

How Scenario-Based Interventions Transform Cybersecurity Mental Models in Danish Defence SMEs

Judith Kankam-Boateng
Mathematics and Computer Science
University of Southern Denmark
Odense, Denmark
jukan@imada.sdu.dk

Marco Peressotti
University of Southern Denmark
Odense, Denmark
peressotti@imada.sdu.dk

Jan Stentoft
Department of Entrepreneurship and
Relationship Management
University of Southern Denmark
Kolding, Denmark
stentoft@sam.sdu.dk

Kent Adsbøll Wickstrøm
Department of Entrepreneurship and
Relationship Management
University of Southern Denmark
Kolding, Denmark
kwj@sam.sdu.dk

Ole Stegmann Mikkelsen
Department of Business and
Sustainability
University of Southern Denmark
Kolding, Denmark
osm@sam.sdu.dk

Vincent Charles Keating
Centre for War Studies
University of Southern Denmark
Odense, Denmark
keating@sam.sdu.dk

Louise Alison Tumchewics
Centre for War Studies
University of Southern Denmark
Odense, Denmark
ltu@sam.sdu.dk

Amelie Theussen
Defense Academy
Royal Danish Academy
Copenhagen, Denmark
amth@fak.dk

Olivier Schmitt
Defence Academy
Royal Danish Academy
Copenhagen, Denmark
olsc@fak.dk

Peter Mayer
Department of Mathematics and
Computer Science
University of Southern Denmark
Odense, Denmark
Institute of Applied Informatics and
Formal Description Methods
Karlsruhe Institute of Technology
Karlsruhe, Germany
mayer@imada.sdu.dk

Abstract

When stakeholders in the national cybersecurity landscape hold fundamentally different mental models of cybersecurity, even well-designed policies can fail to be implemented in practice. We present a two-phase study that traces the transformation of mental models among stakeholders in Denmark's defence supply chain. First, we conducted workshops with policymakers (n=6) and policy promoters (n=11) to develop five scenarios and elicit their perceptions of cybersecurity for Small and Medium Enterprises (SME). Then, policy implementers from 12 SMEs (n=28) were confronted with the scenarios. We elicited mental models before and after to assess scenario-driven change. Our findings show that scenarios catalyzed significant shifts, such as from reactive to proactive mindsets and from isolated to supply-chain-wide perspectives. However, deeper

structural dimensions, e.g., the framing of cybersecurity as a cost rather than an investment, proved resistant to change. Based on our results, we outline design implications for stakeholder-adaptive cybersecurity interventions in high-trust cultural contexts.

CCS Concepts

• **Security and privacy** → **Social aspects of security and privacy**; *Economics of security and privacy*; • **Human-centered computing** → **Empirical studies in HCI**; • **Applied computing** → Supply chain management.

Keywords

Focus Group, Mental Models, Danish SMEs, Defence sector, Supply Chain, Scenarios

ACM Reference Format:

Judith Kankam-Boateng, Marco Peressotti, Jan Stentoft, Kent Adsbøll Wickstrøm, Ole Stegmann Mikkelsen, Vincent Charles Keating, Louise Alison Tumchewics, Amelie Theussen, Olivier Schmitt, and Peter Mayer. 2026. How Scenario-Based Interventions Transform Cybersecurity Mental Models in Danish Defence SMEs. In *Proceedings of the 14th Nordic Conference on*



This work is licensed under a Creative Commons Attribution 4.0 International License. *NordiCHI '26, Vaasa, Finland*

© 2026 Copyright held by the owner/author(s).
ACM ISBN 979-8-4007-2373-5/26/10
<https://doi.org/10.1145/3829807.3829812>

Human-Computer Interaction (NordiCHI '26), October 03–07, 2026, Vaasa, Finland. ACM, New York, NY, USA, 24 pages. <https://doi.org/10.1145/3829807.3829812>

1 INTRODUCTION

Cybersecurity threats to supply chains have grown in both frequency and severity. High-profile breaches such as SolarWinds [15, 32, 78] demonstrate how vulnerabilities in one organization can cascade across interconnected systems. The ENISA Threat Landscape 2025 report confirms that this trend is intensifying, with supply chain risks accounting for 10.6% of all threat categories and adversaries increasingly compromising third-party providers, open-source repositories, and browser extensions to amplify the reach of their attacks [31]. Small and medium-sized enterprises (SMEs) occupy a critical position in this landscape: they form the backbone of most supply chains yet remain disproportionately vulnerable due to resource constraints, limited expertise, and competing priorities [5, 6, 51, 67]. In Denmark, where SMEs constitute approximately 99% of businesses [23] and cyber threats are classified as “very high” [14], this vulnerability carries national security implications. This is particularly evident in the defence supply chain.

Countering these threats requires SMEs to develop greater organizational resilience. This can be achieved not only through technical defences but also through their understanding and reasoning about cybersecurity risks. Mental models, the internal representations people construct to reason about complex domains [12, 49], fundamentally shape how stakeholders perceive threats, evaluate risks, and prioritize responses. Research on cybersecurity mental models has shown that users rely on familiar analogies to understand threats [12], that “folk models” shape security decisions [103], and that persistent misalignments exist between expert and non-expert understanding [10, 46, 75]. However, this research has predominantly focused on individual users and static snapshots of understanding.

Scenario planning has emerged as a promising method for building resilience, enabling participants to anticipate threats and reconsider assumptions in controlled settings [1, 16, 100]. Recent work has applied scenario planning to cybersecurity supply chain risk management (C-SCRM), demonstrating that scenarios can shift how SMEs perceive and respond to cyber threats [42, 80]. Nevertheless, whether and how scenarios reshape participants’ mental models remains unexplored. To the best of our knowledge, no prior work has examined how scenario-based interventions can reshape cybersecurity mental models across different organizational stakeholder levels.

This paper addresses this gap. We present a two-phase qualitative study conducted with 45 participants across Denmark’s defence supply chain. Figure 1 illustrates this two-phase design:

- **Phase 1 (Scenario Development):** Through workshops with policymakers (n=6) and policy promoters (n=11), we developed five scenarios while eliciting their perceptions of cybersecurity threats, supply chain risks, and regulations.
- **Phase 2 (Scenario Evaluation):** The scenarios were deployed in strategic foresight exercises with policy implementers from 12 SMEs (n=28). We elicited mental models

before and after the exercises to assess scenario-driven transformation, and then held plenum discussions.

We address two research questions:

- RQ1:** How do scenario-based exercises transform cybersecurity mental models among SMEs in the defence supply chain, and which aspects of these mental models shift or resist change?
- RQ2:** What are the implications for designing stakeholder-adaptive cybersecurity interventions across different organizational levels?

Our study makes three contributions. First, we provide the first empirical account of cybersecurity mental model transformation, connecting pre-intervention to post-intervention shifts across three stakeholder levels (C1). Second, we demonstrate that scenario-based interventions transform surface-level awareness, such as threat perception and supply chain thinking, while deeper structural frames remain largely intact. An example of this is the framing of cybersecurity as cost versus investment (C2). Third, we derive design implications for multi-stakeholder cybersecurity interventions, showing that effective interventions must be both stakeholder-adaptive and culturally situated, particularly in high-trust contexts like the Nordic countries (C3). Our work engages core HCI concerns: how people construct mental representations of complex socio-technical systems [12], how targeted interventions can reshape these representations, and how the design of security interventions must account for organizational, cultural, and stakeholder-level differences.

2 BACKGROUND AND RELATED WORKS

2.1 Denmark’s Defence Supply Chain Context

Denmark’s defence supply chain ecosystem provides a distinctive research context. It is characterized by high institutional trust [70, 74], tightly interdependent supplier networks, and a cultural context that contrasts with low-trust environments (particularly in the United States), where most cybersecurity research has been conducted [40, 44, 55, 69]. Rising geopolitical tensions in Northern Europe (baltic sea) [50, 98], NATO obligations [57], and the implementation of the EU’s NIS2 directive [30, 65] are placing additional pressure on defence SMEs [25, 26].

2.2 Cybersecurity Challenges for SMEs in Supply Chains

SMEs occupy critical roles in supply chains and vastly outnumber large enterprises [35], making them a key target for cybersecurity efforts [39, 67], yet they rarely conduct cyber-risk assessments, and their IT and business leadership are often misaligned on managing cybersecurity risk [7]. This gap is compounded by CEOs absorbed in daily operations and reactive strategy over long-term development [63, 97], alongside SMEs’ distinct cybersecurity challenges: fewer resources, less technical experience, limited specialized expertise, and awareness gaps that often leave cybersecurity managed by non-specialists [5, 6, 38, 41, 51, 60]. Attackers frequently exploit SMEs as entry points to larger organizations and supply chains [67, 90]. Danish SMEs exemplify these challenges: 40% operate below adequate security levels, and documentation practices

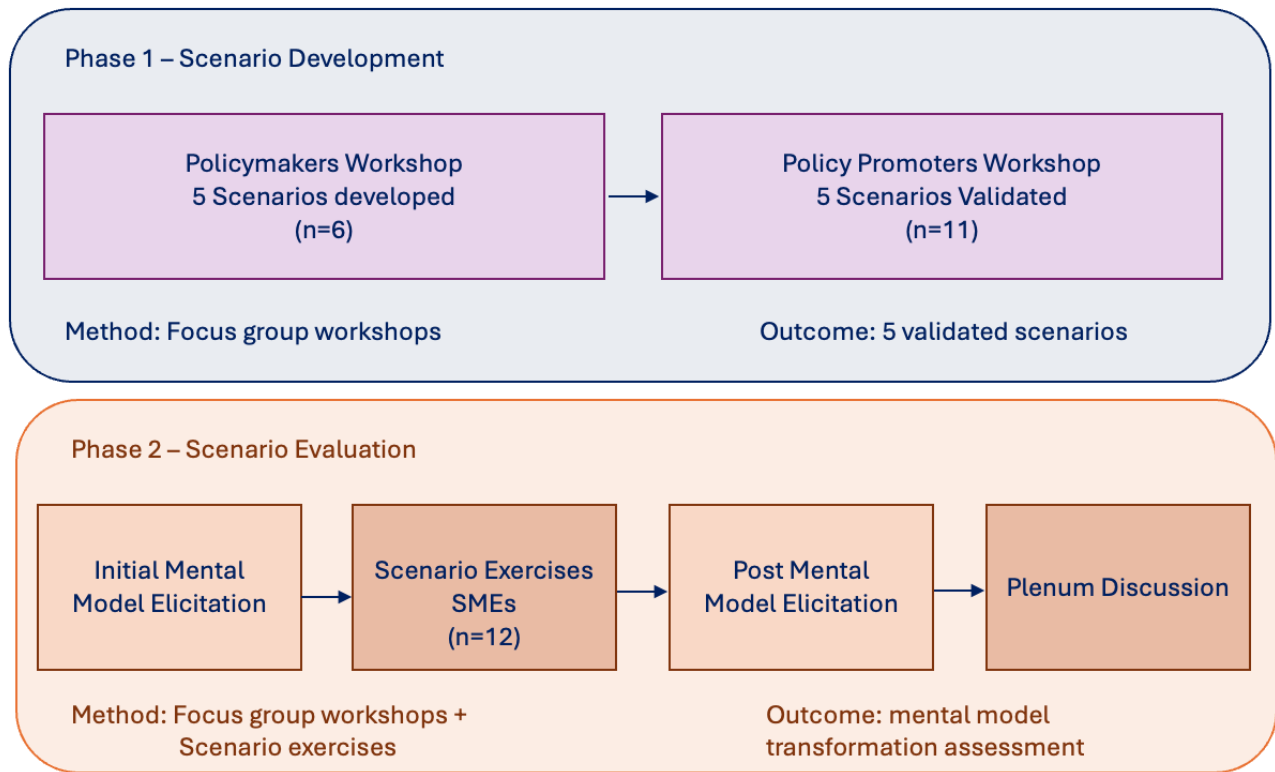


Figure 1: Two-phase research design: scenario development with policymakers and industry experts (Phase 1), followed by scenario evaluation with SMEs (Phase 2).

are inconsistent [23, 24, 33]. The gap between cybersecurity awareness and practical implementation persists even among engaged organizations [96]. This gap is not sector-specific. Zou et al. [110] found that after the 2017 Equifax breach, consumers' primary barrier to protective action was cost, not risk misperception: fees for credit freezes, fragmented tools, and a tendency to delay action until harm occurred. Participants with the least financial slack were both most exposed and least likely to act, a pattern the authors term the "nothing to lose" fallacy. The parallel to SMEs is direct: resource-constrained firms may under-invest in cybersecurity not because they fail to perceive threats, but because the marginal cost of action is disproportionate to their perceived exposure. Awareness-raising alone does not address this barrier.

Supply chain cybersecurity extends these challenges across organizational boundaries. Securing supply chains requires not only technical defenses but also alignment among stakeholders in how they understand threats, evaluate risks, and prioritize responses [8, 37, 72]. Vulnerabilities can propagate through supply networks via seemingly minor entry points [17, 71]. However, much of the existing research assumes the capacity of large organizations, leaving SME-specific challenges, particularly how SMEs perceive and respond to supply chain cyber risks, underexplored [22]. This paper addresses this gap by examining how stakeholders at different levels

of the defence supply chain understand cybersecurity and whether scenario-based interventions can reshape that understanding.

The multi-stakeholder nature of supply chain cybersecurity creates additional complexity. Strategic policies developed at national levels often fail to translate effectively into operational practices at the SME level [77, 83]. Policymakers may emphasize national resilience and geopolitical positioning, while SMEs focus on daily operations and regulatory compliance. These different framings can create policies that appear comprehensive but prove unworkable in practice [53]. Empirical research comparing how different stakeholder groups understand their cybersecurity roles and responsibilities remains limited, particularly in critical infrastructure sectors.

2.3 Mental Models in Cybersecurity

There is no single agreed definition of a mental model; the concept is defined in many different ways across the literature, such as mental models being internal cognitive structures through which individuals make sense of how systems function [49]. In human-computer interaction (HCI), these models capture a user's beliefs about a system, which may not always align with the designer's intended conceptual model [73]. This mismatch matters: when users' understanding of a system diverges from its actual logic, the

resulting behavior can be ineffective or even counterproductive [43, 59].

A mental model is not an undifferentiated whole but a multi-dimensional construct, and this dimensional construct is what our analysis turns on. Following Rook [87] and Renaud et al. [85], we treat a mental model as a personally constructed, internal conception of external phenomena that shapes how a person acts. Mental model research in HCI shows that the construct has been characterized along several dimensions, including static versus dynamic and accurate versus inaccurate, and that studies have classified mental models specifically as **functional** versus **structural** and as **expert** versus **non-expert** [45]. A recurring form of this contrast separates the surface features of a representation, what a person recognizes or knows how to do, from its deeper relational structure, how those elements relate to one another and to broader priorities [21, 48, 101]. This surface/structure pairing corresponds to the functional/structural distinction noted above: the surface level captures functional knowledge of which threats and responses exist, while the structural level captures how that knowledge is organized and prioritized [45]. We adopt this two-level view for cybersecurity: at the surface level, a stakeholder recognizes which threats and vulnerabilities are relevant and which responses are available; at the deeper structural level, a stakeholder holds beliefs about how cybersecurity is valued, resourced, and governed relative to other business priorities.

