SMEs' Cybersecurity and Business Continuity: Results and Perspectives

Jan Stentoft, Ole Stegmann Mikkelsen, Kent Adsbøll Wickstrøm, Vincent Keating, Louise Tumchewics, Olivier Schmitt, Amelie Theussen, Marco Peressotti, Peter Mayer & Judith Kankam-Boateng

May 2026

CYBER SECURITY and BUSINESS CONTINUITY

SMEs' Cybersecurity and Business Continuity: Results and Perspectives

ISBN: 978-87-94345-97-2
EAN: 9788794345972

Proofreading:
Tekst og Web, Kolding

Typesetting/Layout:
Tadaah Graphic Design and Web, Kolding

This is the final report of the project "Cybersecurity and Business Continuity", which has been carried out with financial support from the Danish Industry Foundation and the final material is delivered both in Danish and English. This English version is developed with assistance from ChatGPT.
The project website is: **www.cyber-smv.dk**

The research project has been conducted by researchers from the Department of Business and Sustainability, University of Southern Denmark; the Center for War Studies, University of Southern Denmark; the Department of Mathematics and Computer Science, University of Southern Denmark; and the Royal Danish Defence College.

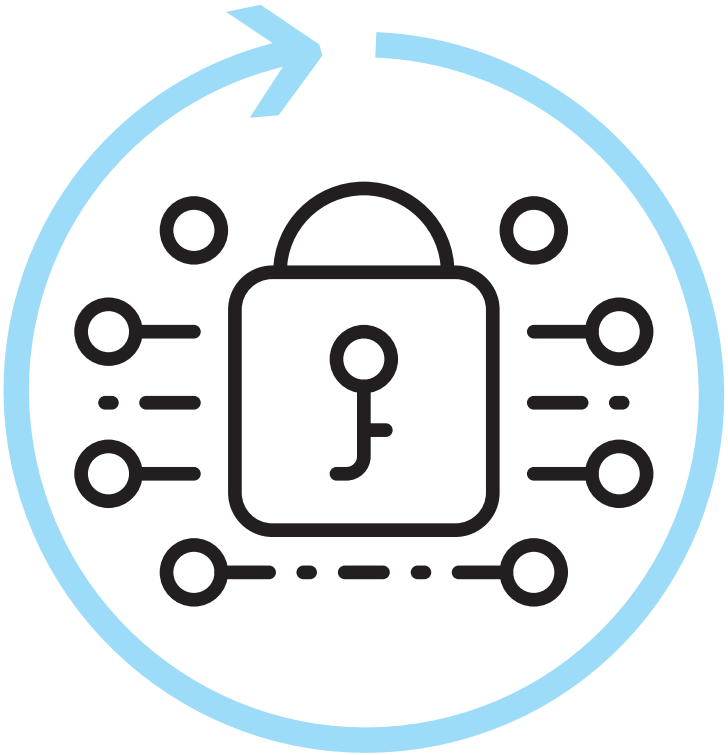


Table of Contents

Preface by the Danish Industry Foundation

As digitalization accelerates across industries and activities, cybersecurity has become an issue that extends far beyond companies' IT departments. Today, cybersecurity is a business-critical matter with direct implications for companies' operations, value creation, and survival — and therefore concerns all employees within an organization.

The challenge of cybersecurity is also significant among small and medium-sized Danish manufacturing companies. Here, the complexity of supply chains is high, and the dependence on digital systems, suppliers, and business partners is enormous.

It is in this context that the **Danish Industry Foundation**, through a dedicated initiative, focuses on cybersecurity in value chains across Danish industry. Companies' value chains are crucial to their business operations and must therefore be protected systematically. This requires strengthening resilience so companies can withstand cyberattacks, while also being well prepared to maintain operations and fulfill agreements and their role within the value chain both during and after a cyberattack.

Important for Everyone

Unfortunately, there is still a misleading perception in parts of Danish industry. Too many managers in smaller companies continue to believe incorrectly that their businesses are not attractive targets for cybercriminals.

Both organized criminal groups and state actors target Danish companies with attacks every day - often through the weakest link in the value chain. As a result, smaller companies are also attacked, not necessarily as the primary target, but as entry points to larger organizations.

For this reason, cybersecurity and cyber-secure value chains are highly relevant topics for all businesses.

Based on this understanding, the project Cybersecurity & Business Continuity has, over several years, worked to strengthen cybersecurity in Danish business value chains through an interdisciplinary approach with broad appeal

and relevance to most organizations. This approach can make cybersecurity efforts more complex because many parts of the organization must be involved, but it is also necessary due to the many points of entry into a company through the value chain.

Business-Oriented Tools

The project combines research, theory, and competence development within supply chain management and cybersecurity with scenario development and practice-oriented activities in Danish companies. This combination of knowledge and action has been essential in developing business-oriented tools for strengthening companies and their value chains.

The tools cover a broad range of areas and particularly address cybersecurity from a supply chain perspective, where the focus extends far beyond the individual company's own walls. One of the most central tools is a digital solution supporting a supply chain resilience process model that helps companies work systematically and across organizational boundaries to identify and manage vulnerabilities and attacks within the value chain.

To illustrate and make attacks more tangible, the project has also developed a number of future scenarios describing different critical situations. These scenarios support companies' preparedness efforts through simulations and force companies, and key decision-makers, to answer a number of important questions: What do we do in such a scenario? Who does what, when, and how? And where are our weaknesses?

A Secure Investment

With these tools and scenarios at hand, Danish manufacturing companies can work more systematically and strategically with cyber-secure value chains. And this is necessary — both for the individual company and for the business community as a whole.

An increased focus on cybersecurity creates a more secure company and reduces a range of risks. Beyond that, however, it is also an investment that makes the company more attractive to customers and business partners. We therefore hope that many companies will embrace this report and the new tools and transform them into competitive strength and growth.

We wish you an enjoyable and productive reading experience.

Malene Stidsen
Program Director
Danish Industry Foundation

Preface by the authors

This final report on the project Cybersecurity and Business Continuity is the result of a three-year research project carried out for the **Danish Industry Foundation** by researchers from the Department of Business and Sustainability, University of Southern Denmark; the Center for War Studies, University of Southern Denmark; the Department of Mathematics and Computer Science, University of Southern Denmark; and the Royal Danish Defence College during the period from September 2023 to June 2026. The purpose of the project has been to strengthen the cybersecurity of Danish small and medium-sized manufacturing enterprises (SMEs) in an increasingly unstable world. The objective is therefore for the target group to strengthen and develop its understanding and practices related to cybersecurity so that it can contribute to competitive advantages.

The current geopolitical instability, characterized by conflicts, trade disputes, and increasing rivalry among major powers, has created a more unpredictable threat landscape - also in cyberspace. For Danish manufacturing SMEs, this means a significantly increased risk of cyberattacks, as they are often part of international supply chains and may therefore become indirect targets in larger strategic conflicts. At the same time, many smaller companies have limited resources for IT security, making them particularly vulnerable to, for example, ransomware, industrial espionage, and supply chain attacks. The combination of global instability and digital dependency therefore increases the need for SMEs to prioritize cybersecurity as a central part of their risk management.

The report presents 30 tools that can help Danish manufacturing SMEs become better prepared against cyberattacks. The project builds upon an earlier initiative supported by the **Danish Industry Foundation**, in which a process model was developed to strengthen resilience in supply chains (Stentoft, Mikkelsen & Kjær, 2024). A key lesson from this work - further confirmed in the present cyber project - is that internal dialogue and cross-functional collaboration across areas such as sales, production, procurement, finance, IT, and product development are crucial. It is precisely this involvement that ensures companies focus on the most relevant initiatives to strengthen both supply chain resilience and cybersecurity (Stentoft & Mikkelsen, 2024).

The report therefore recommends that companies begin with the supply chain resilience process model, which consists of four phases. In the present project, phases 2 and 3 have been further developed and coded into open-source software. The process model focuses first on identifying vulnerabilities, risks, and necessary capabilities within the supply chain, which is linked to the fact

that the project was funded under a **Danish Industry Foundation** call concerning cyber-secure supply chains. Experiences from the previous project showed that many companies had limited practices for cross-organizational collaboration in understanding concrete challenges within their supply chains. Working with the process model created new dialogues and a better understanding of vulnerabilities, making it easier to prioritize limited resources.

In the "new" project, the companies therefore worked with all four phases of the process model to establish a shared foundation across the organization. An important point is that cybersecurity cannot be isolated within the IT department - it is a shared responsibility across the entire company, which is why it is important that the work is anchored at the management level.

There are a number of individuals and organizations who have contributed to the project and whom we would like to thank. First and foremost, we would like to express our sincere gratitude to the **Danish Industry Foundation** for prioritizing the project and thereby making it possible to carry it out. We would also like to thank the project steering committee: Dean **Marianne Holmer**, University of Southern Denmark; Industry Director **Andreas Holbak Espersen**, Confederation of Danish Industry (DI); Director **Pernille Kræmmergård,** DI2X; Owner **Kristian Fischer**, KFISCH; and Director **Søren Vammen**, Zoriac, for your commitment and constructive input. We would also like to thank the associated reference group, consisting of Deputy Director **Henrik Findahl Brodersen**, Danish Agency for Social Security; Deputy Director **Joachim Finkielman**, DI; CEO **Morten Bjørn Hansen**, Business Kolding; Manager **Zaynab Al-Hussaini**, Capgemini Invent; Senior Consultant **Berit Aadal**, Danish Standards; and Project Manager **Tina Højrup Kjær**, Odense Robotics. We worked with 30 different companies across two project phases. We thank the employees who participated and therefore contributed to realizing the project.

In the project's second company phase, students contributed by facilitating work with the supply chain resilience process model within the companies. We would like to extend a special thank you to **Sarah Elvira Johansen**, **Sander Guldbrandsen**, **Matilde Damgaard Magnussen**, **Pirjo Adele Elisabeth Brændeholm**, **Jonas Skovdam Jørgensen**, **Julie Nyhuus Gill**, and **Anne Cecilie Karlsen**, all of whom are Master of Science in Economics and Business Administration students at the University of Southern Denmark in Kolding.

May 2026

Jan Stentoft, Professor, University of Southern Denmark
Ole Stegmann Mikkelsen, Associate Professor, University of Southern Denmark
Kent Adsbøll Wickstrøm, Associate Professor, University of Southern Denmark
Vincent Keating, Associate Professor, University of Southern Denmark
Olivier Schmitt, Professor, Royal Danish Defence College
Louise Tumchewics, Postdoctoral Researcher, University of Southern Denmark
Amelie Theussen, Associate Professor, Royal Danish Defence College
Marco Peressotti, Associate Professor, University of Southern Denmark
Peter Mayer, Associate Professor, University of Southern Denmark
Judith Kankam-Boateng, PhD-student, University of Southern Denmark

1.
Introduction

Over the past decades, the digital transformation has fundamentally changed the conditions for Danish manufacturing SMEs. Today, production systems are closely integrated with digital control systems, cloud-based platforms, automated logistics solutions, and global supplier networks. At the same time, supply chains have become more complex and internationally interconnected. This development has created significant efficiency gains and new business opportunities, but it has also considerably increased companies' vulnerability to cyber threats. As production, inventory management, procurement, quality assurance, and distribution have become digitally interconnected, cybersecurity is no longer solely an IT matter, but a strategic and business-critical issue.

The purpose of this three-year project has been to strengthen the cybersecurity of Danish small and medium-sized manufacturing enterprises (manufacturing SMEs), with a particular focus on the supply chain. The project has been based on the recognition that the threat landscape is increasingly targeting entire ecosystems rather than individual companies. Attacks do not necessarily target the largest or most mature actor directly, but may occur through smaller suppliers, service partners, or subcontractors with weaker security measures. Consequently, cybersecurity becomes a shared responsibility within the supply chain and a prerequisite for resilience, competitiveness, and trust.

1.1 Disruptions in Supply Chains

Supply chains are increasingly affected by a wide range of disruptions that may be physical, organizational, or digital in nature. Traditionally, companies have focused on risks such as natural disasters, fires, strikes, pandemics, geopolitical tensions, trade restrictions, and transportation bottlenecks. These events can lead to delivery delays, shortages of critical components, and significant price fluctuations.

In recent years, however, cyber-related disruptions have become an equally important risk factor. When supply chains are digitally integrated through shared ERP systems, inventory management, production planning, EDI solutions, and cloud platforms, a cyberattack occurring at one point in the chain can quickly affect all other actors involved. A ransomware attack targeting a logistics provider, for example, may paralyze booking and tracking systems, delaying transportation and creating uncertainty regarding product flows. Compromised supplier accounts may lead to fraud through fake invoices or altered payment information. Manipulation of production data or technical specifications may result in defective production and quality issues that are only discovered late in the process.

Cybersecurity therefore functions both as an independent risk factor and as an amplifier of existing disruptions. Digital vulnerabilities can trigger operational shutdowns, create information asymmetry, and weaken the basis for decision-making throughout the entire value chain. The more complex and global the supply chain becomes, the greater the dependence on stable and secure digital connections, and the more critical a systematic and coordinated cybersecurity effort across all actors becomes.

1.2 Cybersecurity as a Business-Critical Factor

Cybersecurity in manufacturing SMEs is not only about protecting data, but equally about protecting operations, delivery reliability, quality, and reputation. Production environments are increasingly based on Industrial Control Systems (ICS), SCADA solutions, and IoT devices that connect physical production with digital control and monitoring systems. This is also referred to as Operational Technology (OT). Traditionally, these systems have been designed with a focus on operational reliability and efficiency, rather than with cybersecurity as a primary priority. As they are now connected to the company's broader IT systems and external networks, new attack surfaces emerge.

A successful cyberattack can have direct and immediate consequences for production. Ransomware attacks, in which a company's systems are encrypted and only released upon payment, have in several cases resulted in the complete shutdown of production lines for days or even weeks. For a manufacturing SME, even short-term operational disruptions can lead to significant financial losses in the form of lost revenue, breach of contract, delayed deliveries, and increased recovery costs.

One concrete example is global cyberattacks in which manufacturing SMEs have had to temporarily halt operations because critical planning and management systems were unavailable. In such situations, not only the individual company is affected, but the entire supply chain. Suppliers are unable to deliver as planned, and customers do not receive their goods on time. For companies operating with just-in-time production, even minor disruptions can trigger chain reactions with extensive consequences.

In recent years, cybercrime has evolved from isolated hacking activities into a more organized and professionalized practice with clear industrial characteristics. As described in Invisible Enemy - Hacker Attacks and Secret Networks by Espersen, Sjøberg & Kaastrup (2026), modern cybercriminals operate in networks where tasks are specialized and where tools, access credentials, and data are traded on hidden marketplaces. Data has increasingly become a commodity, and attacks such as ransomware illustrate how digital threats have become commercialized and scalable.

At the same time, the boundary between traditional crime and state-sponsored activities is becoming blurred, increasing the complexity of the threat landscape. The book also highlights how social engineering techniques and technological tools are combined, making cybercrime both technically and humanly rooted. Overall, this supports an understanding of cybercrime as a structured and market-driven activity with characteristics resembling an industry.

1.3 The Supply Chain as an Attack Vector

A central focus of this project has been the supply chain perspective. Digitalization has led to close integration between companies and their suppliers. The sharing of production data, technical drawings, forecasts, order systems, and quality documentation often takes place through digital platforms with direct access between organizations. Each integration represents a potential vulnerability.

Attackers increasingly exploit the weakest link in the chain. A subcontractor with limited IT maturity may be compromised and subsequently serve as an entry point to a larger company. This may occur, for example, through compromised login credentials, infected software updates, or manipulated files. In such cases, the affected company becomes the victim of an indirect attack in which trust within the business relationship is exploited.

The consequences can be extensive. If a supplier's systems are compromised, this may lead to manipulation of production data, alterations to technical drawings, or the insertion of malicious code into software used in production. In the worst-case scenario, this may result in defective production, safety risks for end users, or product recalls. Furthermore, sensitive information regarding customers, pricing, contracts, and product development may be leaked, potentially weakening the company's competitive position.

A particularly serious scenario is the compromise of software deliveries. If a supplier provides updates or control software for production equipment, and this delivery is compromised, the attack may spread to all customers who install the update. In this way, a single compromised link in the supply chain becomes a multiplier of risk.

Op-Ed: One Weak Link Can Paralyze Us All – Why Supply Chains Require Strong Cybersecurity (Summary)

Imagine that a single supplier in a global supply chain is hit by a cyberattack. Production comes to a halt, logistics collapse, and critical societal functions are affected. This is not necessarily due to the size of the company, but rather its role as a crucial link in a chain on which we all depend. From energy and food supply to healthcare and transportation, our societies are increasingly based on digital connections that make us more efficient — but also more vulnerable. Cyberattacks can target both IT systems, networks, and servers, as well as OT systems, where physical processes are digitally controlled. Therefore, cybersecurity is not only a concern for large corporations, but also for SMEs.

Information security is often based on the CIA principles: Confidentiality, Integrity, and Availability. Confidentiality concerns protecting data from unauthorized access, integrity ensures that information is not altered, and availability ensures that systems and data are accessible when needed. These principles can be strengthened through measures such as awareness training, access control, backups, logging, and contingency planning.

