber threats.

This approach not only provides insight into potential systemic vulnerabilities that enhance cascade cyber threats but also enhances an organization's capacity to adapt to and mitigate cyber risks more systematically through What-If analysis. This work sheds light on the dynamic and adaptive interactions between attackers and defenders, illustrating how threats can evolve and escalate. The results of this study highlight the importance of continuous learning and adaptation in cybersecurity strategies. Organizations must not only implement strong defenses but also develop mechanisms to anticipate and counteract evolving threats effectively.

The What-If analysis evaluates various cascade cyber-attack scenarios and their potential impacts on an organization's security posture. It is often difficult for individuals to assess the consequences of interactions of vulnerabilities in a cascade chain. Using AI techniques, as done by Mestour et al, to support this is a powerful way to assess potential future consequences under different contextual characteristics.

The adaptive network modeling approach allows for systematic examinations of critical variables, termed 'If' factors, that can significantly influence the outcomes of cyber incidents. Complementing the What-If analysis, risk assessment quantifies the likelihood of each scenario. The adaptive network model presented in this study offers a comprehensive approach to understanding and managing cascade cyber risks in institutions.
The computational network-oriented modeling for cyber risk management problems appears to be very promising. This is substantiated by research addressing a wide variety of cyber risk management decision problems using this method in domains like: the health domain, decisions for government and municipality, air traffic control, NATO and war time decisions, financial institutions, insider threats, password authentication, AI-coaching and bio-hacking etc. (Abromaitytė et al, 2024, Akers, et al, 2024 D; Bart et al, 2024; Bell, et al., 2024; Börcsök, et al., 2024; Bouma, et al, 2024a; Bouma, et al, 2024b; Caneva, J. et al, 2024l; Capră, et al, 2024; Daza, et al., 2024; Erdogan, et al., 2024; Hoffmans, et al, 2024; Ivan, et al., 2024; Jeffery, et al., 2024; Keijzer, et al,. 2024; Van den Hout, et al, 2024; Dragosin, et al., 2024; de Jong, R. et al., 2024; Belkuyu, et al., 2024; Lepădatu, et al, 2024; Babayusuf, Y. et al., 2024).

However, one additional factor is also critically crucial. This is the collection of real time data in cyber risk management situations. The field of cascade cybersecurity is sometimes characterized as one with many frameworks, but no data. The research method to address this factor too is described in the next session.

8. Addressing Misalignment: in The Cybersecurity Living Lab (CSyLL) Method

The Cybersecurity Living Lab (CSyLL, pronounced 'CHILL') Initiative addresses the need to increase alignment in cybersecurity that is addressed above. The misalignment as described among governmental authorities, businesses, academia, and society is addressed by leveraging the Quadruple Helix framework (Carayannis et al., 2009, 2012, see Figure 6)) in a so-called Living Lab. A Living Lab is a

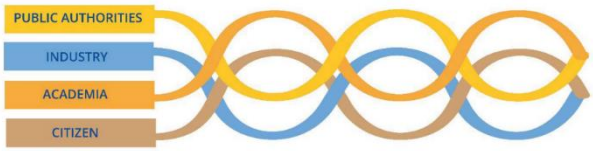

Figure 6. The Quadruple Helix

research method for co-creating and co-designing complex systems. The observed five misalignments in cascade cybersecurity can be resolved through a process of co-designing resilient security pathways with representatives from these stakeholders (Lupp, 2021; Roelofsma et al., 2024). The misalignments described in section 6 occur within and between these stakeholder groups. By bringing these groups together and initiating mutual interaction and co-creation, a process of alignment can evolve. The literature also indicates that the Quadruple Helix model can enhance corporate social responsibility (CSR) initiatives, as discussed by Akmalluddin (2023). The collaboration among government, industry, academia, and society under this model can lead to innovative solutions that address societal needs, including those related to cybersecurity. This collaborative approach is essential in developing comprehensive strategies that can effectively mitigate cyber risks.

The Living Lab method involves an adaptive knowledge-sharing process to foster collaboration and innovation, ensuring that each sector's unique perspectives and expertise contribute to comprehensive cybersecurity solutions. The concept of the Quadruple Helix was developed to enhance the understanding of innovation systems by incorporating four key stakeholders: academia, industry, government, and civil society. It addresses the issue of knowledge circulation and adaptation among these four stakeholder groups.

Additionally, CSyLL aims to establish a comprehensive environment that integrates a Security Operations Center (SOC) and Security Information and Event Management (SIEM) setting where such data collection and analysis of them can take place. This provides real-time monitoring of cybsersecurity of a cascade cyber chain. This SOC will enhance the ability to detect, respond to, and mitigate cyber threats as they occur, further strengthening the cybersecurity posture of all involved stakeholders. The SOC will be build and led by students as part and innovative education programs will be developed.

As mentioned in the section of misalignment, there is a notable observed lack of empirical data in the field of cybersecurity science. The Living Lab approach addresses this gap by providing a real-world environment where data can be collected and analyzed, before, during and after incidents in a supply chain. Such empirical data are crucial for developing evidence-based strategies and solutions, enhancing the overall effectiveness and reliability of cybersecurity practices in cascade cybersecurity risks management.

8.1. Cybersecurity Living Lab Initiative

This initiative prioritizes the end user, facilitating the development of practical applications and knowledge transfer. The Living Lab serves as an open experimental and learning environment where cybersecurity organizations, academic institutions, government entities, and businesses collaborate to find realistic data based solutions to pressing societal and geopolitical issues, particularly in enhancing resilience against cyber threats and managing associated risks amid increasing digital dependency.

8.2 Objectives and Opportunities

Another key objective of the Cybersecurity Living Lab is to accelerate the development of the cybersecurity market, which currently faces challenges such as advanced threats, regulatory pressures, and a shortage of skilled professionals. Organizations across various sectors seek individuals with practical experience in cybersecurity risk management and SOC operations to strengthen their security posture. The Netherlands, with its large base of early adopters, presents significant economic opportunities in this sector. The Living Lab aims to connect

educational, businesses, related organizations, and cybersecurity institutions to leverage these opportunities.

8.3 Integrating Practical Cybersecurity Principles

The initiative represents a vital effort to integrate practical cascade cybersecurity risk management principles with real-time threat monitoring, incident response capabilities, and innovative research and development. The Lab will thus focus on developing the SOC of the future, combining risk management methodologies with SOC activities within an educational framework. This approach will provide students and researchers with invaluable hands-on experience while addressing the growing demand for skilled cybersecurity professionals.

8.4 Social Network Governance and Life Cycle Approach

Governance of this process , as described by Imperial et al. (2016; Peris-Ortiz, 2016) is crucial for the success of the Cybersecurity Living Lab. Living Labs have life cycles, the concept of a 'healthy and useful life cycle' underscores the constant nurturing required by the stakeholders processes.

Key aspects of this social network governance approach include:
Attracting Suitable Members: Social networks need to attract members who represent their respective organizations and participate on their behalf.
Providing Space, Flexibility, and Time: Politicians, managers, and funders should give networks the space, flexibility, and time needed for network processes to develop at their own pace.
Institutionalizing Social Relationships: The ability of a network to survive for a long period requires institutionalizing the social relationships upon which that network is founded.
Recognizing the End of a Functional Life Cycle: It is important to recognize when a network has come to the end of its functional life cycle and to redeploy network resources to more productive public purposes.