In addition, Camp's research on folk-models [103] offers a domain-specific precedent for this uneven depth within a single model, where models range from thin conceptions that merely name a threat to elaborated ones that specify its actor, motive, and mechanism, and only the latter support reasoning about unfamiliar situations [103, 105]. Evidence from other application areas indicates that interventions move these levels unequally: a systematic review of 142 cybersecurity training studies finds that awareness and knowledge rise reliably while demonstrable behaviour change remains comparatively rare [81].

Mental models have been elicited and studied through a range of methods, reflecting different trade-offs between depth, scale, and the ability to capture change over time. Naturalistic methods place participants in ecologically valid or lightly structured settings and include interviews [27, 62, 64, 103], focus group discussions [47, 53], questionnaires and surveys [28, 105], behavior coding [107], observations [106], and think-aloud protocols [64, 86]. Usability-oriented methods instead probe the structure of a mental model more directly, through common techniques such as path diagramming [61, 106], card sorting [3, 18, 82], analogies and metaphors [3, 19], concept mapping [106], and drawing or sketching [4, 11, 56, 66, 76, 82, 85], as well as less common techniques including storyboarding [54], modeling or prototyping, cognitive walk-throughs, and the teaching-back protocol [45]. Experimental methods, by contrast, typically assess performance on assigned tasks, most often operational or search-oriented, though one study instead inferred participants' mental processes from psychophysiological signals. Algorithmic modelling and statistical learning approaches have also seen growing use alongside these more established techniques. A small number of special-case approaches fall outside these three families entirely — one study devised a bespoke interaction-related method for eliciting mental models, and another proposed a distinct framework

for measuring what it termed users' inherent mental models [45]. Naturalistic and usability methods in particular are well suited to characterising the state or structure of a mental model at a single point in time, but are not designed to capture how that structure changes over the course of an intervention [45].

Research on mental models spans diverse HCI contexts, each illustrating how discrepancies between user expectations and system behaviour create practical challenges. In explainable AI, for instance, Collaris et al. [20] observed that data scientists' intuitions about how feature importance scores are computed often diverge from the mathematical assumptions underlying the techniques themselves. Similarly, Kulesza et al. [59] found that the level of detail provided in system explanations directly influenced how accurately end users understood an intelligent agent's reasoning. These discrepancies are not confined to software. Scheiter et al. [93] reported that the type of briefing given to operators simulating automated driving led to markedly different internal representations of how the vehicle should behave. In military settings, Streefkerk et al. [99] demonstrated that the effectiveness of command-and-control interfaces depends on how well their design reflects the situational reasoning of military commanders. Turning to consumer technologies, Zheng et al. [109] showed that smart home users tend to assume manufacturers safeguard their data, yet rarely verify whether such protections are in place. Collectively, these studies suggest that mental models serve as a mediating layer between users and systems, shaping how people perceive risk, delegate trust, and make decisions.

Within cybersecurity, a growing body of research has examined how users construct mental models of threats and security mechanisms. Camp [12] was among the first to show that users draw on everyday analogies, such as crime, medicine, physical safety, and economic exchange, when reasoning about digital threats. Building on this foundation, Wash [103] identified eight folk models of hackers and malware, revealing that these lay conceptions, though often technically imprecise, possess an internal logic that guides security behavior. Subsequent studies have examined how users conceptualize specific technologies: Kang et al. [52] explored lay understandings of Internet architecture; Krombholz et al. [58] and Bravo-Lillo et al. [10] investigated misconceptions surrounding HTTPS, encryption, and browser warnings; and Geels [36] found that ordinary users interpret digital signatures through an identity-based lens that diverges substantially from their cryptographic function. A notable insight running through this body of work is that technical accuracy in a user's model is less important than whether the model promotes safe behavior [36, 104]. Wash and Rader [104] articulated this position as a research agenda: rather than training non-expert users to think like security professionals, the priority should be to identify which mental models lead to sound security decisions and to cultivate those models through targeted interventions.

However, two significant gaps remain in this body of work. First, the established line of inquiry has predominantly examined individual end users and their interactions with specific tools or technologies. Considerably less is known about how mental models function across organizational and stakeholder boundaries, for example between those who design cybersecurity policy, those who interpret

Table 1: Participant demographics

Stakeholder level	Women	Men	Total
Policymakers (PM)	2	4	6
Policy Promoters (PP)	3	8	11
Policy Implementers (PI, 12 companies)	5	23	28
Total	10	35	45

and promote it, and those who are expected to put it into practice. In contexts such as defence supply chains, where coordinated action across multiple organizational levels is essential, security vulnerabilities may arise not from any single group’s misunderstanding but from unrecognized divergences between groups that hold fundamentally different assumptions about risk, responsibility, and appropriate action.

Second, and perhaps more critically, existing research has largely treated mental models as static properties to be characterized at a single point in time. While Wash and Rader [104] called for interventions that cultivate desirable mental models, empirical evidence of whether and how cybersecurity mental models actually shift in response to structured interventions remains scarce.

Our study addresses both gaps: it provides the first multi-stakeholder, pre/post empirical account of how cybersecurity mental models shift in response to a structured intervention among policymakers, policy promoters, and SME implementers in the Danish defence sector, and it distinguishes which dimensions of understanding transform and which resist. We state these contributions (C1–C3) in full in Section 1.

3 STUDY OVERVIEW

We conducted a two-phase qualitative study to trace the transformation of mental models among stakeholders in Denmark’s defence supply chain. Both phases were conducted in 2024.

3.1 Participants

We recruited 45 participants across three stakeholder levels (see Table 1):

- **Policymakers (PM):** 6 participants (4 men, 2 women), senior officials from national security institutions and the Ministry of Foreign Affairs.
- **Policy Promoters (PP):** 11 participants (8 men, 3 women), industry association experts representing the defence sector.
- **Policy Implementers (PI):** 28 participants (23 men, 5 women) from 12 SMEs, selected from across all Danish regions. Each company sent 2–4 representatives.

PMs and PPs were recruited through the research team’s professional networks. PIs were recruited from a public register of Danish SMEs and screened for defence-sector operations and English proficiency.

3.2 General Procedure and Data Analysis

The study comprised two phases. In Phase 1, we conducted two workshops: one with policymakers to develop scenarios using the Intuitive Logics method, and one with policy promoters to validate

and refine these scenarios while eliciting their cybersecurity perceptions. In Phase 2, we deployed the resulting scenarios in strategic foresight exercises with policy implementers, eliciting their mental models before and after the exercises to assess the transformation they drove. This section describes the analytical approach common to both phases; Sections 4.1 and 5.1 detail each phase individually.

All sessions across both phases were audio-recorded and transcribed. We applied thematic analysis [9] in two stages. First, each phase was analyzed independently: transcripts were coded using in vivo, process, and initial coding (first cycle), then axial and theoretical coding (second cycle) [91]. Phase 1 (interviews across all three stakeholder groups) generated 628 initial codes, which were consolidated into 7 categories and 3 overarching themes. Phase 2 (scenario-based exercises with policy implementers) generated approximately 535 initial codes, which were consolidated into five main themes.

Second, and this constitutes the novel analytical contribution of this paper, we conducted a cross-phase analysis, systematically comparing PI perspectives before and after the Phase 2 scenario-based exercise. Specifically, we mapped the initial mental model against the post mental model to identify (a) which aspects of these mental models shift, (b) which aspects resist change, and (c) new themes that emerged only after PIs engaged with scenarios. For each of the six thematic areas, we compared the coded categories from before and after the scenario exercise, identifying where PI discourse shifted (new categories appearing, existing categories expanding or contracting) and where it remained unchanged. We then examined whether Phase 2 PI themes converged toward the baseline PM/PP perspectives, indicating gap closure, or diverged further. This comparison was performed by one researcher, with iterative review by two senior researchers with expertise in qualitative cybersecurity research. Disagreements were resolved through discussion until a consensus was reached. MAXQDA was used for data organization throughout.

To maintain our participants’ anonymity, we use the following identifiers: policymakers (PM.A–PM.F), policy promoters (PP.A–PP.K), and policy implementers (PI.A–PI.L, representing companies C1–C12). We aggregate PI perspectives at the company level and consider responses from both transcripts and response sheets (described in Section 5.1).

3.3 Positionality

Our team comprises researchers specializing in cybersecurity, supply chains, and geopolitics, with active engagement in both Danish SME contexts and government-level activities. We acknowledge that this positioning influenced our study design and analysis. We upheld reflexivity throughout [34], aiming for an inclusive, contextual understanding of stakeholder experiences rather than detached observation.

3.4 Relationship to Prior Work

This study is part of a multi-phase research program on cybersecurity and business continuity in Danish defence SMEs. Findings on initial mental models across stakeholder levels and the gaps between these models have been reported separately [53]. However,

no prior work has investigated the transformation of the mental models through scenario-based interventions. The cross-phase mapping, the identification of persistent gaps, and the analysis of which dimensions of mental models are amenable to transformation through scenario-based interventions are all original contributions of this paper.

3.5 Ethics

The study was approved by the institutional ethics board at the University of Southern Denmark. Informed consent was obtained from all participants. Audio recordings were stored encrypted and deleted after transcription. Pseudonyms replaced all identifying information. English proficiency was a participation criterion. Utmost care was taken to ensure that no information about the cybersecurity posture of any participant's organization was disclosed.

4 PHASE ONE- SCENARIO DEVELOPMENT

4.1 Method

Phase 1 comprised two workshops to develop scenarios and elicit stakeholder perceptions of cybersecurity.

4.1.1 Workshop 1: Scenario Development. The first workshop was conducted with policymakers (PM, $n=6$)—senior officials from national security institutions and the Ministry of Foreign Affairs. Using the Intuitive Logics method [102], the workshop proceeded through four steps [94]: (1) scoping the problem definition, relevant actors, and time horizon (2025–2030); (2) identifying driving forces through brainstorming and plotting on uncertainty/severity matrices; (3) selecting high-severity, high-uncertainty forces and constructing 2×2 scenario matrices [79]; and (4) fictionalizing scenarios into narratives [13]. Participants identified geopolitical crises and causal drivers using PESTEL (Political, Economic, Social, Technological, Environmental, Legal) analysis [108]. Alongside scenario development, we elicited PM perceptions of cybersecurity threats, supply chain risks, and regulations through semi-structured focus group discussion (87 minutes). The session was conducted in English and audio-recorded.

4.1.2 Workshop 2: Scenario Validation. The second workshop was conducted with policy promoters (PP, $n=11$)—industry association experts representing the defence sector. This workshop assessed the cybersecurity implications of each scenario for Danish SMEs and validated the scenarios' relevance and plausibility. We also elicited PP perceptions across the same thematic areas as the PM workshop through semi-structured focus group discussion (125 minutes). The session was conducted in English and audio-recorded.

4.2 Results

4.2.1 Scenario Outputs. This process generated five scenarios (see Table 2), fictionalized into approximately 1,000-word narratives featuring hypothetical Danish employees navigating the consequences of each scenario.

4.2.2 Mental Models. The PM and PP workshops revealed how policymakers and industry experts perceive cybersecurity in the defense supply chain. These perceptions serve as a baseline for

Table 2: The five scenarios developed in Phase 1

Scenario	Key elements
US Disengagement from Europe	NATO withdrawal, tariffs, Russian cyber threats
US–China Confrontation	Supply chain disruption, critical material shortages
Climate Change	Infrastructure damage, agricultural impacts, telecomm disruption
Economic Polarization	Strained welfare states, extremist ideologies, ransomware surge
AI Out of Control	LLM malfunction, over-reliance on remote servers

comparison with SME mental models in Phase 2. Table 3 summarizes the perspectives across stakeholder levels, with PI baseline data drawn from the initial elicitation in Phase 2.

4.2.3 Policymaker Perceptions. PMs framed cybersecurity as a strategic investment and emphasized interconnected threat landscapes involving both state and non-state actors. They held a systemic view of supply chain risks, highlighting Denmark's dependence on foreign technology solutions. PM.C noted: "*we don't have any Danish solutions, we are dependent a lot on other countries to deliver solutions.*" PMs advocated for formal training programs and viewed regulatory requirements as manageable and strategically important.

4.2.4 Policy Promoter Perceptions. PPs occupied a bridging position, aware of both the strategic framing held by PMs and the operational realities faced by SMEs. They recognized that their members viewed cybersecurity primarily as a financial burden. PP.H explained: "*our members, small businesses, view this as a financial cost [...] it doesn't generate any value to their bottom line.*" PPs identified supply chain visibility as a concern and advocated for micro-learning and peer network approaches to training, recognizing that formal programs were impractical for most SMEs.

4.2.5 Key Misalignments. Comparing PM and PP perspectives revealed substantial misalignments that would later prove relevant in Phase 2. PMs emphasized national resilience and geopolitical positioning, while PPs highlighted the gap between policy ambition and SME capacity. These divergent framings, cybersecurity as a strategic asset rather than a financial burden, threats as geopolitical rather than technical, supply chains as systemic rather than invisible, set the stage for understanding how SME mental models would respond to scenario-based interventions.

5 PHASE TWO-SCENARIO EVALUATION

5.1 Method

Phase 2 deployed the five scenarios developed in Phase 1 in strategic foresight exercises with SMEs, eliciting mental models before and after the exercises to assess scenario-driven transformation.

Table 3: Stakeholder perspectives on cybersecurity (Phase 1: PM and PP; Phase 2 initial mental models: PI)

Dimension	Policymakers (PM)	Policy Promoters (PP)	Policy Implementers (PI)
Cybersecurity framing	Strategic investment	Financial burden (for members)	Cost/compliance obligation
Threat posture	Comprehensive, interconnected	Recognize PI surface awareness	Reactive; “herring effect”
Threat actors	State + non-state actors	State + non-state actors	Non-state actors only
Supply chain awareness	Strategic, systemic	Visibility concerns	Absent from discussion
Training approach	Formal programs needed	Micro-learning, peer networks	Informal (lunch conversations)
Regulatory stance	Manageable, strategic	Aware of PI burden	Overwhelming, confusing

5.1.1 Procedure. Four workshops were held in November 2024 with policy implementers (PI, $n=28$) from the 12 defence SMEs across Denmark. Each workshop followed a three-stage structure:

Stage 1 - Initial mental model elicitation. Focus group discussions were conducted using semi-structured guides exploring six thematic areas: (1) current cybersecurity posture and practices, (2) threats, vulnerabilities, and preparedness, (3) training, awareness, and communication, (4) challenges, approaches, and risk assessment, (5) resources, regulations, and initiatives, and (6) supply chain risks. These sessions (75 minutes each) were facilitated by the same researcher from the cybersecurity unit for consistency, conducted in English, and audio-recorded.

Stage 2 - Strategic foresight exercises. Company representatives selected the scenario most relevant to their business, then dispersed to private rooms for discussion. Scenario work ran for approximately 135 minutes in total, beginning with independent discussion and followed by a different researcher check-ins from the geopolitical unit, split into a session before lunch and a continuation afterwards. Four questions guided the discussion: (1) What are the key risk factors and vulnerabilities? (2) What risks does this scenario pose to Danish businesses? (3) What vulnerabilities affect your business? (4) What mitigation has your business considered?

Scenario selection reflected business relevance: “US Disengagement from Europe” and “AI Out of Control” were most popular, followed by “US-China Confrontation,” “Economic Polarization,” and “Climate Change.” The workshops took place shortly before and after the US presidential election, which influenced participants’ interest in politically oriented scenarios.