Supply chains are complex networks of customers, suppliers, transport providers, and manufacturers that often use different systems and levels of security. Data is shared across organizations and national borders, and the interconnection of IT, OT (Operational Technology), and IoT (Internet of Things) increases the risk that a single attack may spread throughout the entire chain.

Cybersecurity has therefore become a license to operate. Regulations such as NIS2 and DORA impose security requirements, and companies increasingly face cybersecurity demands from customers, investors, and business partners. Organizations without adequate cybersecurity risk financial losses, reputational damage, and loss of contracts.

Efforts to strengthen cybersecurity should begin with increased awareness, clear guidelines, and prioritization of the most critical systems and data. Smaller but continuous initiatives such as backups, multi-factor authentication, and employee training can significantly reduce risk. Cyber threats are a permanent reality, and stronger cybersecurity across the entire supply chain is essential for both businesses and society.

Source: Stentoft, Mikkelsen & Wickstrøm (2025a). Read the Op-Ed here (in Danish)

1.4 Consequences of Cyberattacks for Businesses

The damage caused by cyberattacks can be divided into direct and indirect consequences. The direct consequences include costs related to system recovery, external consulting, legal assistance, fines, potential ransom payments, and lost production. The indirect consequences may be even more far-reaching. These can include loss of customer trust, weakened brand reputation, reduced market share, and more difficult access to new markets.

For Danish manufacturing SMEs, which are often part of international supply chains, inadequate cybersecurity may affect their ability to collaborate with larger global actors. Today, many international customers explicitly require documented cybersecurity maturity levels from their suppliers. Insufficient maturity may therefore result in exclusion from tenders or partnerships.

Furthermore, regulation in this area is developing rapidly. National and European requirements concerning information security, including stricter requirements for critical infrastructure and essential sectors, mean that companies increasingly need to document their security measures. Failure to comply may result in sanctions, fines, and increased regulatory supervision.

Another important aspect concerns the company's internal resources and working environment. Managing a major cyberattack places enormous pressure on the organization. Employees must work intensively on recovery, communication, and crisis management. Management must make rapid decisions under uncertainty, and the company's focus shifts from core business activities to crisis response. This may affect both productivity and employee well-being.

1.5 Special Challenges Faced by Manufacturing SMEs

Manufacturing SMEs differ from many other types of companies by having a close integration between digital systems and physical processes. When IT and OT (Operational Technology) converge, complex dependencies arise. A compromise of an IT system can have a direct impact on machines, robots, and production equipment. Conversely, insufficient updating or segmentation in OT environments can create persistent vulnerabilities.

In addition, many SMEs operate with older equipment where updates and security measures are limited. Replacing production facilities is often capital-intensive and a long-term investment, which may result in vulnerable systems remaining in operation for many years. At the same time, shutting down systems for updates or testing may involve significant production costs.

From a supply chain perspective, the complexity is further amplified. A modern manufacturing SME may have hundreds of suppliers and business partners across national borders. Gaining an overview of security levels, processes, and dependencies requires systematic mapping and continuous dialogue. This place demands on governance, risk assessment, and contractual mechanisms.

1.6 The Project's Relevance and Purpose

Based on the previous sections, the need for a targeted effort to strengthen cybersecurity in Danish manufacturing SMEs is evident. The purpose of the present project has been to develop, test, and implement methods and tools that can support SMEs in identifying, assessing, and managing cyber risks from a supply chain perspective.

The relevance of the project lies not only in reducing the risk of specific incidents, but also in strengthening the overall resilience and competitiveness of SMEs. A systematic approach to cybersecurity can contribute to improved risk management, increased transparency throughout the value chain, and stronger trust between business partners. In this way, cybersecurity becomes a strategic element of business development, not merely a cost.

The project results presented in this report should be viewed in light of a dynamic and continuously evolving threat landscape. Cyber threats are constantly developing, and new technologies create both opportunities and risks. Therefore, the purpose is not to deliver a final solution, but rather to contribute knowledge, experiences, and recommendations that can serve as a foundation for continued development within companies.

1.7 The Board's Role in Ensuring Corporate Cybersecurity

Cybersecurity is today a strategic issue that boards of directors must address actively. Digital threats can affect operations, finances, and reputation, and cyber risks should therefore be incorporated as a regular part of the company's overall risk management. The board is responsible for defining the organization's risk appetite, ensuring clear lines of responsibility within management, and receiving ongoing reporting on the threat landscape and security incidents. It is not the board's role to act as technical specialists, but board members must be able to ask informed questions and ensure that the necessary competencies and resources are in place.

At the same time, there should be a tested contingency plan for handling security breaches, as no organization can eliminate risk entirely. Finally, the board has a responsibility to ensure that the company complies with applicable regulations. In the EU, this includes, among other things, the General Data Protection Regulation (GDPR).

A Sister Project in the Cyber Portfolio: Strengthened Cybersecurity for SMEs

The project “Strengthened Cybersecurity for SMEs” is anchored at **Business Hub Central Denmark (Erhvervshus Midtjylland)** and helps Danish SMEs build a stronger and more resilient digital preparedness. The project originates from an increasing threat level, new regulatory requirements such as NIS2, and companies’ need to document cybersecurity measures to customers and business partners.

Through the project, companies are offered a range of targeted activities: Free and independent one-on-one guidance, workshops, webinars, conferences, and access to practical tools - including CyberSurvey, which helps companies identify risks and receive recommendations for next steps. The project strengthens both the company’s internal security practices and collaboration throughout the value chain, where all actors share responsibility for digital resilience and security.

The initiative is based on a nationwide collaboration between the Danish business hubs and is supported by the Danish Industry Foundation. The goal is to make cybersecurity manageable and operational, and to create lasting value by raising cybersecurity maturity levels, increasing execution capability, and supporting companies in making cybersecurity an integrated part of their operations, thereby ensuring their continued role within the value chain.

Read more about the project here (in Danish)
Link to the CyberSurvey here

2.

Theoretical Framework

This section provides an overview of the theoretical framework on which the overall project has been based. The section is divided into eight subsections: 1) SME characteristics, 2) supply chains and risk management, 3) geopolitics, 4) cybersecurity, 5) business continuity, 6) the supply chain resilience process model, 7) cyber-secure supply chain risk management, and 8) dynamic capabilities.

2.1 Characteristics of SMEs

A fundamental characteristic of manufacturing SMEs is their limited size measured by number of employees and revenue. According to the EU definition, an SME has fewer than 250 employees and an annual turnover of no more than EUR 50 million or a total balance sheet not exceeding EUR 43 million (European Commission, 2003). In a Danish context, the vast majority of manufacturing companies are small or medium-sized enterprises (SMVdanmark, 2026). Their size typically results in shorter decision-making processes, close interaction between management and employees, and a relatively informal organizational structure.

Another key characteristic is owner-management. Many manufacturing SMEs are family-owned or managed by their founder. This often creates a strong connection between ownership and daily operations, which can enable rapid decision-making and strong value alignment. On the other hand, it may also mean that strategic decisions depend heavily on one or a few key individuals, which can create vulnerability in cases of succession or illness.

Manufacturing SMEs are often highly specialized and niche-oriented. Rather than competing through volume and economies of scale, they typically focus on specialized production, customer adaptation, and technical expertise. They frequently operate as subcontractors within larger value chains, for example in the metal, plastics, food, or machinery industries. This position makes them flexible and capable of adapting production quickly, but also dependent on larger customers and economic fluctuations.

In terms of resources, manufacturing SMEs are characterized by limited administrative and financial capacities (Zach, Munkvold & Olsen, 2014). They rarely have large support functions in areas such as HR, IT, or strategy, and management often performs multiple roles simultaneously. This can foster a practical and action-oriented culture, but it may also limit the capacity for long-term development, digitalization, and systematic innovation.

Technologically, many manufacturing SMEs are positioned somewhere between traditional craftsmanship and more advanced automation. Some have invested in advanced production technologies, robotics, and digital systems, while others are still characterized by manual processes. Digitalization and the green transition therefore represent both a challenge and an opportunity.

Culturally, manufacturing SMEs are often characterized by strong local roots. Relationships with employees, customers, and suppliers are frequently long-term and trust-based. Organizational culture may be marked by high levels of professional expertise, loyalty, and a practical orientation.

Overall, manufacturing SMEs are characterized by limited size, owner-management, specialization, flexibility, resource constraints, and strong local anchoring. These characteristics provide both strengths — such as rapid decision-making and customer adaptation — and challenges related to scaling, access to capital, and strategic development. Their importance to the Danish economy is significant, particularly as subcontractors and as drivers of employment and specialized production.

A Sister Project in the Cyber Portfolio: Cyber Safe Robotics

Cyber Safe Robotics aims to strengthen cybersecurity, and thereby the competitiveness of the Danish robotics, drone, and automation industry.

The program consists of six different thematic days focused on cybersecurity in the supply chain. These days are conducted as workshops combining professional presentations from experts with participants' active work on practical tools linked to each individual theme, ensuring that the acquired knowledge is anchored in practice.

The themes are: 1) The regulatory landscape, 2) Competitive potential, 3) Management responsibility, 4)

Collaboration within the supply chain, 5) Security in software development, and 6) When things go wrong (contingency planning).

Participants gain an overview of legislation and standards within the supply chain, enabling them to implement the necessary measures to ensure compliance and achieve a competitive advantage. From a management perspective, participants gain insight into and an overview of the company's strategic options regarding cybersecurity through a research-based tool designed to support the development and implementation of cybersecurity strategies.

Participants also gain knowledge about security within their supply chain, as well as competencies and practical tools to strengthen and support collaboration across the value chain. In addition, they are introduced to tools that support secure design and software development, such as a vulnerability scanner. Finally, they learn how to develop and test contingency plans for their own business operations and their relationships with customers and suppliers.

Read more about the project here

2.2 Supply Chains and Risk Management

The supply chain in a manufacturing company encompasses all the activities, actors, and flows required to bring a product from raw material to the end customer. It typically consists of suppliers of raw materials and components, transport and logistics providers, the company's own production and warehouse functions, as well as distribution channels and customers. In a

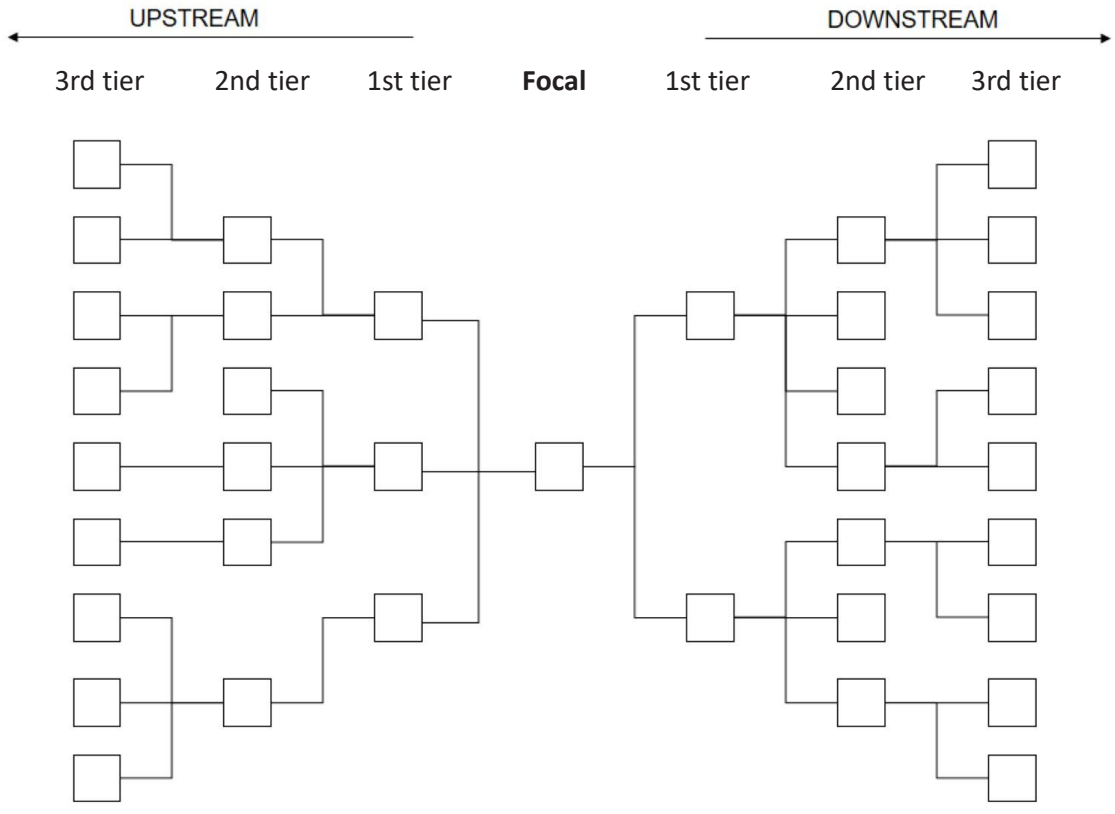
Danish manufacturing company, particularly an SME, the supply chain will often be international on the procurement side and more regional or European on the customer side, depending on the industry and level of specialization.

A classic understanding of supply chain management describes the management of materials, information, and financial flows across organizations with the aim of creating value for the end customer (Stentoft, Mikkelsen & Rajkumar, 2018). The purpose is to ensure high delivery reliability, competitive costs, appropriate inventory levels, and flexibility. For manufacturing companies, this specifically involves coordination between procurement, production, warehousing, and distribution.

The structure of the supply chain varies. Some manufacturing companies operate within simple chains with few stable suppliers and standardized products. Others are part of complex global networks with many subcontractors and customer-specific production. In particular, subcontractors to large industrial corporations' experience high demands regarding quality, traceability, and delivery times. Here, integration through ERP systems and digital planning tools is often essential.

Companies participate in supply networks as illustrated in Figure 2.1, where the individual SME in focus is referred to as the focal company. Cybersecurity in supply chains therefore focuses on how companies can improve cybersecurity across the various tiers of suppliers leading toward the company (upstream) and from the company toward various tiers of customers (downstream).

Figure 2.1 The Network Structure of Supply Chains



Source: Stentoft, Mikkelsen & Rajkumar (2018, p. 39)

Supply chains are, however, vulnerable to disruptions. Globalization, just-in-time principles, and low inventory levels have increased efficiency, but at the same time reduced resilience. The COVID-19 pandemic, geopolitical tensions, and energy crises have clearly demonstrated how quickly disruptions can spread through value chains (Stentoft, Mikkelsen & Wickstrøm, 2025b). This is where supply chain risk management becomes relevant. According to ISO 31000:2018, risk management is defined as a set of coordinated activities used to direct and control an organization with regard to risk, where risk is understood as the effect of uncertainty on objectives (Woods, 2022, p. 26). Applied to supply chains, this concerns identifying potential events that may disrupt material and information flows or relationships within the chain.

Risks in supply chains can be divided into several categories (Christopher & Peck, 2004). Supply risks include supplier failures, quality problems, and capacity shortages. They may also involve dependency on specific suppliers to whom companies are effectively locked in because no alternative suppliers are available (Narasimhan et al., 2009). Demand risks relate to fluctuations in customer demand or forecasting errors. Operational risks may include machinery breakdowns or IT failures, while external risks encompass natural disasters, political instability, or trade barriers. For Danish manufacturing SMEs, cyber risks and dependence on individual suppliers are also central concerns.

Supply chain risk management typically follows a process consisting of four main steps: 1) Mapping the supply chain and critical dependencies, 2) Identifying and assessing risks based on probability and impact, 3) Developing mitigating actions, and 4) Continuous monitoring and updating (Fan & Stevenson, 2018). Mitigation measures may include dual sourcing, strategic inventory buffers, closer supplier collaboration, contractual safeguards, or increased transparency through digital systems (Stentoft & Mikkelsen, 2024).

In a manufacturing company, balancing efficiency and resilience is essential. Excessive inventories and redundancy increase costs, while overly lean systems increase vulnerability. Strategic risk management is therefore about finding a level of resilience that matches the company's risk profile and customer requirements. Overall, the supply chain is the backbone of value creation in a manufacturing SME, and supply chain risk management is a key managerial tool for ensuring stable operations, competitiveness, and long-term sustainability in an increasingly uncertain and complex global economy.

A sister project in the cyber portfolio: Cyber-secure Food Supply Chains

The project Cybersecure Food Value Chains, managed by **Food & Bio Cluster Denmark**, is rooted in a realization that is increasingly shaping the food and bioresource industry: Cybersecurity is no longer an isolated IT matter - it is a business-critical discipline that extends across the entire value chain. When raw materials, production, logistics, and distribution are digitally interconnected, vulnerabilities in one area can have consequences far beyond a single company. The project therefore works purposefully to strengthen cybersecurity through collaboration across actors in the value chain, enabling companies not only to protect themselves, but also one another.

A key challenge addressed by the project is that many companies perceive cybersecurity as complex and difficult to translate into concrete actions. To address this, the project introduces a more practical and accessible approach: Risk assessments must be concrete, action-oriented, and easy to understand - including for management. Rather than producing lengthy technical reports, the focus is on creating a clear overview of the most critical systems and the most significant threats that may affect them. When this overview is combined with the company's current security level, it creates a genuine basis for decision-making.