8.5. Shared Mental Models and Organizational Learning

The Living Lab approach links to the development of shared mental models and organizational learning, which are crucial for effective collaboration and innovation. Integrating these elements into the Living Lab's operations can enhance its effectiveness and sustainability. Recent research by Roelofsma, Jabeen, Taal, and Treur (2024) further supports the need for shared mental models and organizational learning in fostering successful innovation ecosystems. The Living Lab Approach will integrate the Quadruple Helix, and Network Governance theory with the Shared Mental Models Theory and Organizational Learning Theory. These theories will be examined to understand how they can support collaboration and knowledge sharing among stakeholders. By fostering shared understanding and continuous learning, the Lab aims to enhance the effectiveness of its collaborative efforts.

8.6. In Sum: The specific key objectives of the Cybersecurity Living Lab

Data collection: Collect data for empirical based cascade risk management.
Co-creation: Co-create and co-design cascade pathways with multiple stakeholders.
Integrated Learning Experience: Provide students with insights into cybersecurity risk management principles, threat detection, incident response, and mitigation strategies within SOC operations.
Practical Skill Development: Equip students with hands-on experience using risk management frameworks, security tools, and techniques for assessing, monitoring, and responding to cybersecurity threats and incidents.

Applied Research Opportunities: Facilitate research collaborations among students, faculty, and industry partners to explore innovative approaches and enhance cybersecurity methodologies.
Continuous Development and Validation: Ensure ongoing verification and validation of new system innovations.
Creation of a Learning Community: Foster a community for cybersecurity professionals to share knowledge and experiences.
Industry Alignment: Ensure that the Living Lab SOC curriculum aligns with industry standards, legal requirements, and emerging trends.

8.7 Research in CSyLL

The Research of CSyLL will be organized along the following three avenues.

1. Platform Shared Cyber Security Risk Management
The Platform for Shared Cybersecurity Risk Management aims to create a collaborative network of organizations focused on innovative cybersecurity solutions. This initiative seeks to bridge the gap between companies offering cybersecurity technologies and those in need of them, fostering new market opportunities. A major challenge in this field is transitioning from pilot projects to widespread implementation, compounded by a lack of awareness among end-users. The platform will feature an AI Dashboard, enhancing education on NIS2 directives and shared risk management, and will work closely with various stakeholders, including educational institutions and municipal services, to bolster innovation in cybersecurity. Using the platform workshops will be held to solve the various misalignments as described earlier and to co-create cybersecurity in the cascade pathway

2. Cyber Security Living Lab SOC/SIEM
The SOC/SIEM Living Lab Environment is designed to develop, test, and validate new cybersecurity solutions while ensuring they meet user needs. By collaborating with cybersecurity companies and educational institutions, this initiative will establish a user-centered approach to designing future Security Operations Centers (SOCs). Research will focus on understanding user requirements through co-creation workshops and enhancing situational awareness using data integration and predictive analytics. Additionally, the initiative will analyze naturalistic decision-making processes within SOCs to improve decision-making frameworks and address biases and motivational issues that may hinder effective cybersecurity responses. It will examine the role of various decision support techniques, team situation awareness, the role of AI, serious gaming and examine how usability and security can meet. The SOC/SIEM will also address how shared threat intelligence can be achieved through a cascadic chain pathway.

3. Innovation in Cyber Security Risk Management Education
The Innovation of Cybersecurity Education work package aims to align educational frameworks with the rapid advancements in cybersecurity. It addresses significant gaps in current educational programs, which often lack relevance due to their static nature. The initiative will promote iterative educational approaches that continually update curricula and make cyber risk management accessible at various educational levels. By integrating artificial intelligence and focusing on the interactions among humans, organizations, and technology, this work package seeks to develop interdisciplinary curricula that equip students with the

skills necessary to thrive in an evolving cybersecurity landscape. A more detailed description of the research program is presented in section 10.

9. **A narrative of change for cascade cyber risk management**

In an age where cyber threats loom larger than ever, organizations are beginning to realize a fundamental truth: no entity can achieve true cyber resilience in isolation. The interconnected nature of our digital world means that a single vulnerability can lead to cascade cyber risks, where one breach triggers a series of subsequent failures across systems, networks and sectors. The ever-evolving landscape of cybersecurity is a complex tapestry woven from the threads of collaboration, shared understanding, and collective action. Just as the people of Babel embarked on a monumental engineering project, we too must undertake a societal transition towards enhanced cybersecurity. Yet, this journey requires a narrative of change, towards a new mindset, one that is framed positively and embraced by all involved.

The story of the Tower of Babel, as recounted in Genesis 11, serves as a poignant reminder of the consequences of division and ambition unmoored from shared responsibility. The people of Babel, united in language and purpose, set out to build the first large engineering project of mankind- a great city with a tower that reached the heavens. Their ambition was clear: to make a name for themselves and avoid being scattered across the earth. However, their desire for fame overshadowed the communal goal of global risk management for safety and security on the planet. In their quest for greatness, they forgot the fundamental principle that true achievement lies in collaboration rather than competition, a principle that is crucial in mitigating cascade cyber risks.

As they toiled together, they spoke the same language, and the possibilities seemed endless. ‘With unity’, they correctly believed, ‘nothing we set out to do will be impossible’. Yet, the moment their egocentric ambitions took precedence, confusion and misalignment ensued. An ‘act of God’ intervened, scattering them and instilling a multitude of languages that created barriers rather than bridges. The tower, a symbol of their collective aspiration, remained unfinished, a lasting testament to the perils of division.

In our contemporary context, the lesson from Babel rings clear: when organizations prioritize individual accolades over collective responsibility, confusion and fragmentation are bound to follow. Cascade cyber risk management is not merely a technical challenge, it is a societal one. We must foster an adaptive shared mental model that transcends organizational boundaries. When we unite and communicate effectively, we can build resilient systems capable of withstanding the most nefarious cyber threats and mitigating cascade cyber risks.

To cultivate this environment of collaboration, we must frame our change management strategies in a positive light. People inherently desire to be part of the solution, but they need to feel empowered rather than coerced. This means creating a culture where individuals understand their role in the larger narrative of cyber resilience —where each contribution is valued and recognized as part of a collective effort. The path to cyber resilience is not solely the responsibility of IT departments or security teams; it is a shared journey that involves every member of an organization and, indeed, every organization within a community, and indeed every individual in society. By encouraging open dialogue, fostering trust, and promoting a sense of shared purpose, we can create an ecosystem where everyone understands the language of resilient security and the importance of addressing cascade cyber risks.

Just as the builders of Babel failed to finish their ambitious project due to division, organizations today risk leaving their cybersecurity initiatives unfinished if they do not

embrace a collaborative mindset. By reflecting on the lessons of Babel, we can commit to a narrative of change that champions unity over ego, collaboration over competition, and shared responsibility over individual ambition. In cascade cyber risk management, we must align rules with reality, ensuring that our strategies are practical and grounded in the real-world dynamics of cybersecurity. When we come together, united in purpose and language, we can transform the cybersecurity landscape into one that is resilient and robust. The challenge is great, but with this collective mindset, we can ensure that our tower—our efforts in cybersecurity—rises high, completed and fortified against the storms of the digital age.

10 Annex: Research program of the lectorate Risk Management & Cybersecurity

The Research Activities in the Cybersecurity Living Lab will be organized in the following three workpackages (WP's):

1. Platform: Shared Cybersecurity Risk Management -WP1-
2. The SOC/SIEM Living Lab Environment -WP2-
3. Innovation of Cybersecurity Education -WP3-

The WP's are described below.

10.1. WP1: Platform for Shared Cybersecurity Risk Management

Aim: The objective of this work package is to establish a network of engaged organizations focused on the development and implementation of innovations in cybersecurity. This initiative aims to connect companies offering solutions with those seeking them, which is critical for the development of new markets. Innovative enterprises often lack adequate connections to institutions. The platform collaborates closely with the DIF Community and relevant stakeholders (Dutch Innovation Factory) addressing similar issues in cybersecurity risk management.