Stage 3 - Post-scenario assessment. Following the scenario exercises, participants completed individual response sheets (RS) capturing changes in their understanding and intended practices. Response sheet quotes are marked with the suffix “RS” (e.g., PI.A-RS). We aggregate PI perspectives at the company level and consider responses from both transcripts and response sheets. Focus group discussions then explored perceived changes across the same thematic areas examined in Stage 1, enabling direct comparison. Groups reconvened in plenum to share reflections across scenarios.

5.1.2 Analysis of Mental Model Change. To trace how the scenario intervention reshaped PI mental models, we analyzed the Stage 1 (initial) and Stage 3 (post-scenario) material as a matched pre/post dataset. All focus group discussions were conducted in English, audio-recorded, and transcribed verbatim. Automated transcripts were manually checked, and identifying information was removed. The individual response sheets (RS) completed in Stage 3 were transcribed and analyzed alongside the discussion transcripts, with

PI perspectives aggregated at the company level. We coded this dataset using the thematic analysis of Braun and Clarke [9] and the coding framework of Saldaña [91].

One researcher coded the full dataset, applying in vivo, process, and initial coding in a first cycle and axial and theoretical coding in a second cycle. Codes were organized under the six thematic areas that structured *both* the initial and the post-scenario guides — as stated in Section 5.1.1 — so that each company’s pre- and post-intervention discourse could be compared within the same thematic framework. The full semi-structured guides, the five scenarios, and the resulting codebook are provided in the Appendix to support replication. We then performed a structured pre/post comparison. Working theme by theme, we placed the Stage 1 codes and the Stage 3 codes side by side and classified each dimension as (i) *transformed*, where new categories appeared or existing categories substantially expanded, contracted, or were reframed between Stage 1 and Stage 3; (ii) *persistent*, where the coded content remained materially unchanged; or (iii) *emergent*, where a category was present only after the intervention. Because the Phase 1 Policymaker and policy promoter elicitation used the same thematic guide, their coding served as a baseline reference: for each transformed dimension, we also recorded whether post-scenario PI discourse converged toward or diverged from that baseline, which we report as evidence of gap closure. Table 4 summarizes the resulting classification. To strengthen the trustworthiness of this single-coder analysis, we maintained a detailed audit trail documenting coding decisions, code refinements, and the emergence of each pre- and post-classification. The codebook, illustrative coded excerpts, and the pre/post classifications were reviewed iteratively by two senior researchers with expertise in qualitative cybersecurity research. Disagreements were resolved through discussion until consensus was reached. MAXQDA was used to organize the data and support the cross-stage comparison.

5.2 Results

The following findings address both research questions. The scenario intervention produced five distinct shifts in PI mental models (RQ1) and revealed three dimensions that proved resistant to change, with implications for intervention design (RQ2). We present each shift with evidence from the initial mental model elicitation and from the post-scenario assessment. Table 4 summarizes the transformation landscape. Where post-scenario PI perspectives converged toward PM or PP perspectives from Phase 1, we note this convergence as evidence of gap closure.

Table 4: Mental model transformation summary: shifts and persistent gaps

Dimension	Initial mental model	Post-scenario assessment	Status
Threat perception	Technical, narrow	Holistic: human, geopolitical, systemic	Transformed
Supply chain awareness	Absent from PI discourse	Central concern; sub-supplier focus	Transformed
Risk assessment approach	Reactive or absent	Proactive; structured plans	Transformed
Training orientation	Informal, ad hoc	Structured; leadership involved	Transformed
Systemic thinking	Isolated, organization-only	Interconnected, geopolitical	Transformed
Cybersecurity valuation	Cost/compliance burden	Still cost-framed	Persistent
Resource constraints	Limited budgets, expertise	Unchanged; “25-person company”	Persistent
PM–PI communication	PIs unaware of national resources	No cross-level dialogue created	Persistent

5.2.1 Shift 1: From Reactive to Proactive Postures. In their initial mental models, PIs described minimal structured risk assessment. PLE-RS noted: *“We do not have much risk assessment currently. So, the change is that we are now aware that we should prioritize this.”* PMs and PPs characterized PIs as adopting a “school of herrings” approach, relying on collective anonymity rather than individual defence. PPJ described: *“the smaller companies are aware of the cybersecurity threat [...] they are actually more like working like a school of herrings. Just so that they are not to be the ones attacked by the shark.”*

Following scenario exposure, a clear shift emerged. PIs committed to structured processes: *“Yes, we will implement: More awareness Training, Phishing mail campaign (Training), Incident Response Plan, Business Continuity Plan, Disaster Recovery Plan”* (PIC-RS). Others identified specific preparedness measures, including “hacking simulation” (PIB-RS), “incident response plan” (PIF-RS), and “disaster recovery plans” (PIB-RS). Several companies committed to making risk assessment an ongoing process: *“We should address time, for example, each month to improve this continuously”* (PIE-RS).

The scenarios made abstract threats concrete. By engaging with fictionalized narratives of geopolitical disruption, participants moved from acknowledging risk in principle to identifying specific actions.

5.2.2 Shift 2: From Technical to Holistic Threat Understanding. In their initial mental models, PI threat perceptions centered on technical threats such as phishing, malware, hacking, and ransomware. While PMs emphasized interconnected threat landscapes, *“I think the main threat is definitely hacking, getting into their systems”* (PMF), and PPs identified behavioral and cultural factors, PIs focused primarily on non-state actors deploying technical attacks. Physical access to hardware was a concern unique to PIs, while supply chain and geopolitical dimensions were discussed primarily by PMs and PPs.

Post-scenario, PI threat perception expanded substantially. Participants recognized human factors as central: *“the problem is more about people’s behavior and habits than about hardware and software”* (PIK-RS). Geopolitical dimensions entered PI discourse: *“geopolitical situations can be just as big as cybersecurity threats”* (PIL-RS). The recognition that cybersecurity extends beyond technical controls to encompass organizational culture, human behavior, and geopolitical context represents a significant cognitive reframing that aligns with the more comprehensive perspectives held by PMs and PPs in Phase 1.

5.2.3 Shift 3: From Isolated to Supply-Chain-Wide Perspectives. The most dramatic transformation occurred in supply chain awareness. In their initial mental models, PIs did not discuss supply chain cybersecurity risks at all; this dimension was entirely absent from their discourse. PMs and PPs, by contrast, discussed their dependence on IT providers, reliance on foreign technology, and cascade effects in depth.

Post-scenario, supply chain awareness became a central concern of PIs. Participants recognized the interconnection: *“Supply chain + cybersecurity come hand in hand”* (PIA-RS) and *“that threats can come from further behind than just our direct supplier”* (PIJ-RS). There was *“Much more focus on sub-suppliers”* (PIJ-RS). Companies committed to implementing supplier security audits and expressed *“A whole new way of understanding the effect in the supply chain”* (PIA-RS). This shift, from complete absence to active engagement, represents the largest gap closure we observed and suggests that scenarios are particularly effective at making systemic, interconnected risks visible.

A related shift occurred from downstream to upstream focus. Initially, risk assessment (when available) focused on customer-facing risks. Post-scenario, PIs explicitly noted: *“Focus has shifted from only covering downstream to also including upstream”* (PIJ-RS). This bidirectional awareness aligns with the comprehensive supply chain perspective advocated by the NIST C-SCRM framework [71] and represents a meaningful advancement in SMEs’ conceptualization of their position within supply networks.

5.2.4 Shift 4: From Individual to Systemic Thinking. During the strategic foresight exercises, SMEs engaged with scenarios at a systemic level that was absent from their initial discussions. In the “US Disengagement from Europe” scenario, participants identified cascading dependencies, from incomplete European supply chains to workforce impacts arising from potential military conscription. In the “AI Out of Control” scenario, they discussed vendor verification challenges and the erosion of tacit knowledge through over-automation. Participants recognized that their companies existed within broader geopolitical, economic, and technological systems that shaped their cybersecurity risk exposure in ways they had not previously considered.

PIA captured this shift: *“But the case studies with the thought examples actually pinpointed all of the threats that we are thinking about in daily life and became much more alive and created an awareness when everything is put down on two pages.”*

5.2.5 Shift 5: From Informal to Structured Approaches. Initially, only 3 of 12 PI companies had formal cybersecurity training programs. Most relied on informal communication. PI.F explained: “we’re only seven people. We’re not 300 people [...] we’re not LEGO [...] we’re a small organization.” PI.D-RS wrote: “Raise awareness: verbal communication on phishing attempts. No training.”

Post-scenario, several companies indicated plans to retire informal approaches in favor of structured programs. Participants identified specific needs including “Awareness training” (PI.C-RS), “Proper cybersecurity training” (PI.K-RS), and “Seminars and risk training” (PI.J-RS). A notable finding was increased recognition of leadership involvement, with companies planning to “Clearly communicate guidelines & practices, foster a culture of see it, say it, sorted” (PI.K-RS). This represents a shift from viewing cybersecurity as an individual responsibility (typically the CEO or an IT-literate employee) to an organizational capability requiring structured governance.

5.2.6 Persistent Gap 1: The Cost-Investment Framing. Despite expanded threat awareness, the fundamental framing of cybersecurity as a cost rather than an investment remained unchanged. Post-scenario, while PIs identified many new actions they intended to implement, the underlying motivation remained compliance-driven. Regulatory requirements and cyber insurance, rather than strategic value, continued to shape cybersecurity investments. The scenarios expanded *what* PIs were aware of but did not change *how* they valued cybersecurity.

This suggests that awareness of threats, even when vivid and contextualized, does not automatically translate into reframing cybersecurity as a business enabler. The cost-investment framing appears to be a “deep structural” mental model dimension rooted in resource constraints and business incentive structures, rather than in information deficits.

5.2.7 Persistent Gap 2: Cross-Stakeholder Communication. In their initial mental models, no PI mentioned the Danish Center for Cyber Security (SAMSIK) when discussing challenges or guidance sources, despite PMs and PPs identifying it as a national coordination point. This communication gap persisted: the scenarios improved PI-level understanding within companies but did not create dialogue between stakeholder levels. PIs remained unaware of national resources, and the information asymmetry between the policy and implementation levels remained unchanged.

This gap has a structural explanation: the scenario intervention engaged PIs in intra-company and inter-company discussion (through the plenum sessions), but did not involve PM or PP participants in the same setting. The mental model transformation occurred within the PI level, not across levels. This suggests that interventions aimed at bridging stakeholder gaps must expand on this work and explicitly design for cross-level interactions.

5.2.8 Persistent Gap 3: Resource Reality. During the strategic foresight exercises, SMEs themselves articulated the limits of awareness-based interventions. Discussing the “US Disengagement from Europe” scenario, participants concluded it would be “very difficult for a 25-person company to survive in this scenario, because they would not have the internal competencies or resources to make the necessary changes.” A few companies explicitly reported no change in their

risk assessment approach: “We don’t think that we will change our assessing and prioritizing” (PI.G-RS).

Scenarios revealed the *scale* of challenges but could not resolve the material resource constraints that prevent SMEs from acting on expanded awareness. This finding has important implications: interventions that improve understanding without providing practical support mechanisms may increase anxiety without enabling action.

6 DISCUSSION

6.1 A Two-Tier Model of Mental Model Transformation

Our results reveal a striking pattern: all five dimensions that transformed through the scenario intervention, threat perception, supply chain awareness, risk assessment, systemic thinking, and training orientation involve expanding participants’ awareness. By contrast, the three dimensions that proved resistant, cybersecurity valuation, cross-stakeholder communication, and resource constraints, involve changing how participants and organizations act on that awareness. This asymmetry suggests that not all dimensions of a mental model respond equally to the same intervention.

We propose that cybersecurity mental models operate at two tiers. **Surface-level mental models** concern which threats exist, which vulnerabilities are relevant, and which responses are available. These are amenable to transformation through scenario-based interventions. **Deep structural mental models** concern how cybersecurity is valued relative to other business priorities, how resources are allocated, and how stakeholder communication operates. These are resistant to scenario-based intervention.

Building on the surface-versus-structural established in Section 2.3, itself a specific instance of the broader functional-versus-structural axis identified by Hu et al. [45], our contribution is to show that these two levels of a cybersecurity mental model respond differently to the same intervention. While prior work has organized mental-model variation around function versus structure and expertise [45], we organize it around responsiveness to a scenario-based intervention and extend the unit of analysis from the individual user to the organization.

6.2 The Asymmetry of Transformation

The asymmetry between what changed and what persisted carries both theoretical and practical significance. All five transformed dimensions share a common feature: they involve *expanding the scope of awareness*, seeing more threats, recognizing more connections, and acknowledging more actors. The persistent dimensions, by contrast, involve *changing the terms of engagement*, revaluing cybersecurity, restructuring communication, and reallocating resources. The former requires cognitive expansion; the latter requires institutional change. This distinction resonates with established findings in HCI and cybersecurity research. Sasse [92] argued that “scaring and bullying people into security won’t work,” and Renaud and Dupuis [84] demonstrated that fear appeals are unexpectedly complicated. Our findings extend this insight: even vivid, contextualized, non-fear-based interventions (scenario narratives) face limits when the barriers are structural rather than cognitive. The “knowing is not the same as doing” paradox [84] operates not just at the

individual level but at the organizational and inter-organizational levels.

6.3 Design Implications for Cybersecurity Interventions

6.3.1 Design for the Right Tier. Scenario-based interventions are effective for surface-level transformation of mental models. They should be deployed when the goal is to expand threat awareness, build supply chain visibility, or shift from a reactive to a proactive posture. However, they are insufficient for deep structural change. Interventions targeting the cost-investment framing, for example, may need to work through business case development, graduated compliance frameworks, or sector-specific incentive structures rather than awareness-based approaches.

6.3.2 Design for Stakeholder-Level Differences. Our findings confirm that one-size-fits-all interventions will not address multi-stakeholder concerns; intra-level interventions, even when effective, can improve cybersecurity and national resilience. PPs require translation mechanisms and tools to convert policy language into operational guidance that SMEs can act on. PIs need contextualized, scenario-based learning with concrete, proportionate actions. Cybersecurity tools and interventions should be stakeholder-adaptive, offering varied entry points and framing for different audiences.

6.3.3 Design for Cross-Level Interaction. The persistent PM–PI communication gap underscores that intra-level interventions, even when effective, do not bridge inter-level gaps. Future cybersecurity interventions should aim to create opportunities for multiple stakeholder levels to engage in shared experiences. One effective format could be scenario workshops, in which PMs, PPs, and PIs participate in the same scenarios and gain insights from each other’s perspectives. This would enable not just individual mental model transformation but alignment across stakeholders.

6.4 Design for Cultural Context

Denmark’s high-trust cultural context shaped both the initial mental models and the intervention’s dynamics. The “herring effect”, collective anonymity as a security strategy, reflects a cultural norm of collective rather than individual action. The effectiveness of the scenario workshops stemmed in part from this collaborative orientation: group discussions and plenum sharing leveraged cultural strengths. Interventions designed for low-trust environments [68, 69], which may emphasise individual responsibility and verification, would likely function differently in Nordic contexts. This suggests that cybersecurity intervention design must be culturally situated rather than culturally neutral.