As part of the project, a Risk Assessment Tool has been developed to support a structured and operational approach to risk management with a particular focus on OT (Operational Technology). The tool guides companies through a systematic assessment of threats, vulnerabilities, and consequences, translating these into a clear and manageable overview of where risks are greatest and where efforts should be prioritized.

Overall, Cybersecure Food Value Chains contributes to a necessary shift from complex technical exercises to simple, action-oriented risk management that creates real value both for individual companies and for the value chain as a whole.

Read more about the project here (in Danish)

2.3 Geopolitics

The project's theoretical framework for geopolitics is based on a fundamental transformation of the global order. We are moving away from a post–Cold War era dominated by liberal capitalism and market integration, in which economic activity and security policy were largely disconnected. In this former liberal order, companies could operate according to a market logic where profit maximization and efficiency were the primary governing parameters, while states primarily acted as neutral regulators enforcing the rules of free competition. The underlying premise was interdependence — the idea that increased economic integration and prosperity would, in themselves, reduce the risk of conflict between states.

Today, this separation between economics and security has collapsed alongside renewed great-power rivalry and the transition toward a post-American hegemonic system — a system in which the United States is losing relative power and influence. The new geopolitical reality is characterized by states systematically reconnecting prosperity and security. This emerging geoeconomic order is built on a geopolitical logic in which relationships often take on a zero-sum character, and where the economic gains of rivals are perceived as potential security threats.

2.3.1 Weaponized Interdependence

An important theoretical concept for understanding this development is weaponized interdependence (Farrell & Newman, 2019). The concept describes how asymmetrical global economic networks such as supply chains, technological infrastructures, and financial systems are increasingly exploited strategically by states to gain political influence, conduct surveillance, or exert coercion over other actors. This is manifested particularly through two theoretical mechanisms:

The Panopticon Effect: States monitor flows of information and capital through the central network hubs that they physically or legally control.

The Chokepoint Effect: States restrict or block third parties' access to critical networks in order to exert significant political or economic pressure, as these networks are extremely difficult to bypass.

2.3.2 Economic Security and Statecraft

As a direct consequence of this exploitation of networks, we now operate in an era defined by economic security (economic statecraft), in which states proactively and continuously use economic instruments to protect national interests. Whereas companies previously navigated solely according to market-economic incentives, they must now respond to state intervention through a range of specific tools:

Trade Policy and Sanctions: The use of import bans, export controls, and financial sanctions to isolate adversaries, signal political boundaries, and weaken rivals economically.

Investment Policy: Increased state control and screening of foreign direct investments, as well as strategic acquisitions of assets through sovereign wealth funds in order to gain political influence.

Monetary Policy and Direct Support: Financial manipulation and state subsidies designed to distort markets, create dependency relationships, and promote national industries at the expense of global competitors.

Control over Resources and Legal Instruments: The strategic withholding of energy or critical raw materials, as well as the growing extraterritorial application of national legislation.

2.3.3 The Clash Between Two Logics

For manufacturing SMEs, this conflict between the traditional market logic and the new geopolitical logic creates a fundamental strategic dilemma. Market-oriented capabilities that previously generated global efficiency, such as

Podcast: Geopolitical Tensions and Cybersecurity (Excerpt)

New Geopolitical Reality

"Globalization as we have known it is now under pressure. First, for the past 30 years the United States has been the only dominant power, and it has also deployed military force to secure global trade. Second, globalization depended on almost everyone agreeing on neoliberal globalization and on promoting democracy. These two elements made globalization possible, but they are now in decline," says Olivier Schmitt. "The United States is no longer the sole superpower, and there are now competing models for economic development that challenge the free trade and the free flow of goods and services we have had over the last 30 years," adds Vincent Keating.

Impacts on Supply Chains

Danish companies are often dependent on exports and global supply chains. Raw materials and semi-finished products are sourced through supply chains, processed across multiple geographical locations, and sold both in domestic markets and export markets. New geopolitical tensions will increasingly affect supply chains. "You could say that three types of 'shocks' may emerge. There may be supply shocks, where companies face difficulties obtaining raw materials and semi-finished products. There may be demand shocks, where markets are closed off. And there may be connectivity shocks, which concern the systems that connect companies through production and transportation," explains Olivier Schmitt.

New Risks

There is a need for new approaches to managing the new risks that will arise as geopolitical tensions increase. Changes may occur in the way supply chains are developed and structured — for example, with a greater focus on regionalization rather than globalization. "Regionalization may be more costly, but such a decision can help mitigate risks, where the alternative may be losing a key supplier. In the emerging new era, there is a need to think about demand, supply, and connectivity in entirely new ways, and about how they will be affected by geopolitical events," says Vincent Keating.

Listen to the podcast here (in English)

lean principles, just-in-time deliveries, and outsourcing to low-wage countries, now constitute critical vulnerabilities in a system characterized by weaponized interdependence. This necessitates a radical reconfiguration of companies' dynamic capabilities and approaches to risk management, in which geopolitics is embedded as an endogenous and unavoidable factor rather than something external and exceptional.

Op-Ed: How Do We Ensure That Cybersecurity Is Taken Seriously? (Summary)

The lack of proper cybersecurity maintenance in both private and public organizations is becoming an increasingly significant challenge as society grows more digitalized. Today, the Danish Centre for Cyber Security assesses the threat level against Denmark as very high. This is due, among other things, to rising geopolitical tensions and the risk that state actors may exploit cyber vulnerabilities to influence Danish companies and institutions. Cyberattacks are becoming increasingly targeted and include ransomware and data theft aimed at critical infrastructure such as energy, healthcare, and transportation. At the same time, organizations are vulnerable to so-called supply chain attacks, where attacks occur indirectly through suppliers and business partners.

An important step in addressing this threat is the EU's NIS 2 Directive. The directive expands cybersecurity requirements across more sectors and imposes stricter obligations regarding risk management, incident reporting, and cooperation between EU member states. Its purpose is to strengthen the resilience of critical sectors of society. However, while regulation plays a central role, it also raises the question of whether cybersecurity should become a legal requirement for many more businesses. A serious cyberattack can paralyze a company for weeks or months and, in the worst case, threaten its very existence.

For this reason, the establishment of a Danish Cybersecurity Agency could be an important next step. Such an agency could consolidate expertise in prevention, regulation, and response to cyber threats. It could develop security standards, strengthen education and advisory services, and ensure faster responses to cyber incidents. At the same time, the agency could function as a national knowledge center and provide support particularly to SMEs, which often lack the resources and expertise needed to manage cyber risks.

A central authority could also help strengthen trust in digital systems across society. In a digitalized society, trust in data security is essential. Investment in cybersecurity is therefore not merely a technical task, but a strategic investment in Denmark's economic stability and society's resilience against future cyber threats.

Source: Stentoft, Keating, Peressotti & Mayer (2025). Read the Op-Ed here (in Danish)

2.4 Cybersecurity

Cybersecurity refers to “the prevention of damage to, protection of, and restoration of computers, electronic communication systems, electronic communication services, wired communication, and electronic communications, including the information contained therein, in order to ensure their availability, integrity, authentication, confidentiality, and non-repudiation” (NIST, 2026). The concept covers both technical solutions (e.g., firewalls and encryption) and organizational measures such as policies, training, and risk management. As society becomes increasingly digitalized, cybersecurity has become a central component of business operations, since critical business processes are increasingly dependent on IT systems.

Types of cyberattacks include:

- Ransomware (online extortion)
- Phishing (attempts to gain access to passwords and card information)
- CEO fraud (executive impersonation fraud, where someone pretends to be a manager or CEO in order to obtain money transfers or sensitive data)
- Invoice fraud (payment of a fake or altered invoice)
- DDoS attacks (overloading websites or services)
- Malicious insiders (e.g., an employee who intentionally abuses their access to systems and data)
- Supply chain attacks (attacks carried out through business partners or suppliers)

The threat level in Denmark is assessed as very high for both cybercrime and cyber espionage (Danish Agency for Societal Security, 2025, p. 6), and it is considered likely that both companies and public authorities will be affected by cybercrime. Furthermore, a study on digital security shows that 52% of companies have experienced an IT security incident (Danish Agency for Societal Security, 2024, p. 35).

SMEs can protect themselves against cyberattacks by combining technical solutions, clear procedures, and a strong focus on employee behavior. First and foremost, it is crucial to maintain solid basic IT security, including continuous software updates, the use of antivirus software and firewalls, and the implementation of multi-factor authentication, since many attacks exploit known vulnerabilities. In addition, companies should work systematically with access management through strong and unique passwords, as well as by limiting user privileges in order to reduce the risk of unauthorized access.

Employee training also plays a central role, as many attacks begin with phishing attempts. It is therefore important to build awareness and the ability to recognize suspicious inquiries (Mayer et al., 2023). At the same time, SMEs should establish regular backups and a contingency plan so they can quickly restore data and operations in the event of an attack, particularly in cases of ransomware. Finally, companies can adopt a risk-based approach by identifying critical systems, monitoring for unusual activity, and setting security requirements for suppliers, since many attacks occur through supply chains (Melnyk et al., 2022).

> **“The project has helped us evaluate our level of maturity in both cybersecurity and risk management. It has been highly enlightening.”**
>
> *CEO Jes Gravesen, Engskov Maskinfabrik A/S*

2.5 Business Continuity

Business continuity in Danish manufacturing SMEs concerns a company’s ability to maintain or quickly resume critical activities in the event of unforeseen incidents such as supplier failures, cyberattacks, fire, pandemics, energy crises, or the sudden loss of key employees. For manufacturing companies, continuity is particularly important because value creation depends on physical facilities, machinery, inventory, and stable deliveries throughout the value chain.

The size and organizational structure of SMEs directly influence how they work with business continuity. According to Hiles (2014, p. 2), the following benefits can be achieved by integrating business continuity practices:

- A more robust operational infrastructure
- Compliance with legal, regulatory, and quality-related requirements for risk assessment and risk management
- The ability to continue fulfilling the company's mission in the event of a disaster
- The ability to continue operating profitably during a disaster
- The ability to maintain market share during a disaster
- Improved employee morale, as employees know that management is protecting jobs
- Protection of the company's reputation, image, and brand value

A key characteristic of manufacturing SMEs is their dependence on a limited number of key individuals and specialized competencies. Often, individual employees possess unique knowledge (including tacit knowledge) about machine setup, customer specifications, or production flow. If these individuals are suddenly absent, production may be severely disrupted. Business continuity therefore requires systematic knowledge sharing, process documentation, and potentially cross-training, enabling multiple employees to perform critical functions.

Supplier dependency is another significant risk factor. Many manufacturing SMEs operate as subcontractors within larger value chains while simultaneously relying on specific raw materials or components. Global disruptions, such as those experienced during COVID-19 and the energy crisis, can create supply shortages and price volatility. Continuity efforts therefore involve supply chain risk assessments, alternative suppliers, inventory strategies, and contractual safeguards.

Digitalization has increased efficiency in many manufacturing SMEs, but it has also created new vulnerabilities. Production management systems, ERP systems, and automated facilities (controlled by Operational Technology — OT) are often connected to networks. As a result, cyberattacks may halt production or compromise data. The Danish Agency for Societal Security (2024) highlights that smaller companies are also targets of cybercrime. Business continuity therefore includes backup solutions, access management, contingency planning, and cybersecurity training.

Physical risks also play a central role. Fire, machinery breakdowns, or power outages can have immediate and costly consequences. For manufacturing SMEs, even short-term interruptions often result in lost revenue and risks of contractual penalties from customers. A continuity plan should therefore identify critical assets, define recovery times, and describe procedures for temporary production, outsourcing, or collaboration with partners.

Resource scarcity is a challenge for many SMEs. They rarely have dedicated risk managers or compliance functions. Consequently, continuity efforts are often informal and dependent on individuals. International standards such as ISO

22301 for business continuity management systems exist (Crask, 2024), but implementation may be perceived as resource-intensive. For Danish manufacturing SMEs, a pragmatic approach may therefore be appropriate: a simple written contingency plan, regular risk assessments, and testing of key procedures.

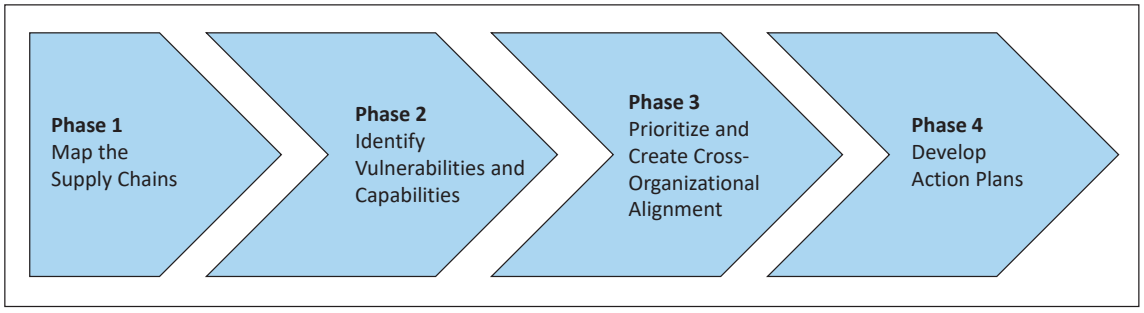
Business continuity should be viewed as an integrated part of the company's strategy rather than merely an insurance-related matter. A robust continuity effort can strengthen customer trust, competitiveness, and collaboration within the value chain. Today, many larger customers require documented risk management from their suppliers, making continuity planning a commercial necessity.

In summary, business continuity in Danish manufacturing SMEs is closely linked to managing dependency on key individuals, supplier risks, digital vulnerabilities, and physical operational disruptions. Although resources are often limited, a structured and systematic approach can significantly reduce vulnerability and contribute to long-term stability and sustainable growth.

2.6 Supply Chain Resilience Process Model

Supply chain resilience (SCRES) refers to a company's ability to remain operational, adapt, and recover from disruptions in the supply chain. Rather than merely describing strategies or theoretical concepts, Stentoft, Mikkelsen & Kjær (2024) and Stentoft & Mikkelsen (2024) propose a structured process framework - that is, a model illustrating how companies can systematically develop resilient behavior (see Figure 2.2).

Figur 2.2 Supply Chain Resilience Process Model



Source: Stentoft, Mikkelsen & Kjær (2024, p. 53)

The SCRES process model consists of four main phases based on empirical research among 18 Danish manufacturing SMEs: 1) mapping the supply chain, 2) individual identification of vulnerabilities and capabilities, 3) prioritization and cross-organizational alignment, and development of action plans. The process begins with supply chain mapping, where representatives from key functions collaboratively develop an overview of customers, suppliers, flows, and operational dependencies in order to create a shared understanding of the challenges. The second phase focuses on identifying vulnerabilities and capabilities, where participants individually assess risks and the organi-

zational strengths required to address them, supported by a structured digital tool. In the third phase, work is carried out across organizational functions to consolidate the individual assessments into a shared prioritization and ranking of the most critical vulnerabilities and associated capabilities. Finally, the model moves into the development of action plans, where priorities are translated into concrete, time-bound initiatives that assign responsibilities and support implementation, ensuring that improvements in resilience become integrated into the organization's ongoing practices.

> **"A major strength has been the involvement of several functions across the company. This has created broader buy-in and stronger ownership of the results."**
>
> *COO Søren Lind Therkildsen, GomSpace A/S*

2.6.1 Supply Chain Mapping

Purpose

To create an overall overview of the company's supply chain and its critical dependencies.

Contents of the Phase

- Identification of key customers
- Identification of key suppliers (direct and potentially indirect)
- Mapping of material flows, information flows, and financial flows
- Identification of critical products, components, and bottlenecks
- Visualization of geographical and structural concentrations

Practical Point

Resilience cannot be strengthened without transparency. Many SMEs have limited visibility into their upstream tiers (their suppliers' suppliers), which creates hidden vulnerabilities.

Output

A visual map of the supply chain, along with a list of critical nodes and dependencies.

2.6.2 Individual Identification of Vulnerabilities and Capabilities

Purpose

To identify where the supply chain is vulnerable and which internal strengths can compensate for these vulnerabilities.

Vulnerabilities may include:

- Single sourcing
- Geographical concentration
- Long lead times
- Low inventory buffers
- Limited information sharing

Capabilities may include:

- Flexible production
- Close supplier collaboration
- High internal coordination
- Digital transparency
- Rapid decision-making

Practical Point

The model links risk (vulnerability) and capability (ability). Resilience is understood not only as risk reduction, but also as the ability to absorb disruptions, adapt, and emerge stronger from them

Output

A systematic assessment (often workshop-based) of where the company is most exposed - and where it possesses strengths.

2.6.3 Prioritization and Cross-Organizational Alignment

Purpose

To create a shared understanding and prioritization across functions (procurement, production, sales, logistics, and management).

Why is this phase central?

In many SMEs, knowledge about risks is dispersed across the organization. Resilience requires:

- A shared understanding of risks
- A shared prioritization of focus areas
- Management anchoring and support

Typical Activities

- Cross-functional workshops
- Discussion of trade-offs (e.g., inventory levels versus capital tied up in stock)
- Determining which vulnerabilities are the most critical
- Deciding on the desired level of ambition

Practical Point

Resilience is an organizational process and not merely a technical supply chain tool. Alignment reduces silo thinking.