Description: A significant challenge in cybersecurity risk management innovation is the transition from pilot projects to large-scale implementation. Additionally, insufficient awareness among cybersecurity end-users limits the utilization of available solutions. The Cybersecurity Shared Risk Management platform aims to unite all parties within the network in an open environment.

An AI Dashboard will be developed where, through interaction with an AI coach, organizations can learn about NIS2 and Shared Cyber Risk Management.
The platform to be established under this project will be further enhanced by initiatives from the Labor Market and Education Platform and Regional Initiatives. Based on the Cybersecurity Risk Management platform and existing networks, a broad initiative will be launched aimed at fostering innovation in cybersecurity in its broadest sense.

Participants: The initiative involves cybersecurity organizations, educational institutions (such as MBO Rijnland and The Hague University of Applied Sciences), networks for businesses (DIF), municipal services (Municipality of Zoetermeer), and other networks in various regions).

Activities: To facilitate interaction among the parties within the platform, several distinct activities will be organized:

10.1.1 Knowledge Sharing, Cybersecurity workplace and Aligning Workshops

Conferences and workshops: Conferences and workshops will be held annually to discuss results and experiences from the Cybersecurity Living Lab project. The target audiences for these events include decision-makers and policymakers from cybersecurity organizations, ICT, and educational institutions.
Communities of Practice: Several communities of practice will be established focusing on specific subtopics in the cybersecurity workplace of the Living Lab. The communities will primarily engage frontline cybersecurity personnel, serving as critical sources for determining priorities and approaches, as well as platforms for practical knowledge dissemination. In addition to conferences, activities may include company visits, workshops, and study trips.
Stakeholder Consultation: A stakeholder consultation group will be formed, comprising leaders from the involved parties. This group will play a significant role in prioritizing pilot projects and scaling successful initiatives.
Collaborative Aligning Workshops Meetings: Regular exchange meetings will be organized to align knowledge development, project execution, business, and educational aspects among initiatives in the field.
Engagement with Businesses: To strengthen relationships with companies, collaborations will be established with specific networks. These engagements will involve establishing Cybersecurity Risk Management projects alongside the Cybersecurity Living Lab and affiliated institutions.

10.1.2. Comparative Study on Cascade Cybersecurity Risk Management

Aims: The aim of this project is to evaluate how EU directives on risk management and cascade supply chain management are implemented and performed in different EU countries, with a specific focus on the Netherlands. These directives are the so called NIS2 directives and active since October 2024.

Identify Best Practices: Identify best practices and lessons learned from various countries' approaches to NIS2 implementation.

Apply Theoretical Frameworks: Examine the extent to which Shared Mental Models and Organizational Learning theories can be applied to improve cybersecurity governance.

Facilitate Knowledge Sharing: Use the Cybersecurity Living Lab to facilitate a hybrid conference for stakeholders to co-create, evaluate, and collaborate on cybersecurity risk management strategies.

Focus on Cascade Risks and Supply Chains: Investigate how cyber risk management practices address cascade risks and supply chain vulnerabilities.

Description: This research line focuses on a comparative study of cybersecurity risk management governance concerning the NIS2 directive. The study aims to examine how NIS2 is implemented in the Netherlands and across the EU, identifying lessons that countries can learn from each other. It will also explore the application of the theory of Shared Mental Models and Organizational Learning in this context. The research will leverage the

Cybersecurity Living Lab to facilitate a hybrid conference for co-creation, evaluation, and collaboration among stakeholders. A particular focus will be on cyber risk management, cascade risks, and supply chain security.

Research Questions:

1. Cascade Risks and Supply Chains

How do current cyber risk management practices address cascade risks within supply chains? What strategies can be developed to mitigate supply chain vulnerabilities in the context of NIS2 implementation? How is the NIS2 directive implemented in the Netherlands compared to other EU countries with regard to this? What are the key differences and similarities in the implementation strategies of NIS2 across the EU?

2. Best Practices and Lessons Learned

What best practices can be identified from the implementation of NIS2 in different countries? What lessons can countries learn from each other to enhance their cybersecurity risk management governance?

3. Theoretical Application

How can the theory of Shared Mental Models be applied to improve the implementation of NIS2? To what extent can Organizational Learning theories enhance the effectiveness of cybersecurity governance under NIS2?

4. Knowledge Sharing and Collaboration

How can the Cybersecurity Living Lab facilitate effective knowledge sharing and collaboration among stakeholders? What are the outcomes of the hybrid conferences and workshops in terms of co-creation and evaluation of cybersecurity strategies?

10.2. WP2: The SOC/SIEM Living Lab Environment

In Work Package 2 (WP2), a Cybersecurity Living Lab environment is established to design, develop, test, validate, and train new solutions for cybersecurity risk management. A critical aspect of this initiative is ensuring user acceptance of these solutions. By practicing in a real-life work environment, suppliers, users, and clients can assess the efficacy of these solutions, thereby facilitating potential scalability.

In collaboration with several cybersecurity companies like, Pinewood Consulting, Infinity IT, MBO Rijnland, the Hague University of Applied Sciences (THUAS) , and other organisations, a generic Cybersecurity Living Lab methodology will be developed and implemented. This methodology will address questions like: ‘What is the optimal Security Operations Center (SOC) of the future?’ This inquiry will also explore the future roles of the Chief Information Security Officer (CISO) and the communication dynamics among various cybersecurity decision-making echelons, such as Computer Security Incident Response Teams (CSIRT), crisis teams, and responsible authorities. The objective is to create a testbed focused on the development and evaluation of technology from various companies. The SOC/SIEM is aim to share intelligence with other SOC’S and form a so called, federated or shared SOC.

The following research activities will be jointly developed:

10.2.1 User analysis and co-creation in cybersecurity, establishing user requirements for future Security Operations Centers (SOC/SIEM).

Aims: The primary aim of this research is to develop a documented set of methods and techniques for determining user requirements for the future Cybersecurity Living Lab's Security Operations Center (SOC/SIEM).

This study emphasizes a user-centered approach, focusing on qualitative needs analysis to inform the design and functionality of the Cybersecurity Living Lab environment. By engaging potential users through co-creation workshops, the research aims to ensure that cybersecurity risk management offerings align closely with user needs (Grober et al, 2021; Moustafa et al, 2021).

Research Questions:
1. What qualitative user requirements can be identified for the Cybersecurity Living Lab SOC based on user-driven analysis?
2. How can co-creation workshops effectively involve potential users in the development of cybersecurity solutions?
3. In what ways can the tension between usability and cybersecurity be addressed in the design of cybersecurity tools and processes?
4. To what extent can the application of the theory of shared mental models facilitate better alignment between user needs and cybersecurity solutions?

Description: This research focuses on conducting a qualitative needs analysis from the user perspective to inform the setup of the Cybersecurity Living Lab environment. Moving away from a technology-driven approach, the study prioritizes understanding user requirements and preferences (Jeong et al, 2021). Through co-creation workshops, potential users will be actively involved in shaping the cybersecurity risk management offerings to ensure they meet real-world demands. Collaboration with other knowledge institutions will further enhance the analysis of needs, particularly concerning authentication challenges within cybersecurity contexts (Liaropoulos et al, 2021). An iterative process will guide the development of concepts and prototypes, allowing for mid-course adjustments based on user feedback. A critical aspect of this research is exploring how the interplay between usability and cybersecurity can be resolved, alongside investigating the potential contributions of shared mental models to support effective user engagement and solution development. This study aims to contribute valuable insights into designing more user-centric cybersecurity systems and practices.