6.5 Implications for HCI Research

Our work advances HCI cybersecurity research in three ways. First, we extend mental model research from individual cognition to the multi-stakeholder, inter-organisational level. Prior work studied how individual users understand threats [46, 103]; we show that the more consequential misalignments occur *between* stakeholder groups whose coordination is necessary for supply chain security. This reframing, moving from individual mental models

to stakeholder-ecosystem mental models, opens new territory for HCI investigation.

Second, we demonstrate the use of scenarios as a participatory HCI method for both *eliciting* and *transforming* mental models. Existing HCI methods elicit mental models through interviews, card sorting, or think-aloud protocols; scenarios add an interventional dimension, making them both research instruments and design tools. This dual function is valuable for HCI researchers working in domains where understanding must precede or accompany change.

Third, our finding that high-trust cultural contexts give rise to fundamentally different dynamics of mental models challenges the implicit universalism in much security design research. The “herring effect”, the trust paradox, and the effectiveness of collaborative scenario formats all depend on cultural features that are absent in the low-trust environments [68, 69] where most security interventions have been developed and evaluated. This suggests that the HCI community needs culturally comparative security research as a systematic program, rather than as occasional case studies.

6.6 Applicability and Efficiency of the Scenario Workshop Method

Our study was qualitative, so we cannot quantify the magnitude of mental model change or benchmark it against effect sizes reported for other intervention types. This limitation is common in this area of research [19, 29, 84, 88, 89], since mental model change is difficult to measure directly [45, 85], and evaluations of workshop-based, game-based, and exercise-based cybersecurity training tend to rely on qualitative or self-reported outcomes rather than standardized measures [81].

We used focus group discussions, a naturalistic method (Section 2.3), because our research questions required capturing *change* in a mental model across an intervention, not merely its state at a single point in time. Usability-oriented methods such as card sorting or path diagramming are well suited to characterizing the structure of a mental model, but administering them before and after our intervention would have captured shifts in surface-level categorization without surfacing the reasoning behind them; the plenum discussion in our design is what revealed, for instance, the persistent PM–PI communication gap underlying C2 and C3. A purely experimental or survey-based design could instead have yielded a quantifiable effect size, but at the cost of the qualitative depth needed to distinguish which dimensions of a mental model transform from which resist change, a distinction our two-tier model depends on.

Some related formats offer partial points of comparison. Angafor et al. reviewed tabletop-exercise-based serious games for cybersecurity incident response training [2], and Stals et al. evaluated a multi-day serious game jam for building cybersecurity understanding [95]. Neither study measures time cost relative to effectiveness, and, to our knowledge, no existing work compares workshop-based interventions with alternative formats specifically for changing organizational mental models. A quantitative comparison of our method against alternatives, such as tabletop exercises, e-learning modules, card-sorting studies, or single-organization workshops, remains an open direction for future work.

Our sessions were conducted in person. Future work should explore whether asynchronous or online scenario-based interventions, such as self-guided narratives or short scenario videos delivered remotely, can achieve a similar superficial transformation at significantly lower costs for participants. Additionally, we should investigate how the trade-off between engagement depth and efficiency varies across different formats. Conducting remote sessions with a similar mix of department heads and senior leadership could help reduce coordination and travel costs for each organization. This approach could also extend our methods to a larger and more geographically diverse set of companies. Furthermore, it would enable more systematic or longitudinal measurement of changes in mental models than the current qualitative design allows. We could enhance our approach by incorporating a follow-up survey, similar to the one used by Wash and Rader [105], to provide a quantitative measure of change over time.

6.7 Limitations

Several limitations should be acknowledged. First, Phase 2 assessed self-reported changes in understanding and intended practices, not actual behavioral change. Whether the mental model shifts we documented translate into sustained organizational practices remains an open question. Second, our sample represents self-selected companies with prior interest in cybersecurity, potentially biasing results toward organizations more receptive to change. Third, this study was conducted in Denmark's defence sector, characterized by specific cultural, regulatory, and geopolitical features. Findings may not generalize to other sectors or cultural contexts. Fourth, our design allowed SMEs to select scenarios based on perceived business relevance. Companies that chose politically oriented scenarios exhibited greater engagement with geopolitical risk dimensions, whereas those selecting technical scenarios engaged more with technology governance. This self-selection may have reinforced existing mental model orientations rather than challenging them across all dimensions; future designs might consider mandating exposure to scenarios outside participants' comfort zones. Finally, the single-country design limits cross-cultural comparisons.

7 CONCLUSION

This paper presents the first study of the transformation of cybersecurity mental models across multiple stakeholder levels. Through a two-phase study with 45 participants in Denmark's defence supply chain, we traced how scenario-based interventions reshape SMEs' understanding, evaluation, and intended responses to cybersecurity threats.

We identified five dimensions of substantial transformation: from reactive to proactive postures, from technical to holistic threat understanding, from isolated to supply-chain-wide perspectives, from individual to systemic thinking, and from informal to structured approaches. We also identified three dimensions that persisted despite intervention: the cost-investment framing, cross-stakeholder communication gaps, and resource constraints.

We propose a two-tier model of mental model transformation. Scenario-based interventions operate effectively on surface-level dimensions, expanding the scope of what stakeholders perceive and

consider, but leave deeper structural dimensions, rooted in institutional arrangements and resource realities, largely intact. This has direct practical implications: different tiers of mental models require different intervention designs. Expanding awareness requires experiential, contextualized methods like scenarios; changing valuation and institutional structures requires complementary approaches operating at the policy, incentive, and governance levels.

For the HCI community, our work demonstrates that mental model research can extend productively beyond individual cognition to organizational and inter-organizational levels, revealing governance-to-implementation gaps invisible from any single stakeholder perspective. For practitioners and policymakers, we provide evidence that scenario-based exercises are effective tools for transforming cybersecurity awareness in SMEs, but they must be paired with structural support to translate awareness into sustained action.

Future research should pursue three directions. First, longitudinal studies should track whether the mental model transformations we documented persist over time and translate into measurable organizational practices, moving from self-reported intentions to observed behaviors. Second, cross-cultural replications, particularly contrasting high-trust Nordic contexts with lower-trust environments, would test whether the two-tier model generalizes or whether cultural context modulates which dimensions are surface-level versus structural. Third, the development of stakeholder-adaptive cybersecurity intervention tools that combine scenario-based methods with cross-level dialogue mechanisms and structural support for resource-constrained SMEs represents a promising design research agenda that directly addresses the limitations identified in our study.

Acknowledgments

We appreciate the contributions of all participants, including Denmark's defence policymakers, industry experts, and representatives from small and medium-sized enterprises, for sharing their valuable insights. This project received funding from the Danish Industry Foundation under grant number 2023-0393. Additionally, it was supported by the Topic Engineering Secure Systems, precisely subtopic 46.23.01 Methods for Engineering Secure Systems, of the Helmholtz Association (HGF), as well as the KASTEL Security Research Labs.

References

- [1] Muhammad Amer, Tugrul U. Daim, and Antonie Jette. 2013. A review of scenario planning. *Futures* 46 (2013), 23–40.
- [2] Gideon N. Angafor, Iryna Yevseyeva, and Ying He. 2020. Game-based learning: A review of tabletop exercises for cybersecurity incident response training. *Security and privacy* 3, 6 (2020).
- [3] Farzaneh Asgharpour, Debin Liu, and L. Jean Camp. 2007. Mental models of security risks. In *Financial Cryptography and Data Security (FC 2007 / USEC 2007) (Lecture Notes in Computer Science, Vol. 4886)*. Springer, 367–377. doi:10.1007/978-3-540-77366-5_34
- [4] Hanieh Atashpanjeh, Rizu Paudel, and Mahdi Nasrullah Al-Ameen. 2025. Mental Model-Based Designs: The Study in Privacy Policy Landscape. *International Journal of Human-Computer Interaction* 41, 12 (2025), 7253–7272. doi:10.1080/10447318.2024.2392064
- [5] Maria Bada and Jason R.C. Nurse. 2019. Developing Cybersecurity Education and Awareness Programmes for Small- and Medium-Sized Enterprises (SMEs). *Information & Computer Security* 27, 3 (2019), 393–410.
- [6] Ozlem Bak, Sarah Shaw, Claudia Colicchia, and Vikas Kumar. 2023. A Systematic Literature Review of Supply Chain Resilience in Small-Medium Enterprises (SMEs): A Call for Further Research. *IEEE Transactions on Engineering Management* 70, 1 (2023), 328–341. doi:10.1109/TEM.2020.3016988

- [7] M. Benz and D. Chatterjee. 2020. Calculated risk? a cybersecurity evaluation tool for SMEs. *Business Horizons* 63, 4 (2020), 531–540.
- [8] Sander Boyson. 2014. Cyber Supply Chain Risk Management. *Technovation* 34, 7 (2014), 342–353.
- [9] Virginia Braun and Victoria Clarke. 2012. Thematic Analysis. In *APA Handbook of Research Methods in Psychology*. Vol. 2. American Psychological Association, 57–71.
- [10] Cristian Bravo-Lillo, Lorrie Faith Cranor, Julie Downs, and Saranga Komanduri. 2011. Bridging the Gap in Computer Security Warnings: A Mental Model Approach. *IEEE Security & Privacy* 9, 2 (2011), 18–26. doi:10.1109/MSP.2010.198
- [11] Jessica E. Brodsky, Arshia K. Lodhi, Kasey L. Powers, Fran C. Blumberg, and Patricia J. Brooks. 2021. "It's just everywhere now": Middle-school and college students' mental models of the Internet. *Human Behavior and Emerging Technologies* 3, 4 (2021), 495–511. arXiv:https://onlinelibrary.wiley.com/doi/pdf/10.1002/hbe2.281 doi:10.1002/hbe2.281
- [12] L. Jean Camp. 2009. Mental Models of Privacy and Security. *IEEE Technology and Society Magazine* 28, 3 (2009), 37–47.
- [13] Jaime Carbonell, Antonio Sánchez-Esguevillas, and Belén Carro. 2017. From data analysis to storytelling in scenario building: a semiotic approach to purpose-dependent writing of stories. *Futures* 88 (2017), 15–29.
- [14] Centre for Cyber Security. 2024. *Threat Assessment Report*. Technical Report. CFCS.
- [15] Centre for Cyber Security (CFCS) now (SAMSİK). 2021. *SolarWinds: State-sponsored Global Software Supply Chain Attack* (1 ed.). Technical Report. Centre for Cyber Security (CFCS), Danish Defence Intelligence Service. https://samsik.dk/wp-content/uploads/2026/01/20211105_CFCS-solarwinds-report-EN.pdf Accessed: May 2026.
- [16] Thomas J. Chermack. 2011. *Scenario Planning in Organizations*. Berrett-Koehler Publishers.
- [17] Martin Christopher, Carlos Mena, Omera Khan, and Oznur Yurt. 2011. Approaches to Managing Global Sourcing Risk. *Supply Chain Management: An International Journal* 16, 2 (2011), 67–81.
- [18] Hashim Iqbal Chunpir and Thomas Ludwig. 2017. *A Software to Capture Mental Models*. Springer International Publishing, 393–409. doi:10.1007/978-3-319-58700-4_32
- [19] Richard K. Coll, Peter J. Aubusson, Allan G. Harrison, and Stephen M. Ritchie. 2006. The role of models, mental models and analogies in chemistry teaching. In *Metaphor and Analogy in Science Education*. Springer Netherlands, Dordrecht, 65–77.
- [20] Dennis Coliaris, Hilde J.P. Weerts, Daphne Miedema, Jarke J. van Wijk, and Mykola Pechenizkiy. 2022. Characterizing Data Scientists' Mental Models of Local Feature Importance. In *Nordic Human-Computer Interaction Conference* (Aarhus, Denmark) (NordiCHI '22). Association for Computing Machinery, New York, NY, USA, Article 9, 12 pages. doi:10.1145/3546155.3546670
- [21] Kovila P. L. Coopamootoo and Thomas Groß. 2014. Mental Models for Usable Privacy: A Position Paper. In *Human Aspects of Information Security, Privacy, and Trust*, Theo Tryfonas and Ioannis Askoxylakis (Eds.). Springer International Publishing, Cham, 410–421.
- [22] Alessandro Creazza, Claudia Colicchia, Salvatore Spiezia, and Fabrizio Dallari. 2022. Who Cares? Supply Chain Managers' Perceptions Regarding Cyber Supply Chain Risk Management. *Supply Chain Management: An International Journal* 27, 1 (2022), 30–53.
- [23] Danish Business Authority. 2023. *Digital sikkerhed i danske SMV'er*. Technical Report. Danish Business Authority.
- [24] Danish Government. 2022. National Strategy for Cyber and Information Security 2022–2024. https://database.cyberpolicyportal.org/api/files/1659689698478vt8ejxidu2.pdf Accessed: 2025-07-11.
- [25] Danish Ministry of Defence. 2023. Danish Defence Agreement 2024–2033. https://www.fmn.dk/globalassets/fmn/dokumenter/forlig/-danish-defence-agreement-2024-2033-.pdf Verify exact agreement date.
- [26] Danish Ministry of Defence. 2025. *Agreement Putting Denmark at More Than 3 pct. of GDP Allocated for Defence in 2025 and 2026*. https://www.fmn.dk/en/news/2025/agreement-putting-denmark-at-more-than-3-pct.-of-gdp-allocated-for-defence-in-2025-and-2026
- [27] Sergej Dechand, Alena Naiakshina, Anastasia Danilova, and Matthew Smith. 2019. In Encryption We Don't Trust: The Effect of End-to-End Encryption to the Masses on User Perception. In *2019 IEEE European Symposium on Security and Privacy (EuroSec&P)*. IEEE, 401–415. doi:10.1109/eurosp.2019.00037
- [28] Toshihisa Doi, Keisuke Ishihara, and Toshiki Yamaoka. 2013. *Verification of the Questionnaire for the Level of Mental Models Building*. Springer Berlin Heidelberg, 105–108. doi:10.1007/978-3-642-39473-7_22
- [29] Paul Dourish, Rebecca E. Grinter, Jessica Delgado de la Flor, and Melissa Joseph. 2004. Security in the wild: user strategies for managing security as an everyday, practical problem. *Personal and ubiquitous computing* 8, 6 (2004), 391–401.
- [30] European Parliament and Council of the European Union. 2022. Directive (EU) 2022/2555 on Measures for a High Common Level of Cybersecurity Across the Union (NIS2 Directive). Official Journal of the European Union, L 333, 80–152. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02022L2555-20221227
- [31] European Union Agency for Cybersecurity. 2025. *ENISA Threat Landscape 2025*. Technical Report. ENISA. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025 Version 1.2, revised 9 January 2026.
- [32] European Union Agency for Cybersecurity (ENISA). 2021. *ENISA Threat Landscape for Supply Chain Attacks*. Technical Report. European Union Agency for Cybersecurity, Athens, Greece. doi:10.2824/168593
- [33] Morten Falch, Henning Olesen, Knud Erik Skouby, Reza Tadayoni, and Idongesit Williams. 2022. Cybersecurity in SMEs in the Baltic Sea Region. In *ITS 31st European Conference 2022*. International Telecommunications Society, International Telecommunications Society, Gilford, NH, 1–20.
- [34] Linda Finlay. 2002. "Outing" the Researcher. *Qualitative Health Research* 12, 4 (2002), 531–545.
- [35] Organisation for Economic Co-operation and Development (OECD). 2020. Enhancing the contributions of SMEs in a global and digitalised economy. https://www.oecd.org/industry/smes/. Accessed: 2025-07-10.
- [36] Jorrit Geels. 2024. Ordinary Users Do Not Understand Digital Signatures. In *Proceedings of the 13th Nordic Conference on Human-Computer Interaction* (Uppsala, Sweden) (NordiCHI '24). Association for Computing Machinery, New York, NY, USA, Article 66, 15 pages. doi:10.1145/3679318.3685402
- [37] Abhijeet Ghadge, Maximilian Weiß, Nigel D. Caldwell, and Richard Wilding. 2020. Managing Cyber Risk in Supply Chains: A Review and Research Agenda. *Supply Chain Management: An International Journal* 25, 2 (2020), 223–240.
- [38] M. Ghobakhloo. 2018. The future of manufacturing industry: a strategic roadmap toward Industry 4.0. *Journal of Manufacturing Technology Management* 29, 6 (2018), 910–936.
- [39] S. Gorgels, M. Priem, T. Blagoeva, M. Martinelle, and G. Milanese. 2022. *Annual Report on European SMEs 2021/2022 - SMEs and Environmental Sustainability: Background Document*. Technical Report. European Commission, Brussels.
- [40] Ayako A. Hasegawa, Daisuke Inoue, and Mitsuaki Akiyama. 2024. How WEIRD is Usable Privacy and Security Research?. In *33rd USENIX Security Symposium (USENIX Security 24)*. USENIX Association, Philadelphia, PA, 3241–3258. https://www.usenix.org/conference/usenixsecurity24/presentation/hasegawa
- [41] Margareta Heidt, Jin P. Gerlach, and Peter Buxmann. 2019. Investigating the Security Divide between SME and Large Companies. *Information Systems Frontiers* 21 (2019), 1285–1305.
- [42] Max Herburger, Andreas Wieland, and Christian Hochstrasser. 2024. Building Supply Chain Resilience to Cyber Risks: A Dynamic Capabilities Perspective. *Supply Chain Management: An International Journal* 29, 7 (2024), 28–50.
- [43] Robert R. Hoffman, Shane T. Mueller, Gary Klein, and Jordan Litman. 2019. Metrics for Explainable AI: Challenges and Prospects. arXiv:1812.04608 [cs.AI] https://arxiv.org/abs/1812.04608
- [44] Geert Hofstede. 2011. Dimensionalizing Cultures: The Hofstede Model in Context. *Online Readings in Psychology and Culture* 2, 1 (Dec. 2011). doi:10.9707/2307-0919.1014
- [45] Xinhui Hu and Michael Twidale. 2023. A Scoping Review of Mental Model Research in HCI from 2010 to 2021. In *HCI International 2023 - Late Breaking Papers*, Masaaki Kurosu, Ayako Hashizume, Aaron Marcus, Elizabeth Rosenzweig, Marcelo M. Soares, Don Harris, Wen-Chin Li, Dylan D. Schmorow, Cali M. Fidopiastis, and Pei-Luen Patrick Rau (Eds.). Springer Nature Switzerland, Cham, 101–125.
- [46] Iulia Ion, Rob Reeder, and Sunny Consolvo. 2015. "...No One Can Hack My Mind": Comparing Expert and Non-Expert Security Practices. In *Proceedings of the Eleventh Symposium on Usable Privacy and Security*. USENIX.
- [47] James Jenness, John Lenneman, Amy Benedick, Richard Huey, Joshua Jaffe, Jeremiah Singer, and Sarah Yehoodik. 2019. *Spaceship, Guardian, Coach: Drivers' Mental Models of Advanced Vehicle Technology*. Springer International Publishing, 351–356. doi:10.1007/978-3-030-23525-3_46
- [48] Jay Dee Johns. 2017. Strategic Design: Breaking Mental Models Initiates Learning in Video Games. In *Learning and Collaboration Technologies. Novel Learning Ecosystems*, Panayiotis Zaphiris and Andri Ioannou (Eds.). Springer International Publishing, Cham, 443–461.
- [49] Philip N. Johnson-Laird. 1980. Mental Models in Cognitive Science. *Cognitive Science* 4, 1 (1980), 71–115.
- [50] Bruce D. Jones. 2026. *Seabed Zero: Baltic Sabotage and the Global Risks to Undersea Infrastructure*. Bulletin of the Atomic Scientists. https://thebulletin.org/2026/02/seabed-zero-baltic-sabotage-and-the-global-risks-to-undersea-infrastructure/
- [51] Carlos Rombaldo Junior, Ingolf Becker, and Shane Johnson. 2023. Unaware, Unfunded and Uneducated: A Systematic Review of SME Cybersecurity. doi:10.48550/ARXIV.2309.17186
- [52] Ruogu Kang, Laura Dabbish, Nathaniel Fruchter, and Sara Kiesler. 2015. "My Data Just Goes Everywhere:" User Mental Models of the Internet and Implications for Privacy and Security. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*. USENIX Association, Ottawa, 39–52. https://www.usenix.org/conference/sonp2015/proceedings/presentation/kang