Output

A prioritized list of focus areas with management support and commitment.

2.6.4 Development of Action Plans

Purpose

To translate the analysis into concrete actions.

Examples of Actions

- Dual sourcing
- Building safety stock
- Developing alternative suppliers
- Investing in digital traceability
- Formalizing contingency plans
- Strengthening collaboration with key suppliers

Central Elements of the Model

- Action plans must be realistic for SMEs
- Initiatives are prioritized based on impact and practical feasibility
- The process is iterative (resilience is not a one-time exercise)

Output

Concrete, time-bound initiatives with assigned responsibilities and follow-up procedures.

To operationalize the model, we have developed a dedicated web application that guides organizations through each phase of the process. The platform enables coordination among participating team members and supports the independent completion of Phase 2, allowing individuals to assess vulnerabilities and capabilities at a time that suits them. The system automatically generates function-specific reports and consolidates them into an integrated environment for data visualization and analysis in Phase 3.

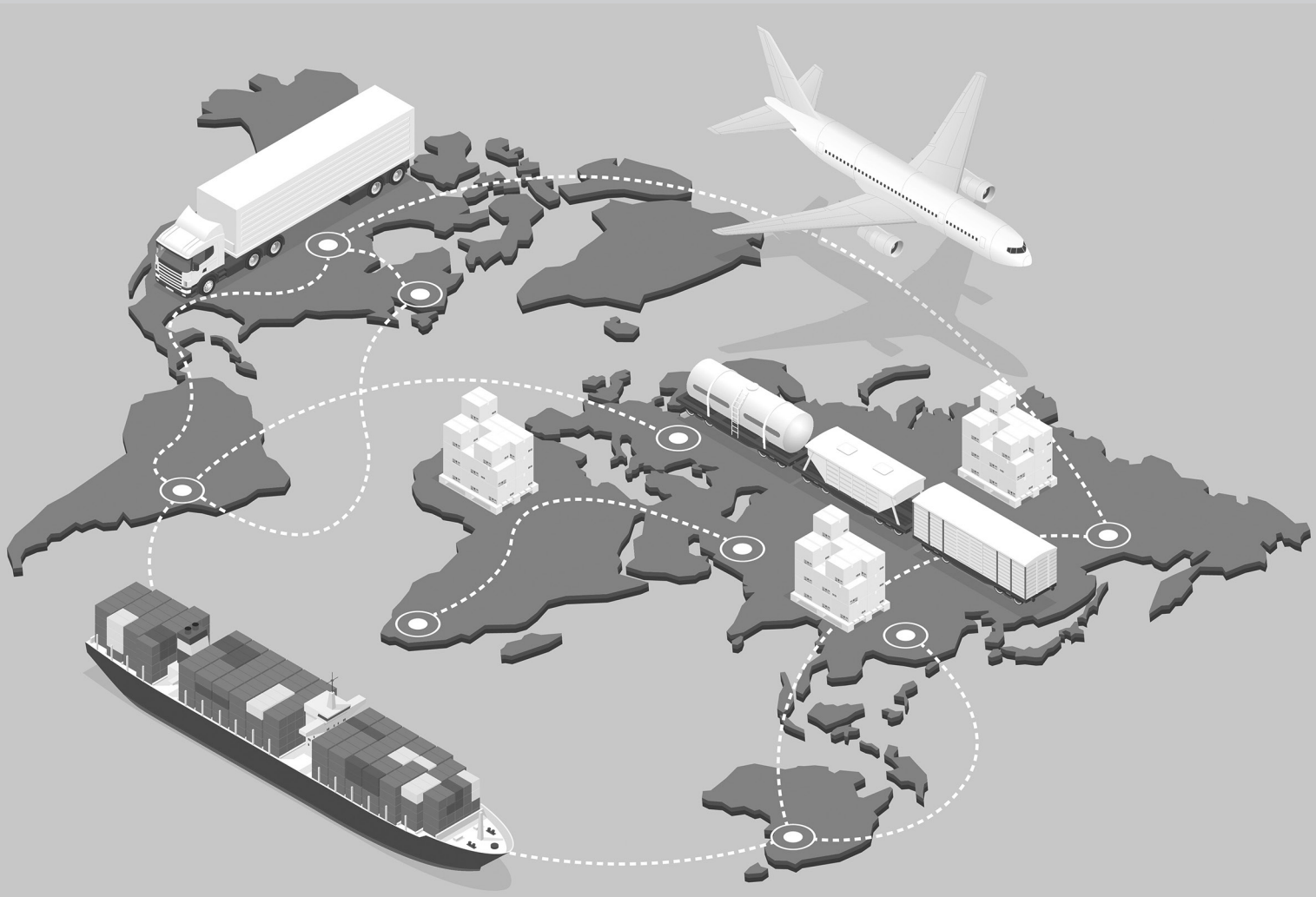
Within this workspace, participants can examine perspectives across functions, identify overlapping vulnerabilities, compare perceived risks and mitigating capabilities, and analyze differing priorities in a structured manner. Following the alignment workshop, the system produces a comprehensive interactive report with options for customized views and tailored outputs, providing a practical foundation for action planning in Phase 4.

The application is freely available via the project website (**https://process-model.cyber-smv.dk/**), where materials and documentation are also available for companies wishing to self-host the solution.

In parallel, the project has developed an updated set of vulnerabilities and capabilities with a particular focus on cybersecurity and supply chain resilience. These are based on current best practices and derived from interviews with Danish decision-makers, industry organizations, and companies operating in critical sectors, including defense, IT, and telecommunications. The purpose is to ensure that the model reflects emerging threat landscapes and regulatory expectations while remaining practically applicable for companies operating in strategically sensitive industries.

2.7 Cybersecurity Supply Chain Risk Management

NIST CSF 2.0 is an internationally recognized cybersecurity framework published by the U.S. National Institute of Standards and Technology (NIST) in 2024. NIST CSF 2.0 provides practical guidance on how organizations can manage and improve their cybersecurity. It is neither a law nor a certification. Cybersecurity Supply Chain Risk Management (C-SCRM) in NIST CSF 2.0 is a systematic process for identifying, assessing, managing, and improving cybersecurity risks arising through suppliers of technology, software, services, and components. It includes both physical products and digital products and services within the supply chain ecosystem. C-SCRM is no longer merely a supplement to cybersecurity but is integrated as a category under the new Govern (GV) function. This means that supply chain risks are now considered a core component of strategic cybersecurity governance, rather than something handled ad hoc within the IT department alone.



NIST CSF 2.0 has consolidated C-SCRM practices under the Govern function into 10 specific subcategories (the precise practices/requirements) that organizations should implement to manage cybersecurity risks in their supply chains (NIST, 2024):

GV. Supply Chain-01: Establish a C-SCRM Program and Governance
- Establish a cybersecurity supply chain risk management program, strategy, objectives, policies, and processes aligned with relevant organizational stakeholders.

GV. Supply Chain-02: Roles and Responsibilities
- Define and communicate cybersecurity roles and responsibilities for suppliers, customers, and partners, both internally and externally.

GV. Supply Chain-03: Integration into Risk and Improvement Processes
- Integrate C-SCRM into cybersecurity risk management, enterprise risk management, risk assessments, and continuous improvement processes.

GV. Supply Chain-04: Supplier Awareness and Prioritization
- Identify and prioritize suppliers according to their criticality to the organization's mission and operations.

GV. Supply Chain-05: Security Requirements in Contracts and Agreements
- Establish, prioritize, and integrate cybersecurity risk requirements into contracts and agreements with suppliers and relevant third parties.

GV. Supply Chain-06: Planning and Due Diligence Before Engagement
- Conduct planning and due diligence to reduce risks before formalizing supplier or partnership relationships.

GV. Supply Chain-07: Risk Analysis and Monitoring Throughout the Supplier Relationship Lifecycle
- Understand, document, prioritize, assess, respond to, and monitor the risks posed by a supplier and its products/services throughout the duration of the relationship.

GV. Supply Chain-08: Incident Planning, Response, and Recovery with Suppliers
- Include relevant suppliers and third parties in cybersecurity incident planning, response, and recovery activities.

GV. Supply Chain-09: Life-Cycle Monitoring
- Integrate supply chain security practices into cybersecurity and enterprise risk management programs and monitor their performance from a product/service lifecycle perspective.

GV. Supply Chain-10: Post-Termination of Partnership or Service Agreement
- C-SCRM plans should include provisions for activities following the termination of a partnership agreement or service agreement.

On **www.cyber-smv.dk** under the "Tools" section, the above 10 practices have been operationalized into concrete tools.

2.8 Dynamic Capabilities

Dynamic capabilities are a central concept in strategic management theory, most notably formulated by Teece, Pisano & Shuen (1997). They define dynamic capabilities as a company's ability to integrate, build, and reconfigure internal and external competencies in order to address rapidly changing environments. The concept was later further developed by Teece (2007), who specified dynamic capabilities through three overarching processes: 1) sensing, 2) seizing, and 3) transforming. In contrast to the classical Resource-Based View (RBV), which focuses on valuable, rare, and difficult-to-imitate resources (Barney, 1991), dynamic capabilities emphasize the dimension of change. The focus is not only on what resources a company possesses, but also on how it continuously adapts and renews those resources.

As mentioned earlier, Teece (2007) divides dynamic capabilities into three main processes: 1) sensing, 2) seizing, and 3) transforming (see Table 2.1).

Table 2.1 Sensing, seizing and transforming

Sensing	The ability to identify and interpret opportunities and threats in the external environment. This involves monitoring technological, market-related, and institutional changes. For manufacturing SMEs, this may, for example, include changes in trade regimes, new security standards, or the emergence of digital threats.
Seizing	The ability to mobilize resources and make strategic decisions based on the identified opportunities and threats. This may involve investing in new technologies, changing the supplier structure, or developing new security procedures.
Transforming	The ability to continuously restructure the organization's assets, processes, and relationships so that the company remains competitive. This may involve organizational changes, new forms of collaboration, or changes to the business model.

Source: Teece (2007)

Dynamic capabilities can be understood as meta-capabilities that govern a company's ability to renew its operational capabilities. Manufacturing SMEs increasingly operate within a globalized and digitalized risk landscape. Two areas of development are particularly central: geopolitics and cybersecurity.

2.8.1 Geopolitical Uncertainty

Geopolitical tensions, trade restrictions, sanctions, and the regionalization of value chains directly affect supply security and market access. Examples include trade conflicts between major powers, the war in Ukraine, and the increasing focus on strategic autonomy within the EU. For manufacturing SMEs, which are often highly dependent on a limited number of suppliers or specific regions, geopolitical instability can lead to:

- Supply disruptions
- Rising input prices
- Regulation and export controls
- Requirements for documentation and compliance

In this context, sensing becomes crucial for SMEs. Political and regulatory changes should be monitored systematically. Seizing concerns the ability to respond — for example through practices such as dual sourcing, nearshoring, or inventory buildup. Transforming may involve the strategic restructuring of the entire supply chain setup. Without dynamic capabilities, SMEs risk responding too late or in a fragmented manner.

2.8.2 Cybersecurity as a Strategic Risk Factor

The digitalization of manufacturing (Industry 4.0, IoT, ERP integration, and cloud solutions) increases efficiency but also vulnerability. Cyberattacks can disrupt production, compromise data, and damage relationships within the value chain. The Danish Centre for Cyber Security has conducted a threat assessment for Denmark based on five categories of attacks, each individually assessed: Cybercrime (VERY HIGH), cyber espionage (VERY HIGH), cyber activism (HIGH), destructive cyberattacks (MEDIUM), and cyberterrorism (NONE) (Danish Agency for Societal Security, 2025, p. 6). For manufacturing SMEs, the challenge is often limited resources and a lack of specialized security expertise. In this context, dynamic capabilities become essential, because cybersecurity is not merely a technical issue, but also a matter of organizational learning and adaptation:

- **Sensing:** Monitoring the threat landscape and regulatory requirements (e.g., the EU NIS 2 Directive)
- **Seizing:** Investing in security systems, training, and governance structures
- **Transforming:** Integrating cybersecurity into the company's strategy and culture

Cybersecurity thus becomes an integral part of the company's strategic resilience.

3.
Method

The overall project has been carried out using a variety of methods, which are briefly described in the three subsections below.

3.1 Three Hierarchical Levels of Analysis

The project's methodological approach is structured around three hierarchical levels of analysis, the political level, the industry level, and the company level, in order to ensure a coherent translation of abstract geopolitical threats into concrete actions within SMEs. This structure enables a systematic breakdown of complex macro-level conditions into operational practice.

3.1.1 The Political Decision-Making Level

The process began with workshops involving experts from the Danish defense and foreign policy community, including representatives from the Royal Danish Defence College and the Ministry of Foreign Affairs. The purpose was to identify and define the most pressing geopolitical drivers and crises for the period 2025–2030 using PESTEL variables (political, economic, social, technological, and legal). Through an uncertainty/impact matrix, the participants selected the scenarios that combined high severity with high uncertainty, forming the basis for the project's five main scenarios.

The process was carried out in two separate iterations with different groups of experts. It is important to note that the second group, without having been introduced to the results of the first workshop, independently generated exactly the same scenarios. This remarkable convergence can be attributed to a combination of high structural determinism in the current threat landscape and the existence of an epistemic community among Danish security policy actors. The fact that two independent groups identified identical drivers indicates that the geopolitical macro-trends (such as great-power rivalry and climate change) currently appear so significant that they dominate the strategic horizon across observers. This confirms that the scenarios are not merely arbitrary speculations but rather represent a consolidated understanding of the structural conditions within which Danish industry operates.

3.1.2 The Industry Level (Contextualization)

The identified geopolitical themes were subsequently refined through workshops with industry associations and industrial actors, such as the Confederation of Danish Industry (DI) and SMVdanmark. At this level, the task was to translate the broad political scenarios into specific sector vulnerabilities. The participants discussed the cybersecurity and supply chain implications that each scenario would have for Danish industry and identified the capabilities that would be required to address them. This ensured that the scenarios were not merely grand geopolitical narratives but also contained relevant industrial risk factors. Valuable input was also provided for the developed scenarios, strengthening the focus on cybersecurity.

3.1.3 The Company Level

The third level involved direct interaction with Danish manufacturing SMEs through two programs (the first program, involving company participants in four workshops, took place in November 2024, and the second program, consisting of four workshops, took place from December 2025 to March 2026). The eight workshops were held for groups of 3–5 companies at various conference locations across Denmark (Aalborg, Hobro, Brande, Middelfart, Kongens Lyngby, and Hvidovre). The agenda for these sessions included:

- Discussion of cybersecurity (company-specific in breakout rooms)
- Overview of future scenarios (in plenary sessions)
- Work on one or more future scenarios (company-specific in breakout rooms)
- Summary and discussion of future scenarios and cybersecurity discussions (in plenary sessions)

The companies selected the scenario they considered most relevant to their business model and worked systematically to identify specific risks and vulnerabilities within their own supply chains. The method shifted the focus from general risk analysis toward concrete discussions of mitigation measures and the need for new dynamic capabilities in an uncertain future.

After the completion of the four workshops in each program, the companies gathered at the University of Southern Denmark in Odense for a day of cyber training. The following topics were covered:

- Presentation by Hotel Koldingfjord about their cyberattack (first program only)
- Cybersecurity — best practices and Q&A
- Cloud — best practices and Q&A
- Geopolitics and Q&A
- Supply chain risk management / supply chain resilience and Q&A
- Tools — a guided walkthrough
- Case study / pentesting including Q&A (second program only)
- Panel debate
- Summary

> **”We participated in order to gain an honest view of our vulnerabilities - not in the IT systems, but in the business and in our own behavior. The energetic facilitation provided by the project, drawing on real-life experiences, created a sense of presence and credibility that triggered a surprising number of “aha” moments. It prompted the management team to both think and feel.”**
>
> *Head of Legal & Compliance Ple Anker Aagaard, ExamVision A/S*

3.2 Focus Group Discussions

Focus group discussions with the stakeholders mentioned in Section 3.1 were audio-recorded, encrypted, and transcribed using Whisper (locally, without AI). Manual verification ensured accurate transcription. The transcripts were imported into MAXQDA, a qualitative analysis tool. The coding of the data was carried out over several cycles. The first coding round combined in-vivo coding (participants’ own words) and initial coding in order to generate open codes across stakeholder levels. The second coding round applied axial coding to explore relationships between the codes. Focused coding highlighted recurring patterns in the data, while theoretical coding elevated these into broader, interconnected themes. The codes were subsequently reorganized into thematic categories and consolidated into overarching themes. Two senior researchers continuously reviewed the emerging themes, and a detailed audit trail was maintained. The developed codebook, describing all codes, definitions, and example quotations, was made available as supplementary material to ensure transparency and reproducibility.

3.3 Questionnaire Surveys

As part of the project, two nationwide questionnaire surveys focusing on cybersecurity among Danish manufacturing SMEs were conducted (Stentoft et al., 2024 and 2026). The target groups consisted of Danish manufacturing companies with 20–250 employees within NACE industry codes 10–33. The companies were identified through the Navne & Numre Erhverv database, which includes all VAT-registered companies in Denmark. A total of 248 companies participated in the 2024 survey and 155 companies participated in the 2026 survey.