10.2.2 Enhancing Shared Threat Intelligence and Shared Situational Awareness through Data Integration and Predictive Analytics

Aims: The primary aim of this research is to propose innovative strategies for research and development (R&D) and technological advancements in Security Operations Centers (SOCs) and Security Information and Event Management (SIEM) systems. This research line seeks to explore how organisational situational awareness can be improved by analyzing and integrating a wider range of data sources, including the potential to incorporate data from other SOCs (Brilingaitė et al, 2022; Haastrecht et al, 2021; Houtamaki, 2021; Mohd Kassim et al., 2022; Dykstra et al, 2023). Ultimately, the goal is to leverage empirical scientific data to

facilitate proactive shared information gathering prior to and after cyber incidents, enabling more accurate predictions of resilient security pathways within cybersecurity chains.

Research Questions:

1. How can the integration and analysis of diverse data sources enhance organisational situational awareness in SOC/SIEM environments?
2. What specific types of additional data sources can be incorporated into existing SOC/SIEM infrastructures to improve predictive analytics?
3. How can data sharing between different SOCs be effectively implemented to enhance the analytical capabilities of individual centers?
4. To what extent can empirical data be utilized to establish cause-and-effect relationships in cybersecurity incidents, moving beyond the limitations of ex post facto data?
5. What biases currently affect predictive analytics in cybersecurity, and how can these biases be addressed to improve the reliability of predictions regarding resilience and security?
6. How can the theory of shared mental models and organizational learning support the development of more effective predictive frameworks in cybersecurity?

Description: This research will investigate the potential for enhancing organisational situational awareness within SOCs through the improved analysis and integration of a broader array of data sources. By examining the effectiveness of incorporating additional types of data and facilitating collaboration between SOCs, the study aims to develop methodologies that allow for proactive and predictive assessments of cybersecurity incidents (Saeed, et al 2023; Ofte, 2024; Jacobseon et al, 2023).

Currently, reliance on retrospective (ex post facto) data limits the ability to establish causal relationships between events. This research will address the inherent biases in existing data analysis methods—including historical biases, timing of data collection, and selection biases—aiming to enhance the predictive accuracy regarding resilience and security in cybersecurity chains.

Furthermore, the research will explore how the theories of shared mental models and organizational learning can contribute to the development of effective predictive frameworks, thereby improving situational awareness and overall security posture within SOCs. The findings are expected to provide valuable insights into the role of data integration and collaborative practices in advancing cybersecurity readiness and response strategies (Roelofsma, et al, 2024; Zhang. 2022).

10.2. 3. Naturalistic Decision-Making Processes in Security Operations Centers and Cyber Decision Echelons

Aims: The primary aim of this research line is to describe and analyze the naturalistic decision-making processes within Security Operations Centers (SOCs) and the various decision echelons of cybersecurity, including CZERT-CSIRT, CERT/CSIRT, temporary crisis teams, senior management, risk owners, supervising bodies, and national cybersecurity authorities. The research will focus on assessing the descriptive validity of existing cyber risk management frameworks and investigating the discrepancies between established protocols and real-world practices. Additionally, the proposal seeks to establish monitoring and attack (blue and purple teaming) initiatives, micro-experiments, and experimental intervention studies to enhance decision-making processes in cybersecurity (Saeed, et al 2023; Ofte, 2024; Jacobseon et al, 2023).

Research Questions:

1. What are the characteristics and dynamics of naturalistic decision-making processes within SOCs and related cybersecurity echelons, and how can shared mental models and organizational learning enhance these processes, particularly in high-stress situations?
2. How can the integration and analysis of diverse data sources, including AI-driven network-oriented modeling, enhance organisational situational awareness and predictive analytics in SOCs, and how do risk perception and risk appetite influence these processes?
3. How valid are existing frameworks for cyber risk management when assessed against observed decision-making practices in SOCs, and what cognitive and motivational biases affect these practices?
4. How can de-biasing and decision support techniques, including AI coaching, be effectively developed and tested to improve decision-making in cybersecurity, and to what extent do variations in team situational awareness correlate with differences in the effectiveness and efficiency of cyber risk management?

Description: This research will investigate the processes and frameworks governing decision-making in SOCs, emphasizing a naturalistic approach. By employing observational studies blue and purple teaming methodologies, the research will explore how cyber risk management models can be validated against real-world decision-making scenarios.

The impact of various attack simulations on SOC decision-making will be analyzed, with a focus on identifying cognitive and motivational biases that may hinder effective responses. Furthermore, the research will develop and test various de-biasing techniques and decision support tools to enhance the quality of decisions made in cybersecurity contexts.

Additionally, the project will examine the concept of distributed decision-making and team situational awareness, investigating how differences in awareness levels affect the overall efficiency and effectiveness of cyber risk management strategies. The integration of AI coaching to facilitate improved decision-making and increase organizational resilience will also be a key focus.

An important aspect of this research will be to assess how adaptive shared mental models among team members can foster better communication, enhance situational awareness, and support collaborative decision-making in SOCs. Furthermore, the role of organizational learning in adapting and refining decision-making processes based on past experiences will be explored, aiming to establish a framework that integrates these concepts into the operational practices of SOCs.

The research will also delve into how risk perception and risk appetite influence decision-making processes within SOCs. Understanding these factors will help in developing strategies that align risk management practices with the organization's overall risk tolerance and capacity.

10.2.4. Evaluating Knowledge Transfer in Cybersecurity War Games: Predictive Validity and Human Performance Measures

Aims: The primary aim of this research is to develop and validate cybersecurity war games for training, research, and personnel selection. This study focuses on identifying relevant human performance measures within these war games and examining their predictive validity concerning real-life decision-making processes in Security Operations Centers (SOCs). By leveraging insights from AI applications in cybersecurity risk management and naturalistic decision-making in command and control environments, this research seeks to enhance our understanding of how training and simulation impact the operational effectiveness of

cybersecurity professionals (Ben-Asher et al, 2015; Mouhmouh, et al, 2023; Romano, 2024; Sullivan et al, 2018).

Research questions:

1. Cybersecurity Risk Management Training

How effective are cybersecurity war games in enhancing the decision-making skills of participants in Security Operations Centers (SOCs)? What specific human performance measures can be identified within cybersecurity war games that predict successful real-life cybersecurity risk management? How do AI applications in cybersecurity war games influence the training outcomes for cybersecurity professionals?

2. Cybersecurity War Games

What is the predictive validity of human performance measures identified in cybersecurity war games concerning real-life SOC operations? How can naturalistic decision-making models be integrated into cybersecurity war games to improve their realism and effectiveness?

What are the key factors that contribute to the successful transfer of knowledge from cybersecurity war games to actual SOC environments?

3. Personnel Selection in Cybersecurity

How can cybersecurity war games be utilized as a tool for selecting personnel for SOC roles? What are the correlations between performance in cybersecurity war games and subsequent job performance in SOC positions? How can the insights gained from cybersecurity war games be applied to develop better criteria for personnel selection in cybersecurity roles?

Description: This research line focuses on developing and validating cybersecurity war games for training, research, and personnel selection. It aims to identify relevant human performance measures within these war games and examine their predictive validity concerning real-life decision-making in Security Operations Centers (SOCs). By leveraging AI applications and naturalistic decision-making models, the study seeks to enhance the operational effectiveness of cybersecurity professionals. Additionally, it addresses the lack of empirical data in cybersecurity science by providing a real-world environment for data collection and analysis. The ultimate goal is to improve training programs, develop better personnel selection criteria, and advance research in cybersecurity risk management.

10.3. WP3: Innovation of Cybersecurity Education

Aim: The objective of this work package is to integrate cybersecurity into educational frameworks while aligning with advancements in industry, government, academia, and society. Despite progress, significant gaps remain in cybersecurity education. Current programs often fail to address the necessary skill sets, as many training topics do not sufficiently account for the rapid evolution of cybersecurity capabilities. This creates a disconnect with training programs that are fixed over four-year periods (Mukherjee, 2024).