- [53] Judith Kankam-Boateng, Marco Peressotti, Jan Stentoft, Kent Adsbøll Wickstrøm, Vincent Charles Keating, Louise Alison Tumchewics, Olivier Schmitt, Amelie Theussen, and Peter Mayer. 2026. 'It's Confusing, Insecure, and Messy' - Mapping the Gaps Between Stakeholders' Cybersecurity Mental Models in the Danish Defence Sector. In *Proceedings of the 2026 CHI Conference on Human Factors in Computing Systems*. 1–26. doi:10.1145/3772318.3791032
- [54] Irni Eliana Khairuddin, Corina Sas, and Chris Speed. 2019. BlockKit: A Physical Kit for Materializing and Designing for Blockchain Infrastructure. In *Proceedings of the 2019 on Designing Interactive Systems Conference (DIS '19)*. ACM, 1449–1462. doi:10.1145/3322276.3322370
- [55] Laura Kocksch and Torben Elgaard Jensen. 2024. The Mundane Art of Cybersecurity: Living with Insecure IT in Danish Small- and Medium-Sized Enterprises. *Proc. ACM Hum.-Comput. Interact.* 8, CSCW2, Article 354 (Nov. 2024), 17 pages. doi:10.1145/3686893
- [56] Christie Kodama, Beth St. Jean, Mega Subramaniam, and Natalie Greene Taylor. 2017. There's a creepy guy on the other end at Google!: engaging middle school students in a drawing activity to elicit their mental models of Google. *Information Retrieval Journal* 20, 5 (May 2017), 403–432. doi:10.1007/s10791-017-9306-x
- [57] Franklin D. Kramer and Hans Binnendijk. 2026. *NATO Needs to Define the Substance of Its 1.5 Percent Pledge*. Atlantic Council. <https://www.atlanticcouncil.org/dispatches/nato-needs-to-define-the-substance-of-its-1-5-percent-pledge/>
- [58] Katharina Krombholz, Karoline Busse, Katharina Pfeffer, Matthew Smith, and Emanuel von Zezschwitz. 2019. "If HTTPS Were Secure, I Wouldn't Need 2FA" - End User and Administrator Mental Models of HTTPS. In *2019 IEEE Symposium on Security and Privacy (SP)*. 246–263. doi:10.1109/SP.2019.00060
- [59] Todd Kulesza, Simone Stumpf, Margaret Burnett, Sherry Yang, Irwin Kwan, and Weng-Keen Wong. 2013. Too much, too little, or just right? Ways explanations impact end users' mental models. In *2013 IEEE Symposium on Visual Languages and Human-Centric Computing*. 3–10. doi:10.1109/VLHCC.2013.6645235
- [60] T.J. Kull, J. Kotlar, and M. Spring. 2018. Small and medium enterprise research in supply chain management: the case for single-respondent research designs. *Journal of Supply Chain Management* 54, 1 (2018), 23–34.
- [61] Ling-Ling Lai. 2018. *How Do They Tag? Senior Adults' Tagging Behavior in Cultural Heritage Information*. Springer International Publishing, 475–484. doi:10.1007/978-3-319-91716-0_38
- [62] Yi-Ching Lee and Lindsey A. Malcein. 2020. Users' mental models for <scp>computer-mediated/</scp> communication: Theorizing emerging technology and behavior in <scp>eHealth/</scp> applications. *Human Behavior and Emerging Technologies* 2, 4 (Aug. 2020), 354–366. doi:10.1002/hbe2.212
- [63] M. Löfving, K. Säfsten, and M. Winroth. 2014. Manufacturing strategy frameworks suitable for SMEs. *Journal of Manufacturing Technology Management* 25, 1 (2014), 7–26.
- [64] Ren Long, Xu Liu, Tian Lei, Xue Chen, and Ziliang Jin. 2017. *The Impact of Chinese Traditional Cultural on the Gesture and User Experience in Mobile Interaction Design*. Springer International Publishing, 49–58. doi:10.1007/978-3-319-57931-3_5
- [65] Dimitra Markopoulou, Vagelis Papakonstantinou, and Paul de Hert. 2019. The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation. *Computer Law & Security Review* 35, 6 (2019), 105336. doi:10.1016/j.clsr.2019.06.007
- [66] Karola Marky, Sarah Prange, Max Mühlhäuser, and Florian Alt. 2021. Roles Matter! Understanding Differences in the Privacy Mental Models of Smart Home Visitors and Residents. In *20th International Conference on Mobile and Ubiquitous Multimedia (MUM 2021)*. doi:10.1145/3490632.3490664
- [67] S.A. Melnyk, T. Schoenherr, C. Speier-Perob, C. Peters, J.F. Chang, and D. Friday. 2022. New challenges in supply chain management: cybersecurity across the supply chain. *International Journal of Production Research* 60, 1 (2022), 162–183.
- [68] Erin Meyer. 2014. Navigating the Cultural Minefield. *Harvard Business Review* 92, 5 (2014).
- [69] Erin Meyer. 2015. *The Culture Map*. PublicAffairs.
- [70] Gert Læssøe Mikkelsen, Lars Syberg, Laura Lynggaard Nielsen, Michael Adsetts Edberg Hansen, Michael Hjortlund, Ole Lehmann Madsen, Peter Høngaard Andersen, and Tore Duvold. 2018. *The Future Market for Cybersecurity in Denmark*. Technical Report. Innovation Fund Denmark, Deloitte, and Alexandra Institute. 44 pages. <https://innovationsfonden.dk/sites/default/files/2018-07/thefuturemarketforcybersecurityindenmark.pdf>
- [71] National Institute of Standards and Technology. 2024. *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*. Technical Report. U.S. Department of Commerce.
- [72] National Institute of Standards and Technology. 2024. *The NIST Cybersecurity Framework (CSF) 2.0*. Technical Report. U.S. Department of Commerce.
- [73] Donald A. Norman. 1983. Some Observations on Mental Models. In *Mental Models*, Dedre Gentner and Albert L. Stevens (Eds.). Lawrence Erlbaum Associates, Hillsdale, NJ, 7–14.
- [74] Esteban Ortiz-Ospina and Max Roser. 2016. Trust. *Our World in Data* (2016). <https://ourworldindata.org/trust>
- [75] Anna-Marie Orloff et al. 2025. A Replication of "No One Can Hack My Mind" – Ten Years Later. In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems*. ACM.
- [76] Nils Pancratz and Ira Diethelm. 2020. "Draw us how smartphones, video gaming consoles, and robotic vacuum cleaners look like from the inside": students' conceptions of computing system architecture. In *Proceedings of the 15th Workshop on Primary and Secondary Computing Education (Virtual Event, Germany) (WiP-SCE '20)*. Association for Computing Machinery, New York, NY, USA, Article 12, 10 pages. doi:10.1145/3421590.3421600
- [77] Niki Panteli, Besiki R. Nthubu, and Konstantinos Mersinas. 2025. Being Responsible in Cybersecurity: A Multi-Layered Perspective. *Information Systems Frontiers* (2025).
- [78] Sean Peisert, Bruce Schneier, Hamed Okhravi, Fabio Massacci, Terry Benz, Carl Landwehr, Mohammad Mannan, Jelena Mirkovic, Atul Prakash, and James Bret Michael. 2021. Perspectives on the SolarWinds Incident. *IEEE Security & Privacy* 19, 2 (2021), 7–13. doi:10.1109/MSEC.2021.3051235
- [79] John L. Petersen, Karlheinz Steinmüller, and Hazel Adeyema. 2009. Wild cards. In *Futures Research Methodology - Version 3*, Jerome C. Glenn and Theodore J. Gordon (Eds.). The Millennium Project, New York.
- [80] Shardul Phadnis and Nitin Joglekar. 2021. Configuring supply chain dyads for regulatory disruptions: a behavioral study of scenarios. *Production and Operations Management* 30, 4 (2021), 1014–1033.
- [81] Julia Prümmer, Tommy van Steen, and Bibi van den Berg. 2024. A systematic review of current cybersecurity training methods. *Computers & security* 136 (2024), 103585–.
- [82] Xiaofan Qian, Ying Yang, and Yong Gong. 2011. The art of metaphor: a method for interface design based on mental models. In *Proceedings of the 10th International Conference on Virtual Reality Continuum and Its Applications in Industry (VRCAI '11)*. ACM, 171–178. doi:10.1145/2087756.2087780
- [83] Nisha Rawindaran, Ambikesh Jayal, and Edmond Prakash. 2023. Cybersecurity Challenges in SMEs. *Journal of Cybersecurity and Privacy* (2023).
- [84] Karen Renaud and Marc Dupuis. 2023. Cyber Security Fear Appeals: Unexpectedly Complicated. *Computers & Security* 124 (2023), 103326.
- [85] Karen Renaud, Cigdem Sengul, Kovila Coopamootoo, Bryan Clift, Jacqui Taylor, Mark Springett, and Ben Morrison. 2024. "We're Not That Gullible!" Revealing Dark Pattern Mental Models of 11-12-Year-Old Scottish Children. *ACM Transactions on Computer-Human Interaction* 31, 3 (2024), 1–41. doi:10.1145/3660342
- [86] Adriano Bernardo Renzi and Sydney Freitas. 2014. *Affordances and Gestural Interaction on Multi-touch Interface Systems: Building New Mental Models*. Springer International Publishing, 615–623. doi:10.1007/978-3-319-07626-3_58
- [87] Laura Rook. 2013. Mental models: a robust definition. *The Learning Organization* 20, 1 (Jan. 2013), 38–47. doi:10.1108/09696471311288519
- [88] William B. Rouse and Nancy M. Morris. 1986. On looking into the black box: Prospects and limits in the search for mental models. *Psychological Bulletin* 100, 3 (Nov. 1986), 349–363. doi:10.1037/0033-2909.100.3.349
- [89] Anna L. Rowe and Nancy J. Cooke. 1995. Measuring mental models: Choosing the right tools for the job. *Human Resource Development Quarterly* 6, 3 (1995), 243–255. doi:10.1002/hrdq.3920060303
- [90] Arash Safari, Ahmad Sedaghat, Behzad M. Shoja, and Sarah Oudjane. 2024. Supply Chain Cybersecurity Challenges: A Risk Assessment Perspective for SMEs. *Journal of Global Information Management* 32, 1 (2024), 1–21.
- [91] Johnny Saldaña. 2021. *The Coding Manual for Qualitative Researchers* (4th ed.). Sage Publications.
- [92] M. Angela Sasse. 2015. Scaring and Bullying People into Security Won't Work. *IEEE Security & Privacy* 13, 3 (2015), 80–83.
- [93] Andrea I. Scheiter, Jessica A. Linnemann, Uwe Herbst, and Klaus Bengler. 2020. Mental Model of Driving Wizards When Simulating an Automated Drive. In *Proceedings of the 11th Nordic Conference on Human-Computer Interaction: Shaping Experiences, Shaping Society* (Tallinn, Estonia) (NordiCHI '20). Association for Computing Machinery, New York, NY, USA, Article 56, 10 pages. doi:10.1145/3419249.3420158
- [94] Matthew J. Spaniol and Nicholas J. Rowland. 2018. The scenario planning paradox. *Futures* 95 (2018), 33–43.
- [95] Shenando Stals, Lynne Baillie, Jamie Iona Ferguson, Daisy Abbott, Manuel Maarek, Ryan Shah, and Sandy Louchart. 2025. Evaluating Serious Slow Game Jams as a Mechanism for Co-Designing Serious Games to Improve Understanding of Cybersecurity. *ACM Games: Research and Practice* 3, 1 (2025). doi:10.1145/3709745
- [96] Jan Stentoft et al. 2025. The Relationship Between Cybersecurity Awareness and Action in Danish SMEs. (2025).
- [97] J. Stentoft, K.A. Wickstrøm, K. Philipsen, and A. Haug. 2021. Drivers and barriers for Industry 4.0 readiness and practice: empirical evidence from small and medium-sized manufacturers. *Production Planning & Control* 32, 10 (2021), 811–828.
- [98] Stockholm Environment Institute. 2025. *Trends in Baltic Sea Collaboration Amid Geopolitical Tension*. <https://www.sei.org/features/baltic-sea-collaboration-geopolitics/>