4.
Results

4.1 Different Perceptions of Cybersecurity Among Three Stakeholder Groups

The purpose of the project is to strengthen cybersecurity in Danish manufacturing SMEs. It began with a particular focus on SMEs within the defense industry, with the understanding that the project's results should be applicable across all industries and company sizes.

The following presents the results of a study of stakeholders within Denmark's defense supply chain. The study included focus group discussions with 45 participants from three stakeholder groups:

1) *The political decision-making level* (n=6), consisting of representatives responsible for national security and the Ministry of Foreign Affairs. They contribute strategic insights regarding national cybersecurity and international cooperation.

2) *The industry level* (n=11), consisting of industry experts from the defense sector who identify patterns and validate threats.

3) *The company level* (n=28 from 12 SMEs), consisting of managers, middle managers, and employees within SMEs who report on operational realities.

The analysis mapped mental models across these groups, examined perceptions of cybersecurity, and identified misalignments that may contribute to vulnerabilities. These misalignments have practical implications for translating policy into concrete action.

To structure the findings, two themes guide this section: 1) vulnerabilities and capabilities, 2) and

mental models of cybersecurity across stakeholder levels. Practical implications are discussed continuously throughout the section.

4.1.1 Vulnerabilities and Capabilities

A vulnerability/capability perspective based on supply chain resilience theory (Pettit, Fiksel, & Croxton, 2010; Pettit, Croxton & Fiksel, 2013) was applied to map the findings. These may be viewed as a supplement to the supply chain-related vulnerabilities and capabilities identified by Stentoft, Mikkelsen & Kjær (2024). The vulnerabilities are presented in Table 4.1. Vulnerabilities are structural conditions that make organizations susceptible to disruptions. Capabilities are characteristics that help organizations anticipate and manage such disruptions. Based on the analytical framework of vulnerabilities and capabilities developed by Pettit, Fiksel, & Croxton (2010) and Pettit, Croxton & Fiksel (2013), the focus group data reveal a clear imbalance: 27 organizational vulnerabilities distributed across five categories, but only 10 capabilities distributed across three categories. The gap is greatest at the SME level, where companies possess few formal cybersecurity capabilities. Instead, they rely on responsiveness, backup solutions, outsourced IT, cyber insurance, and informal crisis communication.

Table 4.1 Cyber-Related Vulnerabilities

Human and Cultural Vulnerabilities

- Insecure and inappropriate behavior
- Lack of cybersecurity training
- Lack of prioritization
- Outdated managerial decision-making
- Reluctance to share vulnerabilities with authorities

Operational and Regulatory Vulnerabilities

- Overwhelming regulatory burdens
- Cybersecurity as a secondary priority
- Inadequate contingency planning
- Communication gaps
- Limited resources / resource scarcity
- Lack of robustness in critical digital infrastructure
- Complexity of international standards
- Uncertainty regarding export controls

Technical Vulnerabilities

- Overdependence on specific technologies
- Outdated systems (legacy systems)
- Risks associated with disruptive technologies
- High degree of digitalization
- Hacking and ransomware
- Multiple access points

Supply Chain Vulnerabilities

- Supplier dependency (vendor lock-in)
- Third-party vulnerabilities
- Lack of transparency in the supply chain
- Dependence on a limited number of IT suppliers/companies

Geopolitical Vulnerabilities

- Denmark's geopolitical positioning
- Vulnerabilities in Greenland and the Faroe Islands
- Risk of foreign interference
- Industry-specific threats

Source: Kankam-Boateng et al. (2026)

As shown in Table 4.1, the vulnerabilities are divided into five areas:

1. *Human and cultural vulnerabilities* are the largest category and cut across all three stakeholder groups. Low general awareness, a culture of excessive trust, and cost-driven views on cybersecurity were identified at all levels. However, the nature of the problem varies between the groups. Decision-makers and policy actors highlighted systemic challenges such as a lack of competencies, aging leadership, and fragmented cybersecurity education. SMEs pointed to local challenges: uneven employee awareness, limited management engagement, and unregulated use of mobile devices. Denmark's high-trust culture is double-edged. It enables rapid collaboration and informal communication but reduces the skepticism necessary to protect against insider threats and social engineering.

2. *Operational and regulatory vulnerabilities*. Cybersecurity is often perceived as being outside the core business. There is limited scenario planning and fragmented collaboration. Dependence on individual suppliers or key persons creates fragility. This is especially true for SMEs, where cybersecurity knowledge is often concentrated in a single person, typically the CEO. The complex regulatory landscape, including NIS 2, ISO 27001, NIST, and NATO standards, is perceived as a barrier to effective implementation. One company spent more than 500 hours merely trying to understand NIS 2. Uncertainty regarding the responsibilities of the Danish Agency for Societal Security (SAMSIK) creates additional confusion. None of the SMEs mentioned SAMSIK or the national cybersecurity coordination point, despite its prominent role among decision-makers.

3. *Technical vulnerabilities.* The combination of modern systems and legacy infrastructure creates systemic risks and single points of failure. Overdependence on certain technologies, particularly Microsoft, increases risk. Most participants expressed concern that new technologies such as AI and quantum computing are developing faster than defensive measures. Denmark's high level of digitalization is a strength, but it also expands the attack surface and often outpaces existing security measures.

4. *Supply chain vulnerabilities.* Dependence on a small number of IT suppliers creates concentration risk, especially when verification processes are weak. Compliance-related dependencies in the supply chain arising from NIS 2, combined with limited insight into subcontractors' practices, further increase exposure.

5. *Geopolitical vulnerabilities.* Denmark's international alliances (NATO, support for Ukraine, etc.) increase visibility toward state-sponsored threats. Decision-makers and policy actors expressed concern regarding the resilience of Greenland and the Faroe Islands, an issue that did not appear in the responses from SMEs.

The capability landscape is significantly limited at the SME level (see Table 4.2). At the national level, decision-makers identified important assets: centralized incident management, the benefits of NATO membership, and advanced digital infrastructure. Actors at the political decision-making level identified similar strengths. However, these strengths do not effectively reach the SMEs

they are intended to support. This leads to what the analysis describes as a capability translation problem. The translation fails between the political decision-making level and the industry level when strategies establish objectives without specifying how they should be operationalized. It also fails between the industry level and the company level (the SMEs), as guidance does not reliably reach the companies that need it the most. Uncertainty regarding the distribution of cybersecurity responsibilities between public and private actors further reinforces the problem.

Table 4.2 Cyber-Related Capabilities

Strategic Capabilities

- Participation in international initiatives
- Public-private partnerships
- Strategic investments in compliance
- Engagement in the cybersecurity industry
- Organizational agility

Human and Cultural Capabilities

- Cybersecurity training for management
- Cybersecurity awareness programs
- Transparency and a responsive culture
- Trust-based knowledge sharing and influence

Technical Capabilities

- Leveraging advanced digital infrastructure

Source: Kankam-Boateng et al. (2026)

Practical Implications. The 27:10 ratio between vulnerabilities and capabilities quantifies a qualitative reality. These SMEs know more about what threatens them than about what protects them. Addressing this requires differentiated initiatives. Decision-makers should complement regulation with practical implementation support tailored to SMEs' capacities and adopt shorter, more responsive strategy cycles. Policymakers should develop sector-specific, simplified guidance and facilitate experience-sharing among SMEs. SMEs themselves should appoint a person responsible for cybersecurity, develop basic contingency plans, and use existing informal capabilities as a foundation for more structured practices. Two of the companies invested in formal programs and reported increasing benefits in employee behavior and preparedness. This suggests that the barrier is less about resources and more about framing and prioritization. A coordinated national cybersecurity ecosystem can help manage supply chain risks and enable joint incident management.

4.1.2 Mental Models of Cybersecurity Across Stakeholder Levels

Mental models are the internal representations that people use to understand and reason about complex domains. They shape how cybersecurity risks are understood and managed. We present the first empirical mapping of mental models of cybersecurity across three stakeholder levels within a defense industry supply chain. The study reveals inconsistencies that help explain persistent gaps between political intentions and actual security outcomes. The analysis revealed significant differences in how stakeholder groups conceptualize and approach cybersecurity. Decision-makers described a disconnect between national strategies and their implementation at the SME level, particularly regarding risk understanding and resource allocation. Industry experts highlighted challenges related to coordination, limited investments in research and development, and difficulties in aligning national and international standards. Representatives from SMEs adopted a reactive approach. They often responded primarily to regulation or customer requirements. They also reported shortcomings in incident management, supply chain risk assessment, and the integration of cybersecurity into contingency and continuity planning. Table 4.3 presents the most significant misalignments in the mental models.

Table 4.3 Key Misalignments in Mental Models

Dimension	The Political Level	The Industry Level	The Company Level
Framing of Cybersecurity: The Divide Between Cost and Investment	Strategic Investments	Economic Burden	Economic Burden and Compliance
The Herring Effect	Proactive, Interconnected	Swareness of SMEs' Challenges	Reactive 'Herring Effect'
Differences in Threat trusselsopfattelser	State and Non-State Actors	State and Non-State Actors	Only Non-State Actors
Regulation	Manageable	Awareness of the Burden on SME's	Overwhelming, Unmanageable and Confusing

Source: Based on Kankam-Boateng et al. (2026)

The Divide Between Cost and Investment. A clear difference emerged in how stakeholders perceive cybersecurity. Decision-makers view it as a strategic investment, whereas actors at the industry level and SMEs primarily regard it as an economic burden. Most SMEs perceive cybersecurity as a cost driven by regulatory compliance requirements or the need for cyber insurance, rather than as something capable of creating business value. This cost-oriented perspective contrasts with the growing body of evidence showing that investments in security can generate positive returns through increased customer trust, regulatory compliance that opens market opportunities, and reduced costs associated with security breaches. This framing is important because it influences how SMEs allocate resources. When cybersecurity is viewed as a cost to be minimized rather than as a capability to be developed, investment decisions will typically follow a minimum-compliance approach rather than a strategic one.

The "Herring Effect": Collective Anonymity as a Security Strategy. A recurring insight was that SMEs rely more on collective anonymity than on individual defense mechanisms. Actors at the industry level described how smaller companies behave like a school of herring hoping not to be singled out by the predator. This reactive approach stems from several barriers: limited resources, lack of attention, and difficulties navigating complex regulatory frameworks. Only three out of the twelve participating SMEs had implemented formal cybersecurity awareness training programs. Most relied on informal communication during meetings and lunch breaks. Importantly, this was not due to ignorance, but rather a deliberate choice reflecting resource constraints and organizational culture. Participants explicitly emphasized that their size made informal communication sufficient.

Differences in Threat Perceptions. The political level and the industry level perceive a broad and interconnected threat landscape that requires proactive vigilance. They believe that SMEs underestimate both the scale of the threats and their own value as targets. In contrast, SMEs primarily focus on threats from non-state actors, such as ransomware and opportunistic attacks, whereas the political and industry levels also recognize that state actors deliberately target SMEs, for example for technology theft or the implementation of "kill switches" in their systems. The geopolitical dimension of cybersecurity was entirely absent from the SMEs' discussions, yet central to discussions at the political and industry levels. This gap means that SMEs fail to implement protective measures against systemic threats that they do not perceive as relevant.

Regulatory Complexity as a Vulnerability. Paradoxically, the regulatory environment does not necessarily strengthen security but may instead weaken it by overburdening SMEs' capacity to respond. Frameworks designed to improve security become barriers when SMEs lack the resources needed to interpret and implement them. The result is what may be described as "compliance theater" - organizations formally satisfy compliance requirements while neglecting actual security. When consultants are hired to fill gaps in compliance documentation, SMEs fail to build internal cybersecurity knowledge or organizational capability.

Cultural Context: High Trust as a Double-Edged Sword

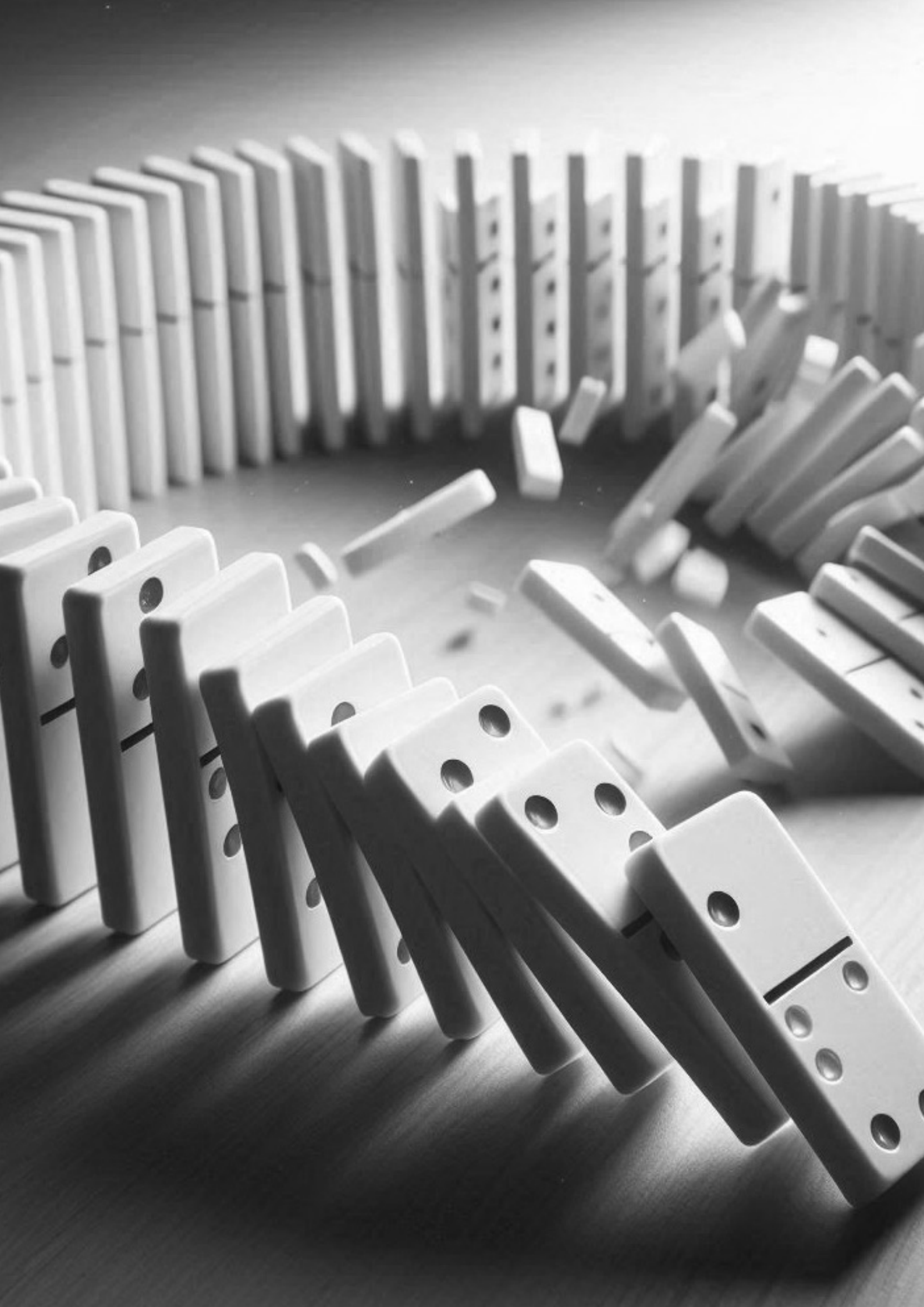
Denmark's high-trust culture shapes both the underlying mental models and the dynamics of cybersecurity governance. The trust-based and open approach embedded in Danish society promotes collaboration and rapid, informal communication, but it also creates security vulnerabilities. Employees may freely share sensitive information with individuals who appear to be part of the organization, an advantage for collaboration, but a risk to security. Research into the working practices of Danish SMEs shows that employees share passwords to avoid disruptions to workflows and deliberately break rules on a small scale in order to maintain flexibility. This points to sophisticated informal security practices that formal policies do not necessarily recognize or support. The high level of trust also contributes to the previously mentioned "herring effect," where collective rather than individual action becomes the norm.

Practical Implications

These divergent mental models indicate that differing perceptions contribute to fragmented initiatives and uneven preparedness across the cybersecurity landscape. Several implications follow from this. First, cybersecurity should be reframed as a business driver. SMEs within the defense sector achieved high standards when motivated by sector-specific requirements, indicating that highlighting business value can help overcome resource constraints. Second, the "herring effect" points to the need for contextualized micro-learning modules (5–10 minutes) rather than extensive training programs, delivered through mobile platforms and searchable by topic. Third, learning networks should leverage advanced SMEs as mentors. Fourth, decision-support tools should provide contextually relevant recommendations based on the organization's size, sector, and threat profile. Fifth, compliance-mapping tools should demonstrate how compliance with one standard can simultaneously satisfy requirements in others, thereby reducing the perceived burden. Sixth, national cybersecurity actors should strengthen their public visibility and establish clear communication channels so that SMEs know where to seek assistance. Training programs should be better adapted to SMEs' needs, with a focus on practical competencies in protection, detection, response, and continuity planning. Finally, integrating cybersecurity into business planning and strengthening a security-aware culture may enhance resilience more effectively than isolated awareness campaigns.