Research Questions:

1. How is knowledge transfer achieved between cybersecurity education and practical application?
2. How can this process be improved?

3. Can artificial intelligence (AI) play a supportive role in enhancing cybersecurity education and its practical application?

Description: The following challenges are addressed in this work package

1. **Iterative Educational Approaches:** Develop a more iterative approach to education that incorporates emerging developments in cybersecurity. This involves continuously updating curricula to reflect the evolving landscape of the field. The need for dynamic and responsive educational frameworks is critical to ensure that students are equipped with the latest knowledge and skills
2. **Accessibility of Cyber Risk Management:** Cyber risk management should not require an increasingly advanced level of general and cybersecurity knowledge. The challenge is to make cyber risk knowledge accessible and applicable even at the vocational (MBO/ROC) level. This could include initiatives such as specialized courses that emphasize the connection between practical experience and education.
3. **Human-Organization-Technology Interaction:** The interaction among humans, organizations, and technology is expected to play an increasingly significant role in the future. Developing educational programs that focus on the intersection of these domains is essential for reducing barriers to effective cybersecurity practices. How can cybersecurity education better align with this critical intersection? Addressing this question involves creating interdisciplinary curricula that integrate technical, organizational, and human factors.

REFERENCES

Abromaitytė, M., Dubero, E., Kruger, Q., Lucassen, B., Vos, T., van den Hout, N.J., Bouma, D., Treur, J., Roelofsma, P.H.M.P. (2024). Computational Analysis of User Experience of Password-Based Authentication Systems. Proc. of the 16th International Conference on Intelligent Human Computer Interaction, IHCI'24. Lecture Notes in Computer Science, Springer Nature. https://www.researchgate.net/publication/382975936

AlDaajeh, S. Saleous, H., Alrabaee, S., Barka, E., Breitinger, F. Choo, K.K.R. (2022). The role of national cybersecurity strategies on the improvement of cybersecurity education. *Computers & Security, 119*, 102754. https://doi.org/10.1016/j.cose.2022.102754

AlDaajeh, S. Alrabaee, S. (2024). Strategic cybersecurity, *Computers & Security, 141*, 103845. https://doi.org/10.1016/j.cose.2024.103845.

Akmalluddin, A. and Ediyono, S. (2023). Quadruple helix model philosophy to enhance corporate social responsibility (csr) creativity. Daengku: Journal of Humanities and Social Sciences Innovation, 3(4), 608-613. https://doi.org/10.35877/454ri.daengku1779

Akers, D., Blomquist, T., Niedziela, J., Šebok, S., Van den Hout, N.J., Bouma, D., Treur, J., Roelofsma, P.H.M.P. (2024). Organizational Response to APT attacks: Computational Analysis by Behavioral Network Modelling. Proc. of the 16th International Conference on Intelligent Human Computer Interaction, IHCI'24. Lecture Notes in Computer Science, Springer Nature. https://www.researchgate.net/publication/382061930

Al-Mhiqani, M.N., Alsboui,T., Al-Shehari, T., Abdulkareem, K.H., Ahmad, R.M., Mohammed,M.A. (2024). Insider threat detection in cyber-physical systems: a systematic literature review Computers and Electrical Engineering, 119,109489.
https://doi.org/10.1016/j.compeleceng.2024.109489

Babayusuf, Y., Bouma, D., Feteasco, A., van Hekezen, L., Vasov, J., Zwarts, N., Treur, J., Roelofsma, P.H.M.P. (2024). Enhancing Cyber Resilience Securing Governmental Applications for Citizens: Computational Analysis. https://www.researchgate.net/publication/382975648

Bart, J., Milani, S., Raïkkönen, Sultani, D., Van ’t Hoff, F., Zwarts, N., Hoffmans, C., Treur, J., Roelofsma, P.H.M.P. (2024). Computational Analysis of Disruptions of Mobile Networks during Wartime: an Adaptive Network Modeling Approach. Proc. of the 8th International Conference on Computer-Human Interaction Research and Applications, CHIRA’24. Communications in Computer and Information Science, Springer Nature. https://www.researchgate.net/publication/382544551

Belkuyu, E., Bijl, T., Nobre Dos Santos, J.R., Sevdalakis, J.I., Hoffmans, C., Treur, J., Roelofsma, P.H.M.P. (2024). Breaking through Escalation of Commitment and Groupthink in Cyber Risk Management by AI Coaching: a Network-Oriented Computational Analysis https://www.researchgate.net/publication/382975602

Bell, A., Flik, Y., Hotsma, N., Tande, P.J.L., Zwarts, N. Hoffmans, C., Treur, J., Roelofsma, P.H.M.P. (2024). CyberAttacks Triggering a Collective Response within NATO: A Network-Oriented Computational Analysis. In: Proc. of the 8th International Conference on Computational Methods in Systems and Software, CoMeSySo'24. Lecture Notes in Networks and Systems, Springer Nature. https://www.researchgate.net/publication/382424047

Ben-Asher, N., Gonzalez, C. (2015). CyberWar Game: A Paradigm for Understanding New Challenges of Cyber War. In: Jajodia, S., Shakarian, P., Subrahmanian, V., Swarup, V., Wang, C. (eds) Cyber Warfare. Advances in Information Security, vol 56. Springer, Cham. https://doi.org/10.1007/978-3-319-14039-1_10

Börcsök, T., Bos, M., Buter, W., Van Der Hoeven, D., Velev, A., Van den Hout, N.J., Bouma, D., Treur, J., Roelofsma, P.H.M.P. (2024). Adaptive Defence Mechanisms: An Adaptive Network Model to Protect HiX Systems Against Cyber Attacks. In: Proc. of the 8th International Conference on Computational Methods in Systems and Software, CoMeSySo'24. Lecture Notes in Networks and Systems, Springer Nature. https://www.researchgate.net/publication/382739769.

Boschetti, N.. Gordon, N., Falco, (2022). Space cybersecurity lessons learned from the Viasat cyberattck. Paper presented at the AIAA Ascend conference. Las Vegas. www.researchgate.net/publication/363558808_Space_Cybersecurity_Lessons_Learned_from_The_ViaSat_Cyberattack

Bouma, D., Hoffmans, C., Van den Hout, N.J., Zwarts, N., Treur, J., Roelofsma, P.H.M.P. (2024). Cyber Security in Hospitals: A Network-Oriented Model for Behavioural Learning of Employees during Phishing Simulations. In: Proc. of the 17th International Conference on Computational Intelligence in Security for Information Systems, CISIS'24. Lecture Notes in Networks and Systems, Springer Nature. https://www.researchgate.net/publication/382186841

Bouma, D., Den Oudsten, T., Naffakh, A, Waliji, M., Treur, J., Roelofsma, P.H.M.P. (2024). Cyber Risk Management and Organisational Alignment Using Endley's Risk Management Model: Computational Analysis from an Adaptive Dynamical System Perspective. In: Proc. of the 8th International Conference on Computational Methods in Systems and Software, CoMeSySo'24. Lecture Notes in Networks and Systems, Springer Nature. https://www.researchgate.net/publication/382739842

Brilingaitė, A., Bukauskas, L., Juozapavičius, A., Kutka, E, (2022) Overcoming information-sharing challenges in cyber defence exercises, *Journal of Cybersecurity*, Volume 8, Issue 1, 2022, tyac001, https://doi.org/10.1093/cybsec/tyac001