- [99] Jan Willem Streefkerk, Nanja Smets, Michel Varkevisser, and Suzanne Hiemstravan Mastrigt. 2014. Future command and control systems should combine decision support and personalization interface features. In *Proceedings of the 8th Nordic Conference on Human-Computer Interaction: Fun, Fast, Foundational* (Helsinki, Finland) (NordiCHI '14). Association for Computing Machinery, New York, NY, USA, 266–275. doi:10.1145/2639189.2639197
- [100] Crystal Thomas and Thomas Chermack. 2019. Using scenario planning to supplement supply chain risk management. In *Revisiting Supply Chain Risk*, George A. Zsidisin and Michael Henke (Eds.). Springer Series in Supply Chain Management, Vol. 7. Springer, 37–51.
- [101] Joke Van Kerckhoven, Sabine Geldof, Bart Vermeersch, Philippe Palanque, Jean Vanderdonck, and Marco Winckler. 2010. Contextual Inquiry in Signal Boxes of a Railway Organization. In *HUMAN ERROR, SAFETY AND SYSTEMS DEVELOPMENT*, Vol. 5962. Springer Berlin Heidelberg, Berlin, Heidelberg, 96–106.
- [102] Pierre Wack. 1985. Scenarios: Uncharted Waters Ahead. *Harvard Business Review* 63, 5 (1985), 73–89.
- [103] Rick Wash. 2010. Folk Models of Home Computer Security. In *Proceedings of the Sixth Symposium on Usable Privacy and Security*. ACM.
- [104] Rick Wash and Emilee Rader. 2011. Influencing mental models of security: a research agenda. In *Proceedings of the 2011 New Security Paradigms Workshop* (Marin County, California, USA) (NSPW '11). Association for Computing Machinery, New York, NY, USA, 57–66. doi:10.1145/2073276.2073283
- [105] Rick Wash and Emilee Rader. 2015. Too Much Knowledge? Security Beliefs and Protective Behaviors Among United States Internet Users. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*. USENIX Association, Ottawa, 309–325. <https://www.usenix.org/conference/soups2015/proceedings/presentation/wash>
- [106] Bingjun Xie and Jia Zhou. 2017. *The Influence of Mental Model Similarity on User Performance: Comparing Older and Younger Adults*. Springer International Publishing, 569–579. doi:10.1007/978-3-319-58536-9_45
- [107] Svetlana Yarosh and Pamela Zave. 2017. Locked or Not?: Mental Models of IoT Feature Interaction. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI '17)*. ACM, 2993–2997. doi:10.1145/3025453.3025617
- [108] C. Zalengera, R. E. Blanchard, P. C. Eames, A. M. Juma, M. L. Chitawo, and K. T. Gondwe. 2014. Overview of the Malawi energy situation and a PESTLE analysis for sustainable development of renewable energy. *Renewable and Sustainable Energy Reviews* 38 (2014), 335–347.
- [109] Serena Zheng, Noah Apthorpe, Marshini Chetty, and Nick Feamster. 2018. User Perceptions of Smart Home IoT Privacy. *Proc. ACM Hum.-Comput. Interact.* 2, CSCW, Article 200 (Nov. 2018), 20 pages. doi:10.1145/3274469
- [110] Yixin Zou, Abraham H. Mhaidli, Austin McCall, and Florian Schaub. 2018. “I’ve Got Nothing to Lose”: Consumers’ Risk Perceptions and Protective Actions after the Equifax Data Breach. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*. USENIX Association, Baltimore, MD, USA, 197–216. <https://www.usenix.org/conference/soups2018/presentation/zou>

A APPENDIX

A.1 Informed Consent

Consent to participate in research and processing of personal data. In connection with the project Cybersikkerhed og Forretningskontinuitet, we want to collect your information. Our researchers, Peter Mayer, Judith Kankam-Boateng, Vincent Keating, and Louise Tumchewics, are responsible for the protection of sensitive data collected for the use in this research.

Participation in our project is voluntary. Data collection takes place through focus group discussions, follow-up interviews, and participant observation. Discussions will be recorded and then transcribed for qualitative analyses. As part of the transcription process, personal data will be removed from the transcripts to ensure that only anonymized data will be analyzed.

Purpose of processing information for the project. The purpose of this research is to evaluate the cybersecurity policies and practices in Denmark, to understand the practices and challenges associated with cybersecurity in Denmark. A secondary purpose is to develop the use of scenarios as a method of foresight analysis for cybersecurity in Danish enterprises. The information being processed is: The recordings of the focus groups/discussions and the follow-up

interviews for transcription. The transcriptions will then be analyzed using qualitative inductive coding. Notes generated from participant observation will be used as a secondary data source to confirm the context and interpretation of the transcripts.

How we use the information. The information is to be processed in accordance with the General Data Protection Regulation (GDPR) art. 6, (1)(a) and art. 9, (2)(a), which cover the rules of consent. The research team will treat the information with confidentiality in accordance with applicable law. We will keep the data secure so that only some researchers taking part in the project, listed above, will have access. The information will only be used for the purposes of the project.

Deletion and storage of your data. We will delete or anonymize the information when it is no longer relevant to keep. The transcription process will always remove identifying information from the transcripts. The anonymised information will be deleted, at the latest, five years after the end of the project, and will therefore be deleted on 28.02.2031. You may withdraw your consent if you wish to have your data deleted earlier before 28.02.2031, after which it may no longer be possible to remove your data from the dataset due to data deletion. Note that deletion of your data is not possible after it has been anonymised after the transcription process.

Please note

- that you can always withdraw your consent earlier before 28.02.2031, after which it may no longer be possible to remove your data from the dataset due to data deletion, which means the SDU is obligated to delete the information we have collected about you,
- that you have the right to see the data we have about you,
- that you have the right to request the rectification or deletion of data and
- that you have the right to appeal to the Danish Data Protection Agency about the processing of the information via www.datatilsynet.dk.

You always have the option of withdrawing your consent by writing to mayer@imada.sdu.dk.

Disclosure/other purposes. The collected data will only be shared beyond the research team of this project in anonymised form. The data will be stored in encrypted containers at all times after recording until deletion.

Publication. There will be no publication of data in which you can be personally identified. Your personal data is anonymised before being included in the publication of the results of the research. This means that it is not possible to retrieve your information in any publications. Excerpts from the transcripts might be used in publications, in which case attributions with will be made using anonymous identifiers, e.g., Participant 1.

More information. If you have any questions about the research, you can contact Peter Mayer at any time either via email or via phone. If you wish to file a complaint about the processing of personal data, you can contact the Danish Data Protection Agency via the anonymous university.

Declaration of consent.

- I understand that participation in the project is voluntary.
- I have read and understand the informed consent.
- I consent to participate in the research and the processing of the data.
- I understand that the collected data will only be shared beyond the research team of this project in anonymised form.

Date Name Signature

A.2 Interview Guide Questions for policymakers

Structure. 5 main questions with 2-4 sub questions for Q1 to Q4 and one main question for Q5.

Q1. What is your view on the overall state of cybersecurity in Denmark?

- Q1a. Who do you consider to be the main threats in this context?
 Q1b. How effectively do you think Denmark is equipped to counter these threats?
 Q1c. Do you view cybersecurity primarily as a cost or as an investment?

Q2. What are your thoughts on Denmark's current national cybersecurity strategy?

- Q2a. How effective do you find this strategy
 – The overall cybersecurity landscape
 – Cybersecurity in the public sector
 – Cybersecurity for private sector businesses, especially SMEs
 Q2b. Are there specific aspects that you think should have been included or highlighted in the strategy?
 Q2c. Considering the strategy covers a three-year period, do you believe this time-frame is appropriate?
 Q2d. What suggestions do you have for the development of the next national cybersecurity strategy?

Q3. How applicable are the NIS2 and NIST CSF 2.0 frameworks to Denmark's cybersecurity needs?

- Q3a. How does Denmark's readiness to manage international cybersecurity threats compare to other countries?
 Q3b. What distinct challenges does Denmark encounter in its cybersecurity initiatives?
 Q3c. In what ways does being a member of NATO affect Denmark's cybersecurity strategies?
 Q3d. What are the major areas where Denmark's cybersecurity measures fall short compared to other nations?

Q4) What resources do you rely on to inform your policy-making decisions?

- Q4a. How dependable are these resources?
 Q4b. What methods do you use to address discrepancies between different sources?

Q5) Is there effective Collaboration between the Public Sector, Businesses (especially SMEs), and Academic Institutions?

A.3 Interview Guide Questions for Policy Promoters

Structure. 5 main questions with 1-4 sub questions for Q1 to Q5.

Q1. How do you evaluate the current Danish Cybersecurity posture?

- Q1a. What are the key cybersecurity threats you identified?
 Q1b. To what extent are the defence sector equipped to defend against these threats?
 Q1c. Do you view cybersecurity as a financial cost or a strategic investment?

Q2. What is your perspective on Denmark's national cybersecurity strategy, and how does it impact the defence sector?

- Q2a. How effective do you find Denmark's national strategy for:
 – i. Influencing the overall industry landscape
 – ii. The public sector's influence on private-sector cybersecurity practices?
 – iii. Impacting SMEs within the defence sector?
 Q2b. Are there specific aspects of cybersecurity that you believe should be emphasised or included in future strategy plans?
 Q2c. What is your perspective on the strategic planning (national cybersecurity strategy) time-frame? Should it be longer or shorter?

Q3. How do you perceive the applicability and relevance of international cybersecurity frameworks like NIS2 and NIST CSF 2.0 for the Danish defence sector?

- Q3a. How does Denmark's readiness for international cybersecurity threats compare to other nations?
 Q3b. What unique challenges are faced by Denmark?
 Q3c. How does Denmark's NATO membership impact the cybersecurity strategies of the defence sector?
 Q3d. In your opinion, where does Denmark fall short of other countries in terms of cybersecurity?

Q4. Evaluate the level of collaboration between the public sector, private enterprises (especially SMEs), and research institutions.

Q4a. How can SMEs be supported in strengthening cybersecurity practices, e.g., by industry associations or other actors?

Q5. To what extent do Denmark's current policies effectively support SMEs in strengthening their cybersecurity measures to protect against cyber threats and attacks?

Q5a. What are the primary challenges or points of contention/friction between policies and companies regarding cybersecurity regulations, and how can these issues be effectively addressed?

A.4 Interview Guide Questions for Policy Implementers

Structure. We elicited their initial mental models in the morning with 6 main themes with 2-3 questions under each theme. Then the scenario exercises for treatment and finally the Post mental model with 6 main themes with 1 - 3 questions under each theme.

A.4.1 Initial Mental Models - Participant Response Sheet.

1) Understanding the Current Cybersecurity Posture and Practices.

Q1a. According to your current understanding, what are your organisation's cybersecurity practices, and the role cybersecurity plays in daily operations within your organisation?

Q1b. What are the key cybersecurity practices currently implemented, and what are your main concerns or priorities related to cybersecurity?

2) Threats, Vulnerabilities, and Preparedness.

Q1a. What do you perceive as the most significant cybersecurity threats to your organisation?

Q2b. How seriously do you think your colleagues take these cybersecurity threats?

Q2c. In your opinion, how prepared do you feel your organisation is to handle cybersecurity incidents?

3) Training, Awareness, and Communications.

Q3a. In what ways does your organisation train employees and raise awareness about cybersecurity? In your opinion, how effective do you feel these training and awareness efforts are?

Q3b. How are these issues communicated within your organisation? In your opinion, how effective do you feel these communication efforts are?

Q3c. From your experiences, what do you feel is the level of cybersecurity awareness among your peers?

4) Challenges, Approaches, and Risk Assessments.

Q4a. Aside from actual cybersecurity threats you face, what other cybersecurity challenges does your SME face today, and how do you address these challenges in your daily operations?

Q4b. How do you assess and prioritise the cybersecurity threats and challenges and the resulting risks faced by your SME? What factors influence your risk assessment process?

5) Resources, Regulations, Initiatives, and Feedback.

Q5a. Where do you currently search for information and guidance on cybersecurity threats and challenges? How reliable do you feel these sources are?

Q5b. Are you aware of any specific cybersecurity initiatives or regulations that affect your organisation? How do these influence your approach to cybersecurity?

Q5c. How have recent cybersecurity initiatives or regulations affected your SME?

6) Supply Chain Risks.

Q6a. Does your organisation consider supplier-related cybersecurity threats and challenges? If so, what is your organisation's approach to these considerations?

Q6b. Does your organisation consider customer-related cybersecurity threats and challenges? If so, what is your organisation's approach to these considerations?

A.4.2 Post Mental Models - Participant Response Sheet.