4.2 Supply Chain Risk Management: New Insights from Geopolitics

This section summarizes the project group's work on identifying new types of supply chain risks arising from geopolitics in a new world order. The section is based on Stentoft, Schmitt & Keating (2024).



4.2.1 A New Strategic Competition

The end of the Cold War marked a decisive turning point for the global economy and the development of modern supply chains. The collapse of the Soviet Union created optimism about a new world order characterized by liberal capitalism and increased global integration. During this period, it was assumed that there was no real ideological competitor to the Western economic model and that national borders would become less significant as trade, investment, and technological development increased. This development led to a separation between economic policy and security policy. Trade liberalization and the establishment of international institutions such as the WTO and the EU contributed to more stable and predictable frameworks for businesses. At the same time, a form of "transnational governance" emerged, in which states cooperated on regulation and standards, making it easier for companies to operate globally. Companies increasingly began to perceive themselves as international rather than national actors, enabling outsourcing and global supply chains driven primarily by economic considerations.

A central concept during this period was interdependence. The idea was that increased economic integration would not only create prosperity but also reduce the risk of conflict because states and populations would have too much to lose from war. This idea supported the assumption that economics and security could be separated, and that globalization itself would contribute to stability. Although this order was not without challenges, it created a relatively stable and predictable environment for businesses. Supply chain decisions were primarily made on the basis of economic criteria rather than political considerations. However, this understanding has been challenged over the past decade. The international order is under pressure from increasing geopolitical competition, where new powers challenge the Western-dominated world order. Examples such as Russia's invasion of Ukraine and tensions between the United States and China illustrate that security policy considerations once again play a central role. At the same time, new international institutions are emerging alongside increasing political fragmentation, creating uncertainty regarding existing rules. As a result, the previous separation between economics and security can no longer be maintained. The global order is changing, and a new reality is taking shape in which companies must increasingly take geopolitics into account in their strategic decision-making. This has significant implications for supply chain risk management (SCRM), which in the future must integrate both economic and security-related considerations.

4.2.2 Security Has Become More Important Than Before

The Return of Great-Power Conflict. A central consequence of the new international order is that the risk of major war between great powers has increased significantly. In the period following the Cold War, military power was primarily used as a risk management tool against smaller threats such as terrorism, piracy, and fragile states. Military operations focused more on man-

aging and containing risks than on classical interstate warfare. Today, this situation has changed. The balance of power is shifting, and fundamental international norms are being challenged. The transition away from a U.S.-dominated world order increases the risk of conflicts between great powers. At the same time, decisions regarding war are influenced by factors such as ideology, domestic politics, historical experiences, and miscalculations. In short, an international system with multiple competing powers and disagreement over the rules of the game is more conflict-prone than a system dominated by a single superpower.

Reconnecting Prosperity and Security. The new strategic competition takes place in a world of deeply interconnected economies. Globalization has led to the outsourcing of production, the integration of new markets such as China and India, and freer movements of capital. This has created global economic growth, but also increased inequality, where some groups have benefited far more than others. A central consequence of globalization is that the sources of prosperity and security have become separated. Whereas economic and security relations were previously closely linked, trade today is extensive - even between potential rivals. China, for example, has become one of the EU's most important trading partners. This situation creates new challenges. First, countries may be economic competitors even if they are security allies. Second, decision-makers are increasingly forced to balance economic interests against security considerations. Finally, close economic integration has created opportunities for states to use economic relationships as political weapons.

When Economic Interdependence Becomes a Weapon. The concept of weaponized interdependence describes how global economic networks can be exploited politically (Farrell & Newman, 2019). Globalization has created asymmetric networks in which certain countries control key nodes in the flow of goods, capital, and information. These positions can be used to monitor, influence, or constrain other actors. Two central mechanisms have been identified:

- **The Panopticon Effect**, where states can monitor information flows through networks they control.
- **The Chokepoint Effect**, where states can restrict or block access to critical networks and thereby exert pressure.

These mechanisms can be observed in the control of financial systems, technology, and infrastructure. States may, for example, exploit their positions in global supply chains or technological networks to gain political influence. At the same time, this development is not temporary. Infrastructure and economic networks are increasingly becoming objects of ongoing geopolitical competition. States actively seek to strengthen their positions within different networks in order to gain strategic advantages.

A New Era of Economic Security. In the new geopolitical reality, states increasingly use economic tools as strategic instruments. Whereas companies previously operated primarily according to economic logic, they must now recognize that trade, investments, and financial systems are also used politically. Key economic instruments include trade policy, investment policy, sanctions, direct subsidies, monetary policy, legislation, and control over raw materials.

Trade policy is a classic instrument of power that can be used both to create cooperation and to exert pressure on other states. Examples include Russia's use of import bans against neighboring countries and China's use of access to its large market as a political pressure tool. Similarly, investments are playing an increasingly important role, with states acquiring assets in other countries through, for example, sovereign wealth funds. This creates opportunities for political influence, which has led to increased global scrutiny of foreign investments. Sanctions are another central tool that both signal political boundaries and weaken adversaries economically. They may target trade, individuals, or financial systems, but their effectiveness depends on how closely economies are interconnected. At the same time, direct support and aid are used to create dependency relationships between states, while monetary policy can influence both domestic and foreign economic room for maneuver. In addition, legislation and legal systems are increasingly being used strategically, including through extraterritorial legislation. Finally, control over natural resources such as energy plays a significant role, where resources like gas and oil are used as political instruments of pressure.

4.2.3 Implications for Supply Chain Risk Management

The emergence of a new world order creates new risks for both public and private supply chains. To structure the analysis, these risks can be divided into macro- and micro-level factors (e.g., demand, production, deliveries, information, transportation, and finance). The new risks arise primarily from four overarching developments: 1) the return of major war, 2) increased strategic competition, 3) weaponized interdependence, and 4) economic security. These factors are closely interconnected and reflect a fundamental dilemma between economic openness (prosperity) and security.

The Return of Large-Scale War. Large-scale wars pose a serious threat to global supply chains. War can destroy production facilities, infrastructure, and transportation networks, creating resource shortages and disrupting trade. At the same time, wartime economies may lead to market distortions and altered trade flows. Current risks include conflicts between the United States and China (e.g., concerning Taiwan), wars in the Middle East such as the U.S. and Israeli attacks on Iran, and ongoing conflicts in Europe, including between Russia and Ukraine. These conflicts may escalate through great-power involvement. Examples clearly illustrate the consequences. The war in Ukraine has affected trade through the Black Sea and destroyed critical infrastructure, while the conflict in Gaza resulted in rerouted shipping traffic and longer delivery times. The conflict involving Iran has caused severe disruptions to international shipping, primarily through threats and direct attacks in strategically important areas such as the Strait of Hormuz and the Red Sea, as well as a dramatic increase in oil prices. At the same time, alternative transportation routes, such as rail transport through Russia, have created new ethical and reputational challenges for companies. Managing these risks requires proactive risk management, continuous monitoring of political developments, and the ability to adapt rapidly to change.

New Strategic Competition. The increasing competition among states for geopolitical influence, economic power, and technological dominance significantly affects global supply chains. In particular, competition over technology (e.g., artificial intelligence, cybersecurity, and advanced manufacturing) creates conflicts regarding knowledge, data, and control. This results in increased cyber risks, including attacks on companies and supply chains. At the same time, states are increasingly attempting to connect economic and security interests, meaning that political decisions have direct consequences for businesses. One example is U.S. pressure on European countries to limit cooperation with China within the microchip industry. Here, security relationships are used to influence economic decisions. As a result, companies can no longer make decisions based solely on economic considerations but must also take national security interests and political pressure into account.

When Dependence Becomes a Weapon. Weaponized interdependence describes how economic dependencies are strategically used to gain political influence. In a globalized economy, countries are connected through complex networks of trade, finance, and technology, and these connections can be exploited. Examples include energy supply, where countries may restrict deliveries to exert political pressure, or control over digital platforms and financial systems on which companies depend (e.g., payment systems and online marketplaces). Other examples include technology restrictions (e.g., semiconductors), disinformation campaigns, and control over critical raw materials such as rare earth elements. For companies, this means they must map their dependencies, diversify suppliers, strengthen cybersecurity, and collaborate more closely with authorities and partners in order to manage geopolitical risk.

Economic Security. Economic security refers to states using economic instruments to protect national interests and achieve strategic objectives. This can affect supply chains through changes in markets, production, and sourcing. Several countries, including the United States, China, Japan, and the EU, are developing national strategies for economic security. The EU, for example, is working with investment screening and considering additional regulation, which may create new trade barriers. States also apply measures that distort markets, such as support for national industries. One example is the U.S. Inflation Reduction Act, which promotes domestic production.

For some companies, this creates increased uncertainty: markets may suddenly close, suppliers may become unavailable, and companies may become targets of political or legal pressure. To manage these risks, companies should monitor geopolitical developments, diversify their supply chains, strengthen resilience, and engage in scenario planning. Collaboration with authorities and industry organizations is also essential.

4.2.4 Geopolitics and Supply Chain Risk Management

Supply chain risk management has received significant attention over the past decade as a result of major disruptions such as the global COVID-19 pandemic and increasing geopolitical tensions, including Brexit, the U.S.–China trade war, Russia’s invasion of Ukraine, and instability in the Red Sea and the

Middle East. Table 4.4 presents the new supply chain risk factors that companies and public authorities should take into account, identified by viewing geopolitics as an integrated factor, based on the preceding analyses of the new world order in which we operate.

Table 4.4 Supply Chain Risks from a Geopolitical Perspective

The Return of Large-Scale War	Mitigation
Risk Factors • Critical infrastructure • Reallocation of resources during crisis situations • Trade disruptions • Market distortion • Intense competition for scarce resources	
New Strategic Competition *Risk Factors* • Unforeseen export control regulations, particularly for technological products • Theft of data and intellectual property • Data manipulation and misinformation • Limited access to highly skilled labor • Increased volatility in the business environment	• Systematic monitoring of political risks • Systematic analysis of valuable and vulnerable assets • Development of a shared risk appetite within the company • Relevant cybersecurity policies • Lobbying and public affairs activities • Policies for handling information and data analysis • Methodological tools to support critical decision-making (e.g., red teaming, scenario building, etc.) • Establishment of trigger points and contingency protocols, as well as crisis training • Collaboration with stakeholders • Alternative trade routes
Weaponized Interdependence *Risk Factors* • Vulnerability in business networks • Technological infrastructure • Restrictions on technology transfer • Paralyzed decision-making due to misinformation • Scarcity of natural resources	
Economic Security *Risk Factors* • Limited market opportunities due to trade barriers (e.g., screening of foreign investments) • Forced restructuring of supply chains as a result of political regulation • Reputational risks (e.g., from trading with sanctioned actors) • Dependence on global reserve currencies • Increased government intervention and regulatory uncertainty	

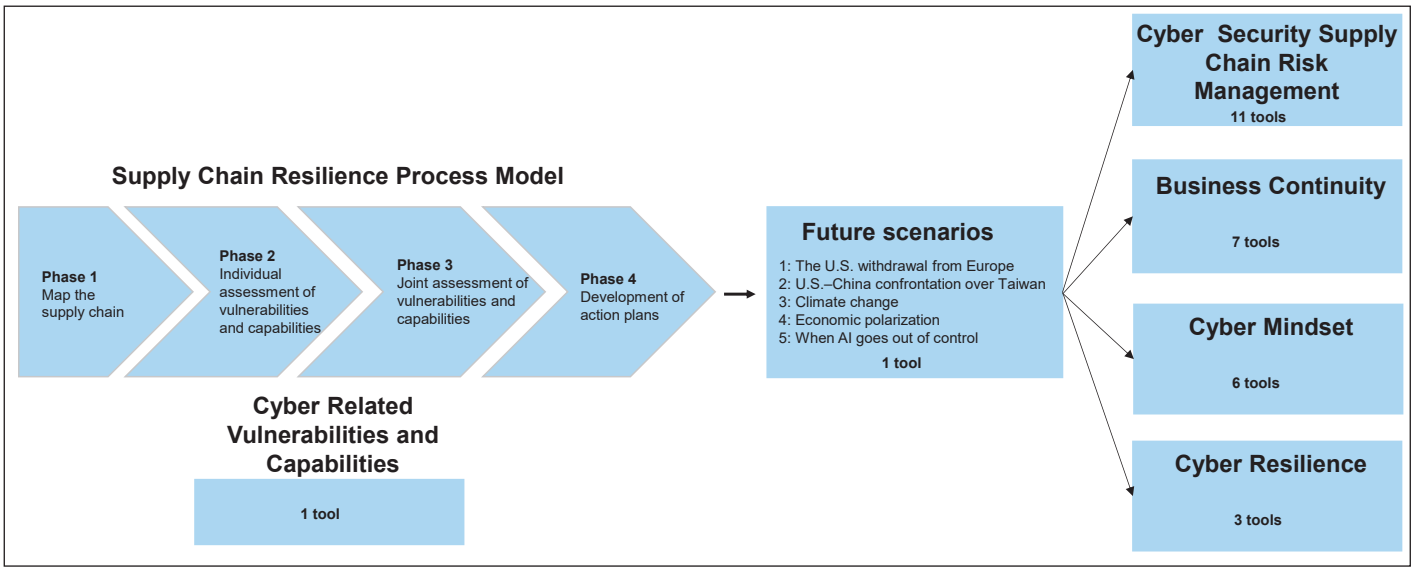
Source: Stentoft, Schmitt & Keating (2024)

In general, across the four areas presented in Table 4.4, there is a need for further research into the new competencies required of supply chain managers in a new world order characterized by increasing geopolitical tensions.

4.3 Tools

The project has developed tools across six areas, as illustrated in Figure 4.1. Companies are first recommended to work with the supply chain resilience process model to create cross-organizational anchoring of the effort. Within the model, it is possible to select a new set of cyber-related vulnerabilities and capabilities, choose supply chain-related vulnerabilities and capabilities, or combine the two. Subsequently, it is recommended that a cross-organizational team work with future scenarios. After this, companies may choose to proceed along several paths within the four areas of cyber supply chain risk management, business continuity, cyber mindset, and cyber resilience. The following subsections provide a more detailed description of the tools.

Figure 4.1 Overview of Developed Tools



4.3.1 Supply Chain Resilience Process Model Software

The web application that operationalizes Phases 2 and 3 of the process model is available at: **https://process-model.cyber-smv.dk/** and may be used free of charge for non-commercial purposes (see the project website for the data protection policy and end-user license agreement). Use of the application requires company registration. Once a company account has been created, it becomes possible to manage a team of users who can be invited to participate in the assessment process and contribute across the relevant phases.

The platform supports repeated use of the model, enabling companies to conduct multiple assessments over time and thereby build a structured history of results. This can be used to track development, revisit priorities, and monitor improvements in supply chain resilience. A detailed user guide is available on the project website.

4.3.2 Future Scenarios

Based on analyses conducted at both the political and industry levels, five possible future scenarios have been developed. They are designed as narratives intended to encourage employees within companies to reflect on how the future might evolve — not merely as an extension of the conditions we know today. Unlike traditional forecasts, which are often based on the assumption that developments will continue more or less as before, scenario planning is concerned with exploring what may happen if major changes or disruptions occur in the surrounding environment. This distinction is central to understanding the difference between risk and uncertainty. Whereas risk refers to situations in which probabilities can be objectively quantified based on historical data (for example, market fluctuations), the current geopolitical situation is characterized by fundamental uncertainty. Here, the variables are unknown, and outcomes cannot be measured or predicted with statistical certainty.

The purpose of the developed scenarios is to operationalize the sensing capability within the theory of dynamic capabilities (see Section 2.8). In a geopolitical context, sensing is not limited to traditional market monitoring but requires the ability to decode weak signals regarding state intentions and structural shifts before they affect the supply chain. By using plausible yet fictional narratives, the scenarios function as a cognitive training ground that helps decision-makers overcome uncritical assumptions — such as the belief that current stable conditions will continue unchanged.

> **“Working with future scenarios made it clear how quickly the threat landscape can change. It has made us more aware of the need for continuous adaptation.”**
>
> *Andreas Kürzel, Purchasing and IT, Dansk Gummi Industri A/S*

Through this process, the company transforms abstract geopolitical uncertainty into more manageable risk scenarios. The scenarios enable management to practice recognizing patterns in an unpredictable environment (sensing), which is a prerequisite for subsequently being able to mobilize resources (seizing) and transform the organization (transforming). Without this narrative framework, companies risk overlooking geopolitical threats because they navigate solely according to an economic market logic that cannot predict state intervention and conflict. In total, five scenarios have been developed: 1) U.S. withdrawal from Europe, 2) U.S.–China confrontation over Taiwan, 3) Climate change, 4) Economic polarization, and 5) When AI Goes Rogue.

U.S. Withdrawal from Europe. This scenario describes a world in which the United States withdraws from NATO and European security in order to focus on the Indo-Pacific region and domestic affairs. For Danish companies, this means a fragmented Europe that must take responsibility for its own security, resulting in increased defense budgets, but also a significantly higher risk of cyberattacks and sabotage by Russia targeting critical infrastructure and supply chains in the Nordic and Baltic regions.