Buldyrev, S. V., Parshani, R., Paul, G. Stanley, H.E., Havlin. S. (2010). Catastrophic Cascade of Failures in Interdependent Networks. *Nature* 464 (7291): 1025–28. https://doi.org/10.1038/nature08932

Cains, M., Flora, L., Taber, D., King, Z. M., Henshel, D. S. (2021). Defining cyber security and cyber security risk within a multidisciplinary context using expert elicitation. Risk Analysis, 42(8), 1643-1669. https://doi.org/10.1111/risa.13687

Caneva, J., Oliver, S., Rietze, N.E., Šileris, L., Barelds, N., Hoffmans, C., Treur, J., Roelofsma, P.H.M.P. (2024). The Unforeseen Blackout and Cyber Risk Management for Business Continuity: Network-Oriented Computational Analysis. In: Proc. of the 8th International Conference on Computational Methods in Systems and Software, CoMeSySo'24. Lecture Notes in Networks and Systems, Springer Nature. https://www.researchgate.net/publication/382562944

Capră, A.M.C., Dekker, E., Hoffmann, L., Hoffmans, C., Hoogstad, M., Mueller, T., van den Hout, N.J., Treur, J., Roelofsma, P.H.M.P. (2024). Computational Analysis of Human Factors in Spear-Phishing Attacks: An Adaptive Network Model. Proc. of the 16th International Conference on Intelligent Human Computer Interaction, IHCI'24. Lecture Notes in Computer Science, Springer Nature. https://www.researchgate.net/publication/382975864

Carayannis, E. G., Campbell, D. F. J. (2009). "Mode 3 and Quadruple Helix: Toward a 21st Century Fractal Innovation Ecosystem. *International Journal of Technology Management, 46,* 3/4, 201-234. DOI:10.1504/IJTM.2009.023374.

Carayannis, Elias G.; Barth, Thorsten D.; Campbell, David F. J. (2012). "The Quintuple Helix innovation model: global warming as a challenge and driver for innovation". Journal of Innovation and Entrepreneurship. 1,1,2. doi:10.1186/2192-5372-1-2.

Canbaloğlu, G., Treur, J., Roelofsma, P.H.M.P. (2022). Computational modeling of organisational learning by self-modeling networks. Cognitive Systems Research, 73, 51-64.

Canbaloğlu, G., Treur, J., Roelofsma, P.H.M.P. (2024). Learning of Safety and Security Management through Cyberspace: An Adaptive Self-Modeling Network Model for Multilevel Organizational Learning. In: Roelofsma, P.H.M.P., Jabeen, F. Taal, H. R. Treur, J. (eds.) Using Shared Mental Models and Organisational Learning to Support Safety and Security through Cyberspace: a Computational Analysis Approach. Springer Nature, Cham, Switzerland.

Colicchia, C., Creazza, A., Menachof, D. (2019). Managing cyber and information risks in supply chains: insights from an exploratory analysis. Supply Chain Management an International Journal, 24(2), 215-240. https://doi.org/10.1108/scm-09-2017-0289

Craik, K.J.W.: The nature of explanation. Cambridge, MA: University Press. (1943).

Cremer, F., Sheehan, B., Fortmann, M. (2022) Cyber risk and cybersecurity: a systematic review of data availability. *Geneva Pap Risk Insur Issues Pract 47,* 698–736 (2022). https://doi.org/10.1057/s41288-022-00266-6.

Daniel, M. Soutar, C. (2022). Systemic Cybersecurity: risk and role of the global community. Managing the unmanageable. World Economic Forum. Global Future Council of Cybersecurity.

Daza, M., Duivesteijn, D., Jouma, M., Reichardt, F., Barelds, N., Bouma, D., Treur, J., Roelofsma, P.H.M.P. (2024). The Delicate Balance of Ethics and Control for Smart Cities: A Network-Oriented Analysis Approach. Proc. of the 8th International Conference on Computer-Human Interaction Research and Applications, CHIRA'24. Communications in Computer and Information Science, Springer Nature. https://www.researchgate.net/publication/382975762

de Jong, R., Geerman, D., Oduber, A., Paterson, B., Popova, K., Zwarts, N., Bouma, D., Treur, J., Roelofsma, P.H.M.P. (2024). Electromagnetic Signature Management on the Battlefield: Computational Analysis by Adaptive Network Modelling https://www.researchgate.net/publication/382975651

Dijkstra, M, Veen, S. (2024) The many languages of risk management and how to navigate them. Paper presented at the ONE conference.

Dragosin, M., Kodradjaya, J., De Mos, E., Pittari, C., Zwarts, N., Treur, J., Roelofsma, P.H.M.P. (2024). Predicting the Persistent: a Computational Network-Oriented Model for Advanced Persistent Threats https://www.researchgate.net/publication/385023029

Dykstra, J., Gordon, L.A., Loeb, M.P,, Zhou, L. Maximizing the benefits from sharing cyber threat intelligence by government agencies and departments, *Journal of Cybersecurity*, Volume 9, Issue 1, 2023, tyad003, https://doi.org/10.1093/cybsec/tyad003

Erdogan, A., Hoffmans, C., Sbita, A., Wach, E., Zuijderduijn, K., van den Hout, N.J., Treur, J., Roelofsma, P.H.M.P (2024). Network-Oriented Computational Analysis of Cyber-Attacks. In: Proc. of the 8th International

Conference on Computational Methods in Systems and Software, CoMeSySo'24. Lecture Notes in Networks and Systems, Springer Nature https://www.researchgate.net/publication/382975658 12.

ENISA (2023a). Threat Landscape 2023. European Union Agency for Cybersecurity.

ENISA (2023b). Good practices for supply chain cyber security. European Union Agency for Cybersecurity.

ENISA (2024). Best practices for cyber crisis management. European Agency for Cybersecurity.

Fayi, S.Y.A. (2018). What Petya/NotPetya Ransomware Is and What Its Remidiations Are. In: Latifi, S. (eds) Information Technology - New Generations. Advances in Intelligent Systems and Computing, vol 738. Springer, Cham. https://doi.org/10.1007/978-3-319-77028-4_15

Feng, C.Q., Wang, T. (2019). Does CIO risk appetite matter? Evidence from information security breach incidents. *International Journal of Accounting Information Systems, 32*, 59-75.

Forscey, D., Bateman, J. Beecroft, N., Woods, B. (2023). Systemic risk: A primer. Carnegie Endowment for International Peace and the Aspen Institute

Furnell, S. (2024). Usable Cybersecurity: A contradiction in terms? *Interacting with Computers, 36*,3–15. https://doi.org/10.1093/iwc/iwad035

Ghadge, A., Weiß, M., Caldwell, N. D., Wilding, R. (2019). Managing cyber risk in supply chains: A review and research agenda. Supply Chain Management: An International Journal, 25(2), 223- 240

Grobler M, Gaire R and Nepal S (2021) User, usage and usability: redefining human centric cyber security. Front. Big Data 4:583723. doi: 10.3389/fdata.2021.583723

Haastrecht, M. A. N. van, Golpur, G., Tzismadia, G., Kab, R., Priboi, C., David, D. (2021). A shared cyber threat intelligence solution for SMEs. *Electronics, 10* (23). doi:10.3390/electronics10232913

Hautamaki, J., Hamalainen, T (2021). A model of Cyber threat information sharing with the novel network topology. International Conference, 7. 1-10. *IAIT '21: Proceedings of the 12th International Conference on Advances in Information Technology*, *7*, 1 – 10, https://doi.org/10.1145/3468784.3468885

Hill, R., Gibson, E.Pickford, R. (2023). Common cascade risk models and how to build them. Report 4. National Foresight Group. Nothingham Trent University.