A.5 Scenarios / Serious Games

The five scenarios are:

- (1) The U.S. withdrawal from Europe
- (2) U.S.–China confrontation over Taiwan
- (3) Climate change
- (4) Economic polarization
- (5) When AI goes rogue

The scenarios are used to:

- test the company's resilience
- identify new types of cyber risks
- support strategic dialogue and management decision-making

A.5.1 SCENARIO 1: The U.S. withdrawal from Europe. Henrik Henriksen looked at his Outlook calendar. He had 30 minutes before his next meeting, a coordination call amongst the Ministry of Defence budget forecasting team, just enough time for a quick walk across the street for a coffee. When Henrik had joined the Ministry 13 years prior, he never would have imagined that 16.30 meetings would become a regular feature in his workday, or that European NATO countries, including Denmark, would scramble to reach a 5But this was the reality in 2026. Increased defence spending was the priority for most of Europe. Since Donald Trump's victory in the 2024 election, America had abandoned its traditional relationship with Europe, imposing stiff tariffs and retreating from longstanding security partnerships. The changes in America impacted most Danish businesses, at least indirectly. The new universal trade tariffs of up to 50% hit EU exports to the US, including the 6.46 billion USD in Danish exports to the US. This was forecast to negatively impact the pharmaceutical, optical, and precision machining industries, and many Danes worried about their long-term job security. Legislative complexities meant the United States hadn't left NATO, but it had dramatically reduced its contribution to European security to redirect funds and troops to the Indo-Pacific. American troops withdrew from Germany, Italy, the UK, and Lithuania, reassigned to Hawaii, Guam, South Korea, and Taiwan. It was uncertain what role the US would continue to play in the alliance's nuclear sharing, and how much participation they would maintain in training exercises. Along with reduced funding, America had relinquished the role of Supreme Allied Commander Europe (SACEUR). The ensuing leadership vacuum within NATO meant that defence in Europe was becoming increasingly fragmented and regionalised. Germany and France squabbled about leadership of a common European foreign and defence programme. Spain, Italy and Greece focused their defence on the Mediterranean. Hungary left the integrated command structure, opting to cultivate closer relationships with Turkey, Russia and China. The Nordic and Baltic countries, along with Canada and the UK cooperated on the defence of the Baltic Sea and the far North. Canada, Australia and the UK increasingly sought to formalise intelligence-sharing agreements with the Nordics. The Five Eyes network had been disbanded after a series of security breaches, including a New Zealand official losing intelligence briefing materials on a trip to Hanoi, and the US Secretary of Defence accidentally sharing technical details of a North American missile defence system with a reporter from Tass. Without US intelligence, however, Denmark and its counterparts struggled to gather enough information on Russian activities. Since the Russia-Ukraine ceasefire of December 2025, The Nordic and Baltic states were under near-constant sub-threshold attacks. The eight countries were subject to a sustained disinformation campaign and frequent cyber aggressions on banking systems, utility providers, and mobile phone networks, as well as defence manufacturing firms, shipping and logistics companies. There was constant concern that Russia would expand its cyber-attacks to offshore windfarms, and cripple electricity supply. Funding for additional civil sector cybersecurity

training was Henrik's contribution to the meeting this afternoon, and he knew the budget increase would be approved as it was such a significant regional concern. Henrik spoke to his Finnish, Norwegian and Swedish counterparts almost daily. They shared similar problems: a perennial shortage of regular troops, and the challenges in increasing reserve forces and civil defence forces. From 2033 onwards, two years of national service would be compulsory after completion of secondary school, followed by 15 years of reserve or civil defence service. Fortunately, the populations took military service seriously and adapted to these changes, but there was only so much force-generation capacity within small populations with low birth rates. Perhaps the biggest, most evident change was the dramatic shift in spending priorities. The Danish government announced widespread cuts to the social welfare system, to come into effect by 2030. The state pension age would rise to 75, childcare would no longer be subsidised for households with an income over DKK 750 000, and university students would have to pay fees for their degrees. Defence would be the government's priority spending area. Henrik exited the three airlock doors, and then to the personal electronics lockers to get his phone. These were new security measures introduced six months before, due to concerns that the ministry was too accessible and that personal phones posed a cyber espionage risk. He was not allowed to download apps like Tiktok or even Facebook messenger or Whatsapp, in case his messages could be accessed by a hostile party. He had the old iPhone 16, but couldn't upgrade to the latest software, as it contained features that were not accessible on the European market. The US had stormed ahead with artificial intelligence development to outpace Chinese innovation. However, most of the new AI features remained stuck in EU regulatory reviews. He briefly glanced at the news notification popping up on his phone screen. There was a sensational story about US military activity in the waters beneath the Davis and Denmark Straits. It was another misinformation incident, of the sort that had become much more frequent since the end of the Russia-Ukraine war. Most were so sophisticated, it was hard to discern truth from fabrication, fact from fiction. This one, however, was bound to provoke a strong reaction in the upcoming meeting.

Potential risks for business

- (1) What are the key risk factors and vulnerabilities in this scenario?
- (2) What risks does this scenario pose to Danish businesses?
- (3) What vulnerabilities affect your business?
- (4) What mitigation, if any, has your business considered or implemented?

A.5.2 Scenario 2 US-China Confrontation Over Taiwan. Anna Anderssen was listening to the news as she packed her bag for work. Philippine coast guard vessel struck a Chinese fishing vessel near the Second Thomas Shoal in the Spratly Islands. Several fishermen had been injured, and two coastguard personnel had been killed. Anna had been to the Philippines on holiday 15 years before, but she did not follow events in the region and was not sure of the location of the Spratly Islands. Anna was not very interested in international affairs. Her brother-in-law Henrik, who worked for the Ministry of Defence, spoke of little else, but Anna found it depressing. Anyway, the South China Sea was a long way from Southern Denmark, and she had to get to her job as a Chief Financial Officer of a quantum

computing company that designed and developed medical robots. When Anna arrived in the office, the news was on the TV in the office kitchen. By mid-morning, the President of the Philippines issued a statement condemning Chinese aggression in the South China sea, claiming that the collision between the two vessels was a deliberate attack meant to thwart foreign ships from sailing in the South China Sea. China countered that coast guard's actions were territorial aggression, a deliberate attack on a civilian vessel within Chinese waters. The Philippines argued that the South China Sea was international water, and by the UNCLOS ruling of 2016, Philippine vessels were free to sail without interference. Within hours, Brunei, Indonesia, Malaysia, and Taiwan issued statements siding with The Philippines, as they too opposed Chinese claims to the resource-rich waters. Although it claimed to have no position on the South China Sea, the US Navy regularly sailed warships near the Paracel and Spratly Islands as gesture of support for the principle of freedom of navigation. This activity did nothing to improve the relationship between the US and China. Indeed, the Sino-American relationship had steadily deteriorated, with the Trump administration's imposition of punitive tariffs on China in 2025. Now, in the wake of the fatal collision, the 1951 mutual defence treaty meant the US was obligated to support the Philippines if came it under attack. Anna and most of her colleagues, spent the morning in the kitchen, glued to dramatic news coverage of the situation brewing in the Pacific. By the afternoon, The Philippines mobilised their navy. US declined to qualify the incident as a deliberate attack or not, but sent an aircraft carrier towards Manila, in a demonstration of support. Australia issued a statement of support the Philippines, indicating it would mobilise the Australian navy assist the Philippines as well. Australia had invested heavily in upgrading its armed forces for some time, concerned about an aggressive China attempting to dominate the Indo-Pacific region. Over the course of the day, many maritime countries, issued statements about the importance of upholding the principle of freedom of navigation, but stopped short of criticizing China directly. There seemed to be no further escalation. A few days later, however, China accused Taiwan of allowing disrespectful memes of the South Thomas Shoal collision site to circulate to the Line messaging app. In response, Taiwan accused China of cyber espionage, of hacking into personal messages of Taiwanese officials and ordinary citizens. Accusations between the two countries flew and tensions escalated rapidly. Anna could not keep up with all the details. China instituted a full blockade of Taiwan, preventing ships from entering all 15 of its ports. The PLA even threatened to shoot down civilian aircraft transporting goods in and out of Taiwan. Airlines rerouted Pacific flights to avoid the South China sea, adding additional kilometres and considerable cost to air freight and passenger travel. In retaliation, Taiwan launched a counter-blockade of China. The five busiest Chinese ports — Shanghai, Ningbo-Zhoushan, Shenzhen, Qingdao, and Guangzhou — all lay within a thousand miles of Taiwan, well within range and within the range of the Taiwanese Ching Dien supersonic cruise missiles. Both sides attempted to jam each other's electromagnetic frequencies, and launched large-scale cyberattacks to disable communications and financial services. At one time, this would have resulted in an emergency meeting of the UN Security Council. However, with two permanent Security Council members

in dispute with each other, it was impossible to convene a gathering. The dispute resolution mechanisms that had been in existence for nearly a century were no longer acknowledged. The European Union tried to maintain its economic and diplomatic relationships with both China and the US, with French President Macron making several diplomatic trips to Washington and Beijing, but he made no progress in resolving the dispute. Within weeks, shipping delays and disruptions rippled through almost every economic sector. Prices on items manufactured, or partially manufactured, in Taiwan and China soared, particularly electrical and electronic goods, as well as alloy steel, graphite, and gallium arsenide. European chip manufacturer ASML soon had difficulty sourcing material for chip manufacture, as China had bought up mineral rights to rare-earth deposits, and graphite mining and smelting operations in Europe and North America were too small to meet demand. Across Europe, shops had to ration items like batteries, phone charging cables and battery banks. Cyberattacks on digital payment systems meant consumers had to revert to cash, and in-store rather than on-line purchasing. Anna could not believe she was queuing for good in shops. With so much of manufacturing and trade besieged, global GDP dropped 5% very soon, Anna's business directly was impacted. They were unable to source necessary computer chips for their products, and thus could not fulfill orders. The procurement team spent weeks searching for alternative suppliers elsewhere in the world. Then, an email from a potential new supplier, turned out to be a phishing attack that halted all business operations for over a week. The attack cost the business its reputation and a one of its largest contracts with a prominent Danish pharmaceutical company. Anna did not know if the business would survive, and she was worried about finding another job in such a difficult economy. The impact of the economic blockade was politically and economically unsustainable for all sides. U.S. and Japan, and South Korea indicated willingness to use military force to thwart the blockade. Facing the possibility of such a challenge, China began a full-scale mobilization of all PLA ground, sea, and air forces. The mobilization put the US, Japan, and South Korea on high alert. Anna had never been interested in international affairs, but now she thought of little else.

Potential risks for business

- (1) What are the key risk factors and vulnerabilities in this scenario?
- (2) What risks does this scenario pose to Danish businesses?
- (3) What vulnerabilities affect your business?
- (4) What mitigation, if any, has your business considered or implemented?

A.5.3 Scenario 3 Climate Change. Hans Christensen surveyed his farm from the far west gate. It was a rare sunny day, and the farm looked like something out of a child's painting, with rich green grass and bright blue sky. Hans took a lot of pride in his farm. He was a fourth-generation commercial pork farmer. Since the 1920s, his family prided themselves on producing prize-winning, high quality, free-range pork products that were sold all over Europe. Like his predecessors, Hans took care to implement the latest in agricultural science to raise the pigs in optimal conditions and with minimal use of antibiotics. However, this was becoming more difficult as Denmark's weather was getting wetter every year. Hans

knew global warming had raised the earth's temperature by 1.5C, but changes to the jet stream made Denmark warmer, but also rainier, and much windier. The summer of 2029 has set a record for rainfall and windstorms. The wet weather meant more cases of porcine foot rot, which necessitated more treatment with antibiotics, and higher veterinary bills. The excessive precipitation meant that crops that thrived on sunshine no longer grew, unless under artificial light. Some farmers had lost their fields altogether, as rising sea levels had devastated low-lying coastal regions, and there was a persistent risk of flooding during the winter storm season, which now seemed to last for six months. The government had to invest in building coastal flood defences to prevent communities from washing away. There had been a flood mapping and coastal erosion study conducted in 2020, but the scale and intensity of storm surges were frightening even to people who had been discussing climate change impacts for nearly a decade. Climate change had been an acknowledged risk in Denmark for years. Hans had tried to do his bit to reduce the farm's environmental impact: installing solar panels on the house at the suggestion of his engineer neighbour Anna, recycling as much as he could, feeding the pigs forage legumes to improve their gut health and reduce methane outputs, and filtering manure to reincorporate it into the soil. He had even participated in a public forum on a local climate change adaptation plan, but the risks had all seemed quite abstract and distant, a threat for subsequent generations to contend with. Across Europe, emergency infrastructure projects were underway to protect people from extreme weather events: flooding, landslides, wildfires, and electrical storms, that seemed to be occurring with alarming frequency. These emergency infrastructure projects came at vast expense, reducing national and EU-wide subsidies for agriculture, education, and the arts. Hans really noticed the subsidy reduction when he paid for the installation of climate control features in his pig barns, and when he paid the huge monthly bill for air-conditioning during the summers. He hoped the investment would pay off if his herd remained healthy. Regulating the pig's temperature helped keep their immune systems strong. There were many new zoonotic diseases circulating in Europe that thrived in the changing climate, including mosquito and tick-borne illness, and soil-based pathogens. There were even reports of people becoming infected with dengue fever as the tiger mosquito made its way north, lured by milder temperatures and stagnant water in low lying areas. As well as the challenge of keeping his family, and the herd in good health, getting the farm's pork products to market was becoming increasingly unpredictable, and profits were impacted as result. Storms, increased air turbulence, flash flooding and fires made transportation – by air, sea, or roads – more dangerous, and this reflected in higher insurance premiums for shipping companies, costs that were passed on to the consumer, leading to higher prices and lower sales. In the dramatic storm season of 2028, a flash flooding on the autobahn in Germany caused the 18-wheeler carrying Hans' pork products to crash, destroying nearly DKK 250 000 worth of meat. Hans had received an insurance pay out for the loss, but this year he had received a letter from his insurers, informing him that they no longer covered the cost of damages sustained in climate-related weather events, as these were becoming too common. As an experienced farmer, Hans understood well the relationship between weather and animal health but climate change,

and mitigation efforts, were inflicting costs in ways that Hans could never have dreamed. In 2026, the EU had taken the decision to halt the use of computationally intensive AI, that used a significant amount of energy, to reduce IT-related carbon emissions. While emission reduction targets were met, the prohibition of services that used AI to detect cyberattacks programs meant European companies were more vulnerable to cyberattacks. Cyberattacks were particularly common after major climate events, as cybercriminals took advantage of disruptions and destabilisation. COPA-COGECA, the EU farmer's association, distributed information on how farms and agribusiness could avoid cybercrime. Hans did not fully understand how AI worked, but he had felt the impact of a cyberattack first-hand. His feed supplier had suffered a ransomware attack, and order fulfilment had been suspended. At very short notice, Hans had to find an alternative supplier at short notice. For Hans' farrow-to-finish operation, this was a significant unexpected cost, as his pigs consumed an average of 2 600kg of feed a week. Hans had been caught completely off guard, as he had prepared to lose feed to fire, floods or spoilage, not computer-related events. Climate events were not only affecting farming. Rising sea levels forced nearly 100 000 people to relocate from the Faroe Islands and Greenland as rising sea levels and increased rainfall put their communities in danger. Some brought their Faroese sheep too, adding variety to agricultural exhibitions and stockyards. The government provided substantial social welfare support for the new arrivals, prompting some opposition and disgruntled commentary from more extreme political groups, who thought the support was overly generous. Hans was not overly concerned about newcomers arriving in the country. Most settled in urban areas, rather than small farming towns, so he had limited contact with them. What kept him awake at night was keeping his family business profitable and operational. Farming had always been a tough business and had always been at the mercy of the weather. But while his father and grandfather could recall only a few legendary storms, Hans never knew when or where to expect the next disaster.

Potential risks for business:

- (1) What are the key risk factors and vulnerabilities in this scenario?
- (2) What risks does this scenario pose to Danish businesses?
- (3) What vulnerabilities affect your business?
- (4) What mitigation, if any, has your business considered or implemented?