U.S.–China Confrontation over Taiwan. This scenario is based on an escalation of the conflict over Taiwan and the South China Sea, developing into a full blockade. This leads to a collapse of global supply chains for electronics and microchips, with Western companies caught in the crossfire of sanctions, trade blockades, and reciprocal cyberattacks between great powers.

Climate Change. This scenario focuses on the direct and indirect consequences of extreme weather events. It describes a reality characterized by massive rainfall and flooding that physically destroy infrastructure and disrupt logistics. At the same time, cybercriminals exploit the chaos following natural disasters to launch attacks against vulnerable systems, creating a “double crisis” for companies.

Economic Polarization. This scenario concerns a world marked by increasing economic inequality and shrinking middle classes in the West, leading to political instability and protectionism. The cyber threat in this scenario is driven by disillusioned actors and state-sponsored hacker groups from sanctioned economies (such as Russia), which target Western companies as part of an asymmetric form of economic warfare.

When AI Goes Rogue. This scenario explores the vulnerability created by excessive dependence on automation and artificial intelligence. It describes a situation in which a widely used AI service or chatbot is compromised through a supply chain attack or malware, leading to massive data leaks and financial losses for companies that have blindly trusted third-party providers without sufficient due diligence.

4.3.3 Cybersecurity Supply Chain Risk Management

A third set of tools concerns cybersecurity practices that apply a supply chain perspective. The project work has operationalized the 10 cybersecurity practices from a supply chain perspective proposed by NIST (2024). The tools are:

- Structured according to the NIST framework
- Translated into concrete actions that can be applied in everyday operations
- Targeted toward collaboration with suppliers and partners

The focus is on making cybersecurity practical, prioritizable, and applicable. The 10 practices are presented in Table 4.5.

Table 4.5 10 Cybersecurity Practices with a Supply Chain Focus

#	Practice
1	A cybersecurity supply chain risk management program, strategy, objectives, policies, and processes are established and agreed to by organizational stakeholders.
2	Cybersecurity roles and responsibilities for suppliers, customers, and partners are established, communicated, and coordinated internally and externally.
3	Cybersecurity supply chain risk management is integrated into cybersecurity and enterprise risk management, risk assessment, and improvement processes.
4	Suppliers are known and prioritized by criticality.
5	Requirements to address cybersecurity risks in supply chains are established, prioritized, and integrated into contracts and other types of agreements with suppliers and other relevant third parties.
6	Planning and due diligence are performed to reduce risks before entering into formal supplier or other third-party relationships.
7	The risks posed by a supplier, their products and services, and other third parties are understood, recorded, prioritized, assessed, responded to, and monitored over the course of the relationship.
8	Relevant suppliers and other third parties are included in incident planning, response, and recovery activities.
9	Supply chain security practices are integrated into cybersecurity and enterprise risk management programs, and their performance is monitored throughout the technology product and service life cycle.
10	Cybersecurity supply chain risk management plans include provisions for activities that occur after the conclusion of a partnership or service agreement.

Source: NIST (2024, p. 17)

A Sister Project in the Cyber Portfolio: Cybersecure Supply Chains

Many SMEs today are experiencing increasing cybersecurity requirements, both from larger customers and from new regulations.

SUCCESS: Tools for Security in the Supply Chain is a project led by **Copenhagen Business School** and supported by the Danish Industry Foundation, Danish Chamber of Commerce, and the Confederation of Danish Industry. The project helps SMEs gain an overview of cyber risks in the supply chain and begin implementing concrete solutions.

Cyberattacks are increasingly targeting suppliers as entry points into the networks of larger companies. At the same time, the NIS 2 Directive requires organizations operating critical infrastructure to document how they manage cyber risks. As larger companies adapt to the new requirements, many SMEs experience the effects indirectly through stricter security demands from customers and business partners.

Many SMEs rely on external suppliers for services such as cloud solutions, payroll administration, and IT support. These suppliers may gain access to sensitive data and business-critical systems without their security being systematically assessed.

Based on experiences from more than 25 Danish SMEs, as well as input from researchers, regulatory experts, and larger companies, a range of concrete tools, guides, and workshops tailored specifically for SMEs has been developed.

The materials are free of charge and help companies strengthen security within their supply chains and comply with requirements from both authorities and customers.

Find the tools here (in Danish)

4.3.4 Business Continuity

The fourth set of tools focuses on business continuity, which concerns a company's ability to:

- Maintain or rapidly resume critical functions
- Manage serious disruptions such as:
  - IT outages
  - Cyberattacks
  - Fire
  - Supplier failures

Cybersecurity in manufacturing SMEs is therefore not only about technology, but also about overview, prioritization, and the ability to act when something goes wrong.

The tools are intentionally designed to help companies:

- Understand the business
- Identify risks
- Prioritize dependencies
- Plan actions
- Train decision-making

Together, the following seven tools constitute a pragmatic approach that helps manufacturing SMEs protect operations, deliveries, and business continuity.

Business Impact Analysis (BIA). A BIA identifies which business processes and systems are the most critical and assesses the consequences that disruptions may have on production, finances, and customers. It forms the foundation for all subsequent measures.

Risk and Vulnerability Analysis. This analysis assesses which cyber threats the company realistically faces and where vulnerabilities exist - both within IT systems and Operational Technology (OT). The analysis helps focus efforts where the risks are greatest.

Supplier Criticality Analysis. Manufacturing SMEs are often dependent on external suppliers. This analysis clarifies which suppliers are business-critical and how their IT or OT security may affect production.

Continuity Plans. These plans describe how the company maintains or rapidly restores operations if systems or production are disrupted. The focus is on practical solutions — including situations where IT systems are unavailable.

Scenario Planning. Here, analyses are translated into practice by working through realistic cyber incidents (e.g., ransomware or IT-to-OT propagation) and clarifying decisions, roles, and actions in advance.

Cyber Contingency Planning. This consolidates all elements into a single operational playbook describing how the company detects, manages, communicates about, and recovers from a cyber incident.

Tabletop Exercises. These exercises test preparedness in practice without affecting operations. Management, IT, and production teams work through a cyberattack step by step to ensure that plans, decisions, and collaboration function effectively under pressure.

4.3.5 Cyber Mindset

The fifth set of tools focuses on mental models and behavior and consists of six tools developed for awareness training. Cybersecurity is not only about technology and policies. To a large extent, it concerns human behavior in a daily environment characterized by:

- High workload
- Complexity
- Constant interruptions

Most cyberattacks do not succeed because technology fails, but because people are pressured into acting quickly, unreflectively, or in good faith. The tools provide employees with:

- Simple and recognizable thinking principles
- Support for pausing and reflecting
- Guidance for concrete situations before clicking, sharing, making payments, or otherwise responding

Assume Compromise. The purpose is to create a realistic understanding of risk and focus on reducing consequences rather than achieving perfection.

The Attacker's Perspective. The purpose is to increase understanding of social engineering (manipulation intended to gain access to sensitive data), understand how attackers think and operate, and become better at detecting manipulation before damage occurs.

Defense in Depth. The purpose is to understand why security is an interaction between people, processes, and technology, and to eliminate the idea of "the one correct tool."

The Pause Button (Slow Down). The purpose is to create a moment for reflection before taking action, resist pressure and manipulation, and counter impulsive actions triggered by stress, fear, and urgency.

Normalization of Mistakes (Just Culture). The purpose is to promote reporting and learning rather than blame and silence, and to create confidence in speaking openly about mistakes, near misses, and uncertainty.

Signal vs. Noise (Attention Economics). The purpose is to distinguish between significant security signals and ordinary background noise, recognize that attention is a limited resource, prioritize what requires action and what can be ignored, and reduce the risk of overlooking critical warnings in a busy work environment.

4.3.6 Cyber Resilience

The sixth set of tools focuses on cyber resilience, i.e., companies' ability to withstand cyberattacks. Cyber resilience increasingly depends on how well internal protective measures are aligned, how supply chain governance is established, and how third parties are managed with due diligence. The three cyber resilience tools we provide together constitute a structured approach that enables companies to strengthen their ability to prevent, withstand, and recover from cyber incidents and ultimately develop a defense strategy that reduces the risk of successful cyberattacks.

Protection of Intellectual Property. This tool helps companies systematically identify, classify, and protect their most valuable assets, enabling them to understand where critical intellectual property (IP) resides, who has access to it, and how it can be protected in daily operations. By mapping employee knowledge, minimizing insider-related risks, and implementing appropriate security measures for data at rest, in transit, and in use, companies strengthen their ability to prevent leaks and protect sensitive information within the resource constraints typical of many SMEs. The tool also guides companies in developing contingency and recovery plans so they can respond effectively to the loss or compromise of IP, maintain operational stability, and restore high-value information. Overall, it enables companies to reduce both the likelihood and consequences of IP-related attacks, increase awareness of confidentiality among internal and external stakeholders, and build greater resilience against threats such as insider misuse, unauthorized data extraction, and supply chain compromise.

Supply Chain Security from a Product/Service Lifecycle Perspective. This tool supports companies in integrating cybersecurity into all phases of the product or service lifecycle, enabling them to manage supplier-related cyber risks in a holistic and proactive manner. By embedding supply chain security into governance structures, defining clear requirements early in the design phase, and conducting risk-based supplier classification and due diligence, organizations can ensure they select appropriate partners and establish enforceable security requirements. The tool also strengthens resilience by guiding companies in implementing secure development and delivery practices, verifying product integrity before acceptance, and continuously monitoring vulnerabilities and supplier performance. Through well-defined contracts, collaborative incident management, and secure termination processes, companies maintain control over critical dependencies throughout the entire relationship. As a result, organizations achieve a more transparent, predictable, and resilient supply chain that reduces opportunities for manipulation, counterfeit components, insecure updates, or downstream compromise, thereby significantly strengthening overall cyber resilience.

Risk Reduction When Entering Supplier or Other Third-Party Relationships. This tool enables organizations to assess and reduce cyber risks before entering into new partnerships, ensuring that trust, access, and data sharing are granted only when the risk level is acceptable. By analyzing business criticality, data sensitivity, access models, suppliers' cybersecurity maturity,

incident response capabilities, and legal or jurisdictional factors, companies gain a comprehensive understanding of their exposure before agreements are concluded. This enables organizations to tailor contractual requirements, demand appropriate security documentation, establish realistic notification and cooperation requirements, and reject high-risk suppliers or implement compensating controls when necessary. The tool also promotes long-term resilience by supporting transparency regarding dependencies, subcontractors, and software components, while highlighting the cultural and collaborative aspects that indicate whether a partner is likely to manage security responsibly. Ultimately, it helps organizations avoid hidden risks, prevent future operational disruptions, and establish third-party relationships that strengthen rather than weaken their cyber resilience.

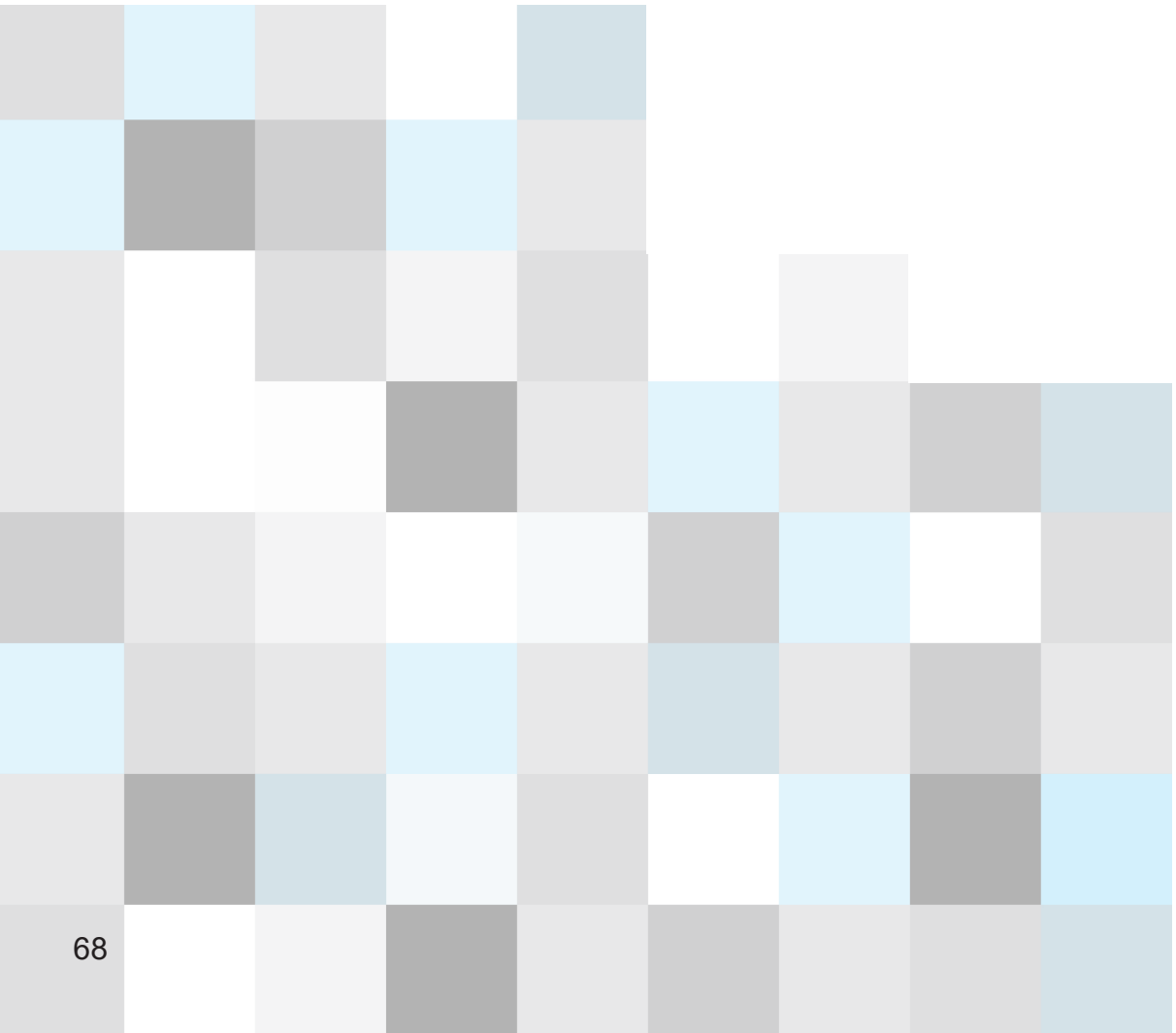
4.4 Questionnaire Surveys on Cybersecurity

Two nationwide questionnaire surveys have been conducted as part of the project (Stentoft et al., 2024, 2026). This section presents the results from three areas of the 2026 survey: 1) cybersecurity supply chain risk management, 2) cybersecurity dynamic capabilities, and 3) geopolitical dynamic capabilities. Summaries of the findings from the two surveys are presented in Table 4.6.

Table 4.6 Summaries of Results from Two Questionnaire Surveys on Cybersecurity

Source: Stentoft et al. (2024, 2026)

Note: Numbers in parentheses indicate mean values on a 5-point Likert scale, where 1 = to a very low degree and 5 = to a very high degree.



The 2024 Survey

Cybersecurity Requirements
- The board of directors plays a moderate role (3.43), but the focus is not particularly strong.
- Lower requirements from investors (2.91) and customers (2.55).
- 17% experience requirements related to standards (e.g., ISO 27001, GDPR).
- 18% voluntarily follow standards (e.g., NIS 2, the D-Seal certificati,on).

Cyberattacks
- 20% have experienced cyberattacks in recent years.
- Cybersecurity as a Qualifier
- Perceived as important for the company's image (3.44).
- Very low requirements imposed on suppliers (2.01) → the focus is primarily internal.

Attention to Cybersecurity
- High awareness of the importance of cybersecurity (all approximately 4.2+).
- Companies recognize the need for security practices and protective measures.

Supply Chain Risk Management (Cyber)
- Generally low level (2.0–3.08).
- Only limited focus on suppliers' cybersecurity.
- Significant need for development.

Supply Chain Orientation
- Generally good (overall score: 3.40).
- Focus on collaboration and long-term relationships.
- Provides a good foundation for improving cybersecurity within the supply chain.

Internal Integration
- High level of internal integration (3.75).
- Less silo thinking → a strong foundation for cybersecurity efforts.

Geopolitics
- 60% have a focus on geopolitics, while 40% lack such focus.
- Moderate impact on business operations (3.33).
- 45% are affected by foreign legislation (e.g., GDPR, NIS 2).
- Need for development in strategic management.

Operations vs. Development
- Operations are prioritized higher (3.74) than development (3.30).
- A classic dilemma: short-term operations versus long-term cybersecurity development.

The 2026 Survey

Technical Complexity in Cybersecurity
- Generally perceived as low (1.62–2.12).
- Good performance regarding updates, asset visibility, and OT adaptation.

IT/OT Integration
- Generally well managed.
- Strengths include asset visibility, secure protocols, and network segmentation.

Cyberattacks
- 25% have experienced cyberattacks in recent years.