Hoffmans, C., van der Does, L., van der Kolk, M., van Rooyen, T., Barelds, N., Treur, J., Roelofsma, P.H.M.P. (2024). Analysing the Rise of Biohacking in a Tech-Driven City: Assessing Risks through Adaptive Network Modeling. Proc. of the 16th International Conference on Intelligent Human Computer Interaction, IHCI'24. Lecture Notes in Computer Science, Springer Nature. https://www.researchgate.net/publication/382975862

Hoppe, F., Gatzert, N., Gruner, P. (2021). Cyber risk management in smes: insights from industry surveys. The Journal of Risk Finance, 22(3/4), 240-260. https://doi.org/10.1108/jrf-02-2020-0024

Hubbard, D.W. (2020). The Failure of Risk Management: Why It's Broken and How to Fix It. Wiley and Sons.

Imperial, M.T., Johnston, E., Pruett-Jones, M., Leong, K., Thomsen, J. (2016). Sustaining the useful life of network governance: life cycles and developmental challenges *Frontiers in Ecology and the Environment.* 14(3): 135–144, doi:10.1002/fee.1249

Ivan, I., van den Hout, N.J., Hendrikse, S.C.F., Treur, J., Roelofsma, P.H.M.P. (2024). Understanding Insider Threats Behaviour: An Adaptive Network Model for the Evolution of an Insider Threat. Proc. of the 16th International Conference on Intelligent Human Computer Interaction, IHCI'24. Lecture Notes in Computer Science, Springer Nature.

Jacobseon Ofte, H., Katsikas, S. (2023). Understanding situation awareness in SOC's: A systematic literature review. Computers and Security, 126, 103069. 10.1016/j.cose.2022.103069

Jazairy, A, Brho, M., Manuj, I., Goldsby, T.J. (2024). Cyber risk management strategies and integration: toward supply chain cyber resilience and robustness. *International Journal of Physical Distribution & Logistics Management*, 54, 11, 1-29. DOI 10.1108/IJPDLM-12-2023-0445

Jeffery, E., Malsagov, U., Tijssen, N., Zeisig, A., Hoffmans, C., Treur, J., Roelofsma, P.H.M.P. (2024). Computational Analysis of the Effectiveness of the Intelligence Cycle for Organizational Cyber Risk Management. In: Proc. of the 8th International Conference on Computational Methods in Systems and Software, CoMeSySo'24. Lecture Notes in Networks and Systems, Springer Nature. https://www.researchgate.net/publication/382060508

Jeong, J.J., Oliver, G., Kang, E. *et al.* The current state of research on people, culture and cybersecurity. *Personal Ubiquitous Computing* **25**, 809–812 (2021). https://doi.org/10.1007/s00779-021-01591-8

Keijzer, S., Lochtenbergh, D., Marsman, T., Voorhoeve, S., Zwarts, N., Bouma, D., Treur, J., Roelofsma, P.H.M.P. (2024). Managing Classified Information by a Third-Party Contractor: A Computational Cybersecurity Analysis. Proc. of the 8th International Conference on Computer-Human Interaction Research and Applications, CHIRA'24. Communications in Computer and Information Science, Springer Nature. https://www.researchgate.net/publication/382061594

Kruti, A., Butt, U. Sulaiman, R. (2023). A review of SolarWinds attack on Orion platform using persistent threat agents and techniques for gaining unauthorized access. https://doi.org/10.48550/arXiv.2308.10294

Kubota, (2024). A computer scientist stake on the Crowdstrike crash. Standord Report. https://news.stanford.edu/stories/2024/07/an-expert-s-overview-of-the-crowdstrike-outage.

Kure, H. I., Islam, S., Mouratidis, H. (2022). An integrated cyber security risk management framework and risk predication for the critical infrastructure protection. Neural Computing and Applications, 34(18), 15241-15271. https://doi.org/10.1007/s00521-022-06959-2

Lepădatu, F., Mihăilescu, T., Spaan, Ţiţei, P., van der Vossen, M., van den Hout, N.J., Hoffmans, C., Treur, J., Roelofsma, P.H.M.P. (2024). Analysis of Management of Phishing Attack Risks Based on an Adaptive Network Model https://www.researchgate.net/publication/382975599

Liaropoulos, A. "A Human-Centric Approach to Cybersecurity: Securing the Human in the Era of Cyberphobia." *Journal of Information Warfare*, vol. 14, no. 4, 2015, pp. 15–24. *JSTOR*, https://www.jstor.org/stable/26487503. Accessed 29 Oct. 2024.

Liu, Z. (2023). Technological Mediation Theory and the Moral Suspension Problem. *Human Studies,* **46**, 375–388. https://doi.org/10.1007/s10746-021-09617-z

Lupp, G., Aude Zingraff-Hamed, J.J., Huang, A.O.,Stephan P. (2021). Living Labs—A Concept for Co-Designing Nature-Based Solutions, *Sustainability, 13*, 1, 188. https://doi.org/10.3390/su13010188.

Marotta, A. and McShane, M. K. (2018). Integrating a proactive technique into a holistic cyber risk management approach. Risk Management and Insurance Review, 21(3), 435-452. https://doi.org/10.1111/rmir.12109

Mason, O.J., Stevenson, C., Freedman, F. (2014). Ever-present threats from information technology: The Cyber-paranoia and Fear scale., *Frontiers in Psychology, 5*, 1298, 1-6.

McDonald, S., Damarin, A. K., Membrez Weiler, N. J. (2022). Organizational perspectives on digital labor market intermediaries. *Sociology Compass, 17*(4). https://doi.org/10.1111/soc4.13061

Melaku, H.M. (2023). A Dynamic and Adaptive Cybersecurity Governance Framework. Journal of Cybersecurity and Privacy. 2023, 3, 327–350. https://doi.org/10.3390/jcp3030017

Melnyk, S. A., Schoenherr, T., Speier-Pero, C., Peters, C., Chang, J. F., Friday, D. (2021). New challenges in supply chain management: cybersecurity across the supply chain. *International Journal of Production Research, 60(1)*, 162-183. https://doi.org/10.1080/00207543.2021.1984606

Mestour, W., van den Hout, N.J., Treur, J., Roelofsma, P.H.M.P. (2024). An Adaptive Network Model to Analyse Cybersecurity: Understanding Cyber Threats in Financial Institutions. Proc. of the 16th International Conference on Intelligent Human Computer Interaction, IHCI'24. Lecture Notes in Computer Science, Springer Nature. https://www.researchgate.net/publication/382975671

Mizrak, F. (2023). Integrating Cybersecurity risk management into strategic management: A comprehensive literature review. Research Journal of Business and Management, 10, 3, 98-108.

Mohd Kassim, S.R., Li S., Arief, B. (2022) Incident Response Practices Across National CSIRTs: Results from an Online Survey. *OIC-CERT Journal of Cyber Security, 4*, 1, 67 – 84.