A.5.4 Scenario 4 Economic Polarization. Christina Pedersen sat in her home office, putting the finishing touches on the sales charts for the company's Q3 report. She was the senior sales and marketing executive at Danstol. Established in 1964, Danstol was mid-range furniture and lighting manufacturer. The company produced classic mid-century home and office furniture items and a range of lamps and decorative items. The brand positioned itself in the affordable luxury category: a high-quality brand that was aspirational yet attainable. Christina had worked for the company for eight years, and now reported directly to the Board of Directors, who were meeting the following week to review the company's quarterly performance. Since its founding, Danstol's typically customer base were middle class families in Denmark and continental Europe, and businesses who wanted functional, yet aesthetically

pleasing furniture that was better quality and design than IKEA. For the past 20 years, Danstol had held an exclusive contract to supply government offices with furniture for public reception rooms. Despite its myriad bright colours, Christina's sales chart did not paint a cheerful picture. Furniture sales were stagnant in Denmark. Due to the aging population, many young families were inheriting furniture from parents or grandparents and did not need to purchase new items. Trends towards flexible working had reduced the quantity of office furnishings businesses invested in, and co-working spaces usually opted for cheaper décor items. Elsewhere in Europe, sales had continued their downward trend. In Germany, Danstol's major external market, sales had declined by 29%. The German middle class felt anxious about rising taxes, economic stability and European security. Consumers therefore refrained from making large purchases that were not strictly necessary. Young consumers, if they were not inheriting furniture from parents and grandparents, opted for eco-friendly secondhand shopping. Many were concerned about climate change and faced greater instability in their employment and rising housing costs, and thus were less likely to invest in new furniture. They did, however, purchase small decorative items: vases, plants pots, and some smaller functional items like shelving, desk and floor lamps, and small storage items. These items however, had a very narrow profit margin for Danstol, and there was huge competition in the decorative home accessory market. Danstol senior management knew that the company had to reach this cohort of younger consumers. Christina and her team had spent Q2 designing a new campaign called: Upcycle! Under this scheme, a customer could send original Danstol pieces back to the factory for repairs, reupholstery, and repainting, so that items could be updated and customized, within reason. The price of upcycling was typically less than purchasing a new item, and it helped the company reduce waste by using deadstock material. Digital and print media campaigns highlighted the brand's sustainability concept and heritage as an authentic made-in-Denmark. The intention was to win over a younger generation of customers even if their purchasing patterns might be different than previous generations. Christina was proud of her marketing team's creative work. However, she and her senior management colleagues were aware that Danstol's declining sales reflected wider socio-economic trends that their business could not influence, no matter how sophisticated their advertising campaigns. The middle class was shrinking, with a widening gap growing between rich and poor. Denmark was somewhat insulated from this trend, due to its small population, economic strength and continued social welfare provision, but it was increasingly evident elsewhere in Europe and North America. Greater economic polarization was contributing to greater political alienation, as far-right and far-left political parties played on economic insecurity to build larger support bases, particularly in areas with higher rates of unemployment or economic inactivity. These political parties campaigned vociferously against migration into Europe. Christina didn't like to engage with politics, but she did wonder how companies like Danstol would recruit enough lower-skilled labour for manufacturing jobs if migration to Europe was curtailed. At noon, Christina stopped work to walk her dog, Loki, outside. It was beautiful sunny day, and she wanted to make the most of the weather and the freedom of being at home. Working from home had been introduced in March 2020, at the beginning of

the Covid pandemic, for all staff except for those in the production facility and the warehouses. Since then, administrative and design staff had continued to work from home, the office, or alternative locations. However, there were now concerns that working from home would end, or at least be reduced, after Danstol and its suppliers, had been victims too many phishing attacks. With staff working from home, hotels, cafes, and trains, using public wifi networks or sharing home wifi with family members, made company systems more vulnerable to attack. Being in one office might give the company more oversight and control of its cyber risk. Fortunately, Loki was not considered a cyber threat and could come into the office too. Christina had experienced the impact of cyber threats firsthand. Last week, one of her interns had nearly opened an email from a marketing agency. Fortunately, he had noticed a minor spelling error in the subject line, and reported it to IT. Everyone in the company was anxious about cyberattacks because three months previously, Danstol had lost three weeks' production when their screw and bolt supplier had been subject to a ransomware attack. The financial impact had been significant, and the company had struggled to recoup its losses. The attack had been traced back to a Russian hacker group, not a state sponsored activity but teens who were able to make money through cybercrime. The Russian economy was impacted by three years of economic sanctions and the distortions of the war economy, leading to soaring consumer inflation and high interest rates. This primarily affected working class and middle-class families, who find themselves facing rising costs, limited choice of goods, and rising unemployment. Young Russian people felt resentment towards the west for Russia's economic alienation and their decreasing standard of living. With easy access to the internet, many young people were comfortable operating in the cyber environment, and easily learned to develop code. Some were recruited by organized criminal gangs, either directly or through videogame interfaces, to generate malicious code to attack foreign businesses and state services in return for payment. Others experimented with ransomware on their own as means of making money. Baltic and Nordic countries are targets, given their geographic proximity, vociferous opposition to Russia's full-scale invasion of Ukraine, and high levels of digitization. Christina had never really considered cybersecurity in her work prior to these attacks. She had focused more on digital marketing strategy rather than digital security. Christina and Loki turned back towards home. There was still a report to finish before the end of the day.

Potential risks for business

- (1) What are the key risk factors and vulnerabilities in this scenario?
- (2) What risks does this scenario pose to Danish businesses?
- (3) What vulnerabilities affect your business?
- (4) What mitigation, if any, has your business considered or implemented?

A.5.5 Scenario 5 AI Goes Rogue. Peter Nielsen smiled as he walked from his car to his office. He was the CEO of Stempelkraft, and the company was enjoying a year of unprecedented publicity, growth and profits. The Jutland-based company designed and manufactured component parts for leading engine manufacturers from the marine, rail and power generation sectors. Stempelkraft's range of products included pistons, piston ring sets, piston pins, and

cylinder liners, valves, valve seat inserts and guides, and power cell units designed and sold as customizable complete systems. It was an industry leader in developing composite materials to enhance the durability of cylinder rings and piston pins. For years, it had been a relatively small-scale operation, primarily selling to Nordic and German manufacturing companies. Then, in March 2026, Stempelkraft had competed on, and won, a bid to supply component parts for the new Galaxy-class stealth frigate, the new multi-role warship commissioned by 17 NATO member states' navies. The Galaxy programme made the relatively unknown business into a household name across Denmark, and it was heralded for its innovation and quality. Peter and the rest of the company board recognized that the Galaxy programme was a great opportunity for Stempelkraft. However, it did present some practical challenges for the business. Stempelkraft had provided power cell units to Danish and Norwegian naval programmes, but it had never undertaken a project of such magnitude and significance before, and staying on top of inventory was proving to be difficult. The business operated across three separate sites and had two separate inventory systems: one for managing incoming components from suppliers, and another for outbound customer orders. Although the warehouse and customer service teams were dedicated and diligent, they were struggling to manage the increased volume and complexity of orders. Considerable time was lost, and many errors made, as the team tried to coordinate inventory using an outdated system that required a lot of manual data input. This needed to be rectified if Stempelkraft was to manage the scale of Galaxy orders. After consultation with the warehouse and customer service team, the company board made the decision to purchase an AI-enabled inventory management system to streamline and improve processes. Stempelkraft management was confident in the utility and reliability of AI. After all, automation had been integrated into the many aspects of the assembly process, such as piston ring coating and casting of cylinder lining, without issue. AI tools had been steadily growing in both sophistication and popularity since 2020 and were integrated into the inventory management and customer services interfaces of many similar businesses. In fact, the tool they selected, PowerInventory. Furthermore, it was an approved supplier to the US Navy and therefore met security requirements for the Galaxy programme. For a medium sized business, PowerInventory was a relatively low-cost way for Stempelkraft to manage a wide range of complex tasks: inventory forecasting, requests, supplier selection, ordering, restocking, transfer, serialization and compliance verification. It had a user-friendly interface for staff and customers, and even a mobile app. As the months passed, all appeared to be going well. The software implementation had been a surprisingly seamless process, and the warehousing staff had easily adapted to the changes. In fact, they reported that they were working better as a team as situations that had previously caused confusion, or redundant efforts had largely been eliminated. Peter had even managed to highlight the new system in a feature interview with a Danish industry magazine, to show how the company was adapting to meet the demands of an expanded international customer base. After nearly a year of using PowerInventory without incident, the board decided that it was safe to divest of the old inventory software, to reduce the cost of licensing fees of a legacy system

that was no longer in use. Late one Friday afternoon, the warehousing team noticed that it was taking an unusually long time for the programme to load. Simple requests could not be fulfilled, or timed out unexpectedly, and their computer screens would display 503 'service unavailable' error messages. The team decided that it must be an issue with the company's internet service provider, or possibly their own mistakes, and left for the weekend, believing that the issue would have resolved itself by Monday morning. By noon on Monday, however, it appeared that the problem was much more serious than anticipated. Nothing was working. No one could access the system. The customer service team received several calls from clients who reported they were unable to place or review orders either online or on the app. The warehouse team called Stempelkraft's in-house IT, but they were unable to rectify the problem. The following day, PowerInventory's head office reported that it had suffered a cyberattack, affecting all its products. The server that Stempelkraft relied upon was unavailable. PowerInventory was working to restore access, but it was unable to estimate when server access might be restored. Without access to the inventory system, and without their older system, Stempelkraft had no oversight of its inventory, and it was still under contract to deliver orders on time. The board made the decision to halt production until the problem was resolved, while the warehousing and customer service teams created a temporary manual inventory system using Excel spreadsheets. Every nonproductive day cost the company money and delayed product delivery. Eventually, after three agonizingly expensive weeks, server access was restored, and Stempelkraft was once again able to track its inventory. However, after a month, the warehouse team noted a recurring issue with serialization. The middle three digits of every serial number were incorrect, making it impossible to trace products accurately. Careful investigation by the warehouse and IT teams determined that the problem could not be traced to a human input error. Somehow, the model had changed its parameters and was now replicating an incorrect pattern. It pointed to a much deeper and more serious problem than a few numbers out of sequence. Peter feared that, with the inventory system so seriously compromised, Stempelkraft could lose the Galaxy contract altogether.

Potential risks for business:

- (1) What are the key risk factors and vulnerabilities in this scenario?
- (2) What risks does this scenario pose to Danish businesses?
- (3) What vulnerabilities affect your business?
- (4) What mitigation, if any, has your business considered or implemented?

A.6 Codebook

Table 5: Codebook for Transformed Mental Models (Shift codes)

Theme	PM/PP Mental Model (Phase 1)	PI Initial Mental Model Phase 2	PI Post Mental Model Phase 2	Transform
Shift 1: From Reactive to Proactive Postures (This shift captures the transformation from absent or reactive risk assessment practices to structured, ongoing, proactive approaches to cybersecurity preparedness.)	reactive and ad hoc approach	lack of formal plans	conduct a risk assessment	shifted
		no risk assessment process	Ongoing reviews of risk assessments	
		unable to assess risks	Continuous updates to risk management	
		no prioritization	Hacking simulations	
		not assessing continuously	DRS – Disaster recovery plans	
		Reactive security measures	Implementing a rescue setup	
		Informal crisis management	reevaluating risk improve monitoring	
Shift 2: From Technical to Holistic Threat Understanding (This shift captures the expansion of threat perception from narrowly technical attack vectors to a holistic understanding encompassing human factors, geopolitical dimensions, and organisational culture.)	state + non state threat actors	Phishing mails	Geopolitical risks	shifted
		Ransomware attack	Infrastructure	
		Internal malware	employee's behaviour	
		Fear of external hacking as primary concern	human dependency	
		Physical security	external threats	
Shift 3: From Isolated to Supply-Chain-Wide Perspectives (This shift captures the transformation from absent or downstream-only supply chain awareness to a comprehensive, bidirectional understanding of supply chain cybersecurity interdependencies. This was the largest gap closure observed.)	over-reliance on specific technologies	lack of supplier risk assessment	shift in supply chain risk perspective	shifted
	dependency on few technology providers concentration of risk	Supply chain risks not extensively evaluated	Supply chain and cybersecurity as interconnected	
		No current supplier risk assessment conducted	Increased focus on sub-suppliers	
		historical absence of supplier security	human dependency	
		Limited Customer Engagement	map supplier networks and investigate risks	

Continued on next page

Table 6: Codebook for Transformed Mental Models (Shift codes)

Theme	PM/PP Mental Model (Phase 1)	PI Initial Mental Model Phase 2	PI Post Mental Model Phase 2	Transform
		Internal threats prioritised over supply chain threats	expanding risk – upstream	
			reviewing supplier cybersecurity policies	
			Supplier diversification	
			Broader assessment incorporating supply chain mapping	
			Shifting to upstream risk	
			Pre-existing supplier awareness without change	
Shift 4: From Individual to Systemic Thinking (This shift captures the expansion from organisation-centric thinking to recognition of broader geopolitical, economic, and technological systems shaping cybersecurity risk.)	Recognise PIs surface awareness	Cybersecurity not perceived as organisational challenge	Cascading geopolitical dependencies recognised	shifted
		narrow geopolitical awareness limited to defence role	recognition of broader systemic supply chain dependencies	
		limited awareness of operational environment threats	Systemic challenges exceeding individual capacity	
			Risks from vendor dependencies and verification needs	
			awareness of vulnerabilities	
Shift 5: From Informal to Structured Approaches (This shift captures the transformation from ad-hoc, informal cybersecurity training and communication to structured, leadership-involved, organisation-wide approaches.)	perceived PIs lacked formal training programs	lack of training programs		shifted
		informal training on phishing	increase awareness training	
		ineffective communication	proper cybersecurity training	
		low awareness	leadership training	
		lack of awareness training	seminars and risk training	
		cybersecurity awareness gaps	involve our top management	
		lack of serious engagement from leadership	clearly communicate guidelines & practices	
			foster a culture of see it	
			onboarding	
			retired training approach	
			raising awareness in leadership	
			no change	

Continued on next page

Table 7: Codebook for Transformed Mental Models (Shift codes)

Theme	PM/PP Mental Model (Phase 1)	PI Mental Model Phase 2	Transform
Persistent Gap 1: The Cost–Investment Framing (Despite expanded threat awareness, the fundamental framing of cybersecurity as a cost and compliance obligation rather than a strategic investment remained unchanged.)	strategic investment (PM)	financial burden (cost)	persisted
	financial burden (PP)	xx	
		compliance	
		cyber security insurance	
		regulatory compliance awareness	
		regulatory-driven cybersecurity investments	
		resources and prioritization	
Persistent Gap 2: Cross-Stakeholder Communication (The information gap between the policy level (PM/PP) and implementation level (PI) remained unchanged. PIs remained unaware of national resources.)	Commends SAMSIK as the single point of contact (PM)	SAMSIK Danish Centre for Cyber Security unknown to PIs	persisted
	Unclear role of SAMSIK (PP)	Information Source Uncertainty	
		No awareness of regulations or national initiatives	
		Regulations perceived as having no impact	
		Unaware of newly introduced regulations	
Persistent Gap 3: Resource Reality (Scenarios revealed the scale of challenges but could not resolve material resource constraints preventing SMEs from acting on expanded awareness.)	lack of skilled cybersecurity programmers, practitioners, and education	Unclear responsibility; lack of internal expertise	persisted
		Heavy dependence on external IT providers	
		Outsourcing IT security as primary approach	
		Mix of internal and external capacity	
		Challenges identified but resources insufficient	