Moumouh, C., Chkouri, M.Y., Fernández-Alemán, J.L. (2023). Cybersecurity Awareness Through Serious Games: A Systematic Literature Review. In: Ben Ahmed, M., Abdelhakim, B.A., Ane, B.K., Rosiyadi, D. (eds) Emerging Trends in Intelligent Systems & Network Security. NISS 2022. Lecture Notes on Data Engineering and Communications Technologies, vol 147. Springer, Cham. https://doi.org/10.1007/978-3-031-15191-0_18

Moustafa AA, Bello A and Maurushat A (2021) The Role of User Behaviour in Improving Cyber Security Management. Front. Psychol. 12:561011. doi: 10.3389/fpsyg.2021.56101

Mukherjee, M.; Le, N.T.; Chow, Y.-W.; Susilo, W. (2024). Strategic Approaches to Cybersecurity Learning: A Study of Educational Models and Outcomes. *Information, 15*, 117. https://doi.org/ 10.3390/info15020117

Murimi, R., Blanke, S., Murimi, R. (2023). A Decade of Development of Mental Models in Cybersecurity and Lessons for the Future. In: Onwubiko, C., *et al.* Proceedings of the International Conference on Cybersecurity, Situational Awareness and Social Media. Springer Proceedings in Complexity. Springer, Singapore. https://doi.org/10.1007/978-981-19-6414-5_7

Ofte, H.J. (2024). The awareness of operators: a goal-directed task analysis in SOCs for critical infrastructure. *International Journal of Information Security.* **23**, 3253–3282 https://doi.org/10.1007/s10207-024-00872-6

Oxford Analytica (2021), Kaseya ransomware attack underlines supply chain risks, *Expert Briefings*. https://doi.org/10.1108/OXAN-ES262642

Palleti, V., Adepu, S., Mishra, V. Cascading effects of cyber-attacks on interconnected critical infrastructure, *Cybersecurity 4*, 8. https://doi.org/10.1186/s42400-021-00071-z.

Panda, A. and Andrew, B. (2020). Cyber security and the disaster resilience framework. International Journal of Disaster Resilience in the Built Environment, 11(4), 507-518. https://doi.org/10.1108/ijdrbe-07-2019-0046

Pandey, S., Singh, R., Gunasekaran, A., Kaushik, A. (2020). Cyber security risks in globalized supply chains: conceptual framework. Journal of Global Operations and Strategic Sourcing, 13(1), 103-128. https://doi.org/10.1108/jgoss-05-2019-0042

Pescaroli, G., Alexander, D. (2015). A definition of cascading disasters and cascading effects: Going beyond the 'toppling dominos' methaphor. *Environment Science*, GRF Davos Planet@Risk, Volume 3, 1, Special Issue on the 5th IDRC Davos 2014.

Peris-Ortiz, M., Ferreira, J.; Farinha, L., Fernandes, N. (2016). Introduction to Multiple Helix Ecosystems for Sustainable Competitiveness. *Multiple helix ecosystems for sustainable competitiveness*. Cham: Springer. pp. 1–14. doi:10.1007/978-3-319-29677-7.

Ray, L.L. (2013). Security Considerations for the Spiral Development Model. *International Journal of Information Management, 33*, 4, 684-686.

Renault, K., Searl, R., Dupuis, M. (2021) Shame in cybersecurity: effective behaviour modification tool or counterproductive foil. NSPW '21: Proceedings of the 2021 New Security Paradigms Workshop, pg. 70 – 87. https://doi.org/10.1145/3498891.3498896

Reuter, C., Iacono, L.L., Benlian, A. (2022). A quarter century of usable security and privacy research: transparency, tailorability and the road ahead. *Behavior & Information Technology, 41*,10, 2035-2048.

Roelofsma, P.H.M.P., Jabeen, F., Taal, H.R., Treur, J. (eds.), Using Shared Mental Models and Organisational Learning to Support Safety and Security through Cyberspace: a Computational Analysis Approach. Springer Nature.

Roesch, M. (2023). Solving the Tower of Babel Challenge. Security Boulevard, Solving the Tower of Babel Challenge - Security Boulevard

Romano, S.P. (2024). Cyber Warfare and Ethical Frontiers: Elevating Conflict to the Digital Frontline of Global Struggles. In: Santoianni, F., Giannini, G., Ciasullo, A. (eds) Mind, Body, and Digital Brains. Integrated Science, vol 20. Springer, Cham. https://doi.org/10.1007/978-3-031-58363-6_15

Saeed, S.; Suayyid, S.A.; Al-Ghamdi, M.S.; Al-Muhaisen, H.; Almuhaideb, A.M. A. (2023) Systematic Literature Review on Cyber Threat Intelligence for Organizational Cybersecurity Resilience. Sensors, 23, 7273. https://doi.org/ 10.3390/s23167273

Šijan, A.; Viduka, D.; Ilić, L.; Predić, B.; Karabašević, D. (2024). Modeling Cybersecurity Risk: The Integration of Decision Theory and Pivot Pairwise Relative Criteria Importance Assessment with Scale for Cybersecurity Threat Evaluation. *Electronics*, *13*, 4209. https://doi.org/10.3390/electronics13214209

Sullivan, D.T., Colbert., Colbert, E.J.M., Hoffman, B.E., Kott, A. (2018). *Journal of Information Warfare, 17*, 3, 92-105.

Talesh, S. A. (2018). Data breach, privacy, and cyber insurance: how insurance companies act as “compliance managers” for businesses. Law &Amp; Social Inquiry, 43(02), 417-440. https://doi.org/10.1111/lsi.12303

Toregas, C. Santos, M. (2019). Cybersecurity and its cascading effects on societal systems. Global assessment report on disaster risk reduction. United Nations Office for Disaster Reduction (UNDRR).

Torres–Barrán, A., Redondo, A., Insua, D. R., Domingo, J., Ruggeri, F. (2021). Structured expert judgement issues in a supply chain cyber risk management system. International Series in Operations Research &Amp; Management Science, 441-458. https://doi.org/10.1007/978-3-030-46474-5_20

Towhidi, G., Pridmore, J. (2023). Aligning Cybersecurity in Higher Education with Industry Needs. *Journal of Information Systems Education, 34*, 1, 70-83. https://aisel.aisnet.org/jise/vol34/iss1/6.

Treur, J. (2020). Network-Oriented Modelling for Adaptive Networks: Designing Higher-Order Adaptive Biological, Mental and Social Network Models. Springer Nature.

Van den Hout, N.J., Bouma, D., Hoffmans, C., Zwarts, N., Treur, J., Roelofsma, P.H.M.P. (2024). Addressing Organizational Cyber Security Challenges in Healthcare using Adaptive Network-Oriented Modeling. In: Roelofsma, P.H.M.P., Jabeen, F., Taal, H.R., Treur, J. (eds.), Using Shared Mental Models and Organisational Learning to Support Safety and Security through Cyberspace: a Computational Analysis Approach. Springer Nature. https://www.researchgate.net/publication/381105413

Vaughn, P. E., Greene, C., Klinger, D. (2024). Revenge Effects and Electronic Control Weapons: A Cautionary Tale about the Unintended Consequences of Technology in the American Justice System. *Journal of Criminal Justice*, *90*, 102144.

Vlijmen, B. (2023). Aggregation dynamics. *Transmathematica.* https://doi.org/10.36285/tm.83

Wallis, T., Dorey, P. (2023). Implementing Partnerships in Energy Supply Chain Cybersecurity Resilience. Energies, 16(4), 1868. https://doi.org/10.3390/en16041868

Welburn, J. and Strong, A. (2021). Systemic cyber risk and aggregate impacts. Risk Analysis, 42(8), 1606-1622. https://doi.org/10.1111/risa.13715

World Economic Forum (2017). Advancing cyber resilience: principles and tools for boards. Future digital economy and society system initiative. REF 110117.

Yusuf, O.I. (2024). Bridging the Gap: Aligning Cybersecurity Education with Industry Needs. *International Journal of Information technology and Computer Engineering, 4*, (43), 1-8.

Zhang, X., Liu, D., Zhan, C., Tse, C. (2017). Effects of cyber coupling on cascading failures in power systems. Ieee Journal on Emerging and Selected Topics in Circuits and Systems, 7(2), 228-238. https://doi.org/10.1109/jetcas.2017.2698163

Zhang, Z., Ning, H., Shi, F. Artificial intelligence in cyber security: research advances, challenges, and opportunities. *Artificial Intelligence Review,* 55, 1029–1053 (2022). https://doi.org/10.1007/s10462-021-09976-0