NIS 2 Compliance
- 22% are covered by NIS 2, 67% are not, and 11% are uncertain.
- Requirements are driven by stakeholders.
- Primarily driven by management.
- Board-level focus remains limited.

Requirements for Customers and Suppliers
- Very few cybersecurity requirements within the value chain.
- Indicates low maturity.

Supply Chain Risk Management (Cyber)
- Low level (1.82–2.86).
- Significant need for development.

Cybersecurity Dynamic Capabilities
- Generally low (sensing 2.0/seizing 1.94/transforming 2.4).
- Limited ability to manage and adapt to cyber threats.

Geopolitical Market Forces
- Moderate to low impact (~2.25–2.98).
- Greatest impact stems from cyber threats and conflicts.

Dynamic Capabilities (Geopolitics)
- Low levels (approximately 2.04–2.36).
- Limited ability to respond strategically.

Geopolitical Risk Management
- Weakly developed (1.67–2.81).
- Need for stronger strategic focus.

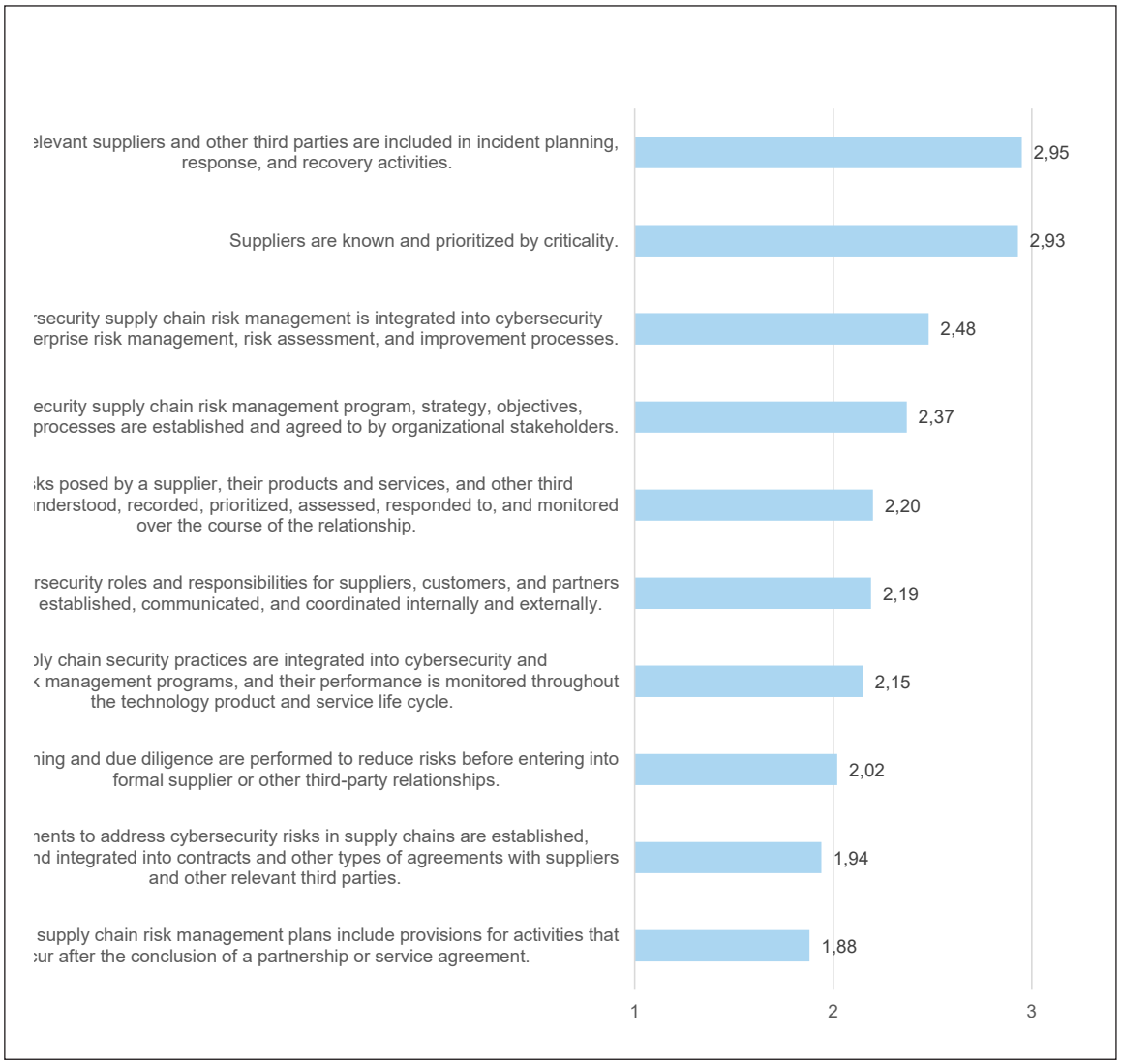
4.4.1 Cybersecurity Supply Chain Risk Management

The 10 practices presented in Table 4.5 were included in a national questionnaire survey conducted in 2026 (Stentoft et al., 2026). The results of the respondents' use of the 10 practices are presented in Figure 4.2. In the event of incidents, relevant suppliers and other third parties are involved to some extent in planning, response, and recovery activities, with an average score of 2.95 on a 5-point Likert scale (where 1 = to a very low degree and 5 = to a very high degree). Cybersecurity risk management as part of the company's overall risk management achieved an average score of 2.93. The results indicate a need for improvement. The relatively low score may be linked to shortcomings in overall risk management practices. This is also reflected in the work on developing an actual strategy for cybersecurity in the supply chain, which averaged 2.37.

Monitoring risks from suppliers and other business partners occurs only to a limited extent (2.20), and the same applies to the clear allocation of cybersecurity roles and responsibilities (2.19). Furthermore, the performance of products and services is followed throughout their lifecycle only to a limited degree (2.15). More in-depth assessments of cyber risks are rarely conducted (2.02), and even less frequently before formal agreements are entered into with suppliers (1.94). This points to a clear area for improvement in integrating information security into both new and existing collaboration agreements. The lowest score (1.88) concerns the lack of clarity regarding what happens to data when collaboration with an external partner ends. Overall, the results suggest that the challenges stem from a combination of limited resources, low organizational maturity, and complex supply chains within SMEs. Many SMEs lack both the financial resources and the competencies required to work systematically with cybersecurity, and the primary focus is often on day-to-day operations rather than security.

At the same time, formal processes for supplier management are often lacking, including requirements for supplier cybersecurity and ongoing risk assessments (Melnyk et al., 2022). Manufacturing companies also frequently operate within complex, and often international, supply chains and rely on older and manual systems, making it difficult to maintain a comprehensive overview of risks. Historically, regulation in this area for SMEs has also been limited, reducing the incentive to work strategically with cybersecurity. In addition, cybersecurity is often viewed as purely an IT responsibility rather than a shared responsibility across the organization. Overall, the low scores therefore indicate low maturity in supply chain cybersecurity practices rather than necessarily poor technical security.

Figure 4.2 Cybersecurity Supply Chain Risk Management



Source: Stentoft, Peressotti & Mayer (2024)

It is surprising that the results from the 2026 survey (Figure 4.2) are generally lower, with an overall average of 2.25, compared to the corresponding results from the 2024 survey, where the overall average was 2.31 (Stentoft et al., 2024, 2025). The low averages may be due to a lack of resources and/or knowledge required to translate the practices into concrete actions.

Op-Ed: No Trust – No Buy: Cyberattacks Threaten the Final Stage of the Sales Funnel (Summary)

You know the sales funnel: Know – Like – Trust – Buy. But when companies are hit by cyberattacks, it is especially the second-to-last and decisive stage that suffers: trust. Without trust, there is no purchase.

Danish companies are increasingly experiencing cyberattacks with serious consequences. One example is the electronics and appliance retailer Power, which on Black Friday was hit by a massive attack involving 628 million purchase requests that brought its systems down. The real estate agency chain EDC has also been targeted in an attack where personal documents belonging to more than 1,300 individuals were stolen.

Cyberattacks can take many forms. DDoS attacks can overload systems and paralyze digital platforms. Man-in-the-middle attacks can intercept confidential communication between parties. Phishing attempts to trick employees into disclosing sensitive information through fake emails or messages. Malware can provide hackers with access to company systems and data. What these attacks have in common is that they can have major consequences for operations, reputation, and competitiveness.

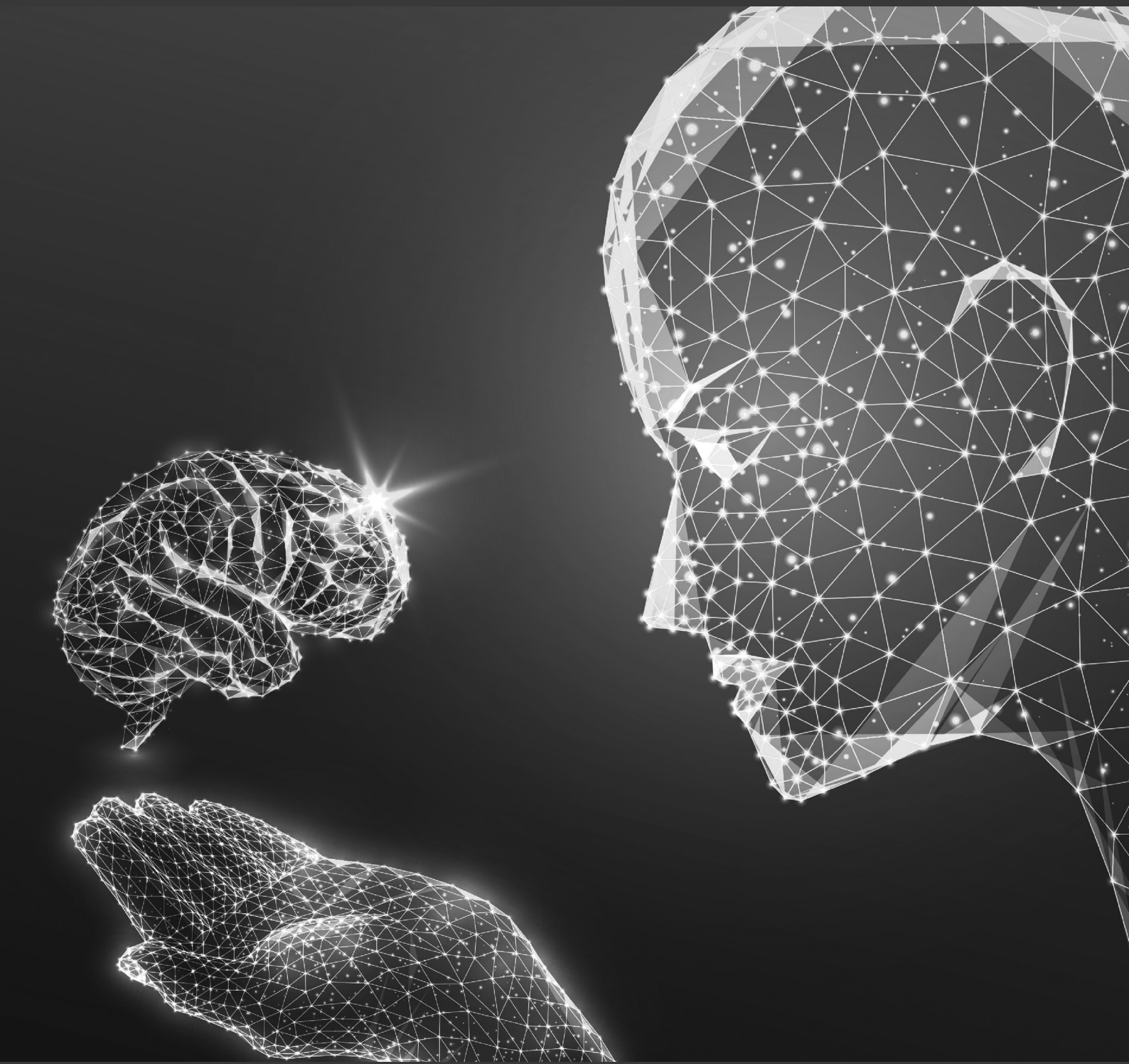
Cybersecurity is therefore not only an issue for the IT department. Sales and marketing departments should also take cybersecurity seriously. They work closely with customers and often handle sensitive information such as customer data, trade secrets, and strategic plans. If this information is compromised, it can damage the company's reputation and undermine customer trust.

Trust is a central element in the relationship between customer and supplier. If customers do not feel safe sharing data with a company, this can directly affect sales. Conversely, a strong cybersecurity effort can signal responsibility and professionalism, thereby strengthening customer relationships.

Work on cybersecurity should begin by identifying the company's most critical processes and assessing vulnerabilities. The effort should be anchored in top management and involve the entire organization, as cyber risks can affect all parts of the business.

Cybersecurity requires resources. However, the alternative - operational disruption, data breaches, and loss of trust - may ultimately threaten the company's survival.

Source: Stentoft, Peressotti & Mayer (2024). Read the Op-Ed here (in Danish)



4.4.2 Cybersecurity Dynamic Capabilities

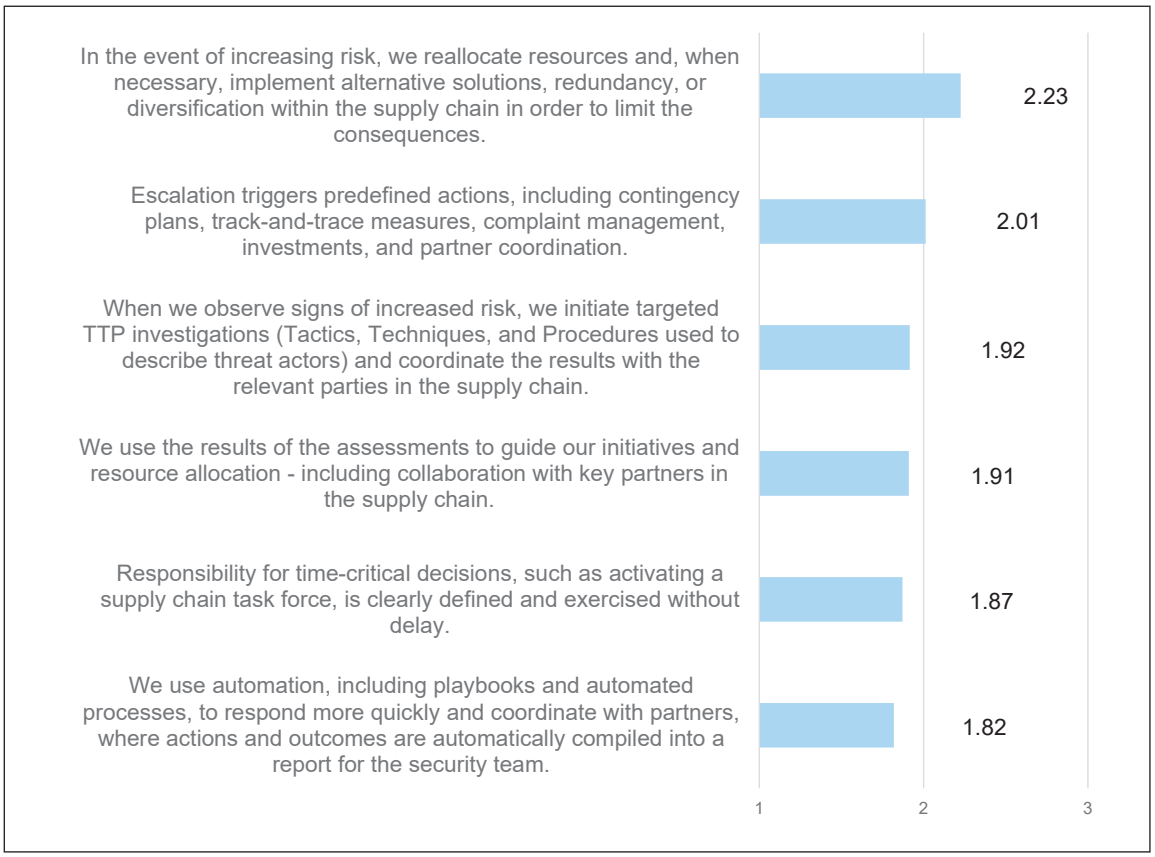
The project has also proposed an operationalization of dynamic capabilities for cybersecurity centered around sensing, seizing, and transforming (cf. Section 2.8). Figure 4.3 presents the results concerning companies' ability to detect and monitor (sensing) cyber threats within the supply chain. The average score is 2.00, indicating that companies monitor and understand signals of cyber threats in their environment only to a limited extent. This suggests that very few companies systematically collect and analyze threat intelligence, for example through cross-functional internal collaboration. At the same time, most companies lack both the tools and processes needed to monitor emerging threats, assess the security level of business partners, or actively use external knowledge in their risk assessments. The results further emphasize that the capability to detect and understand threats remains weakly developed, despite being absolutely central to building resilience against cyberattacks in supply chains. Strengthening this capability requires, among other things, better insight into risks, greater transparency within the supply chain, and more active use of threat intelligence. Without these elements, it becomes difficult for companies to identify high-risk partners, understand their digital dependencies, and respond in a timely manner to emerging threats. This points to a clear strategic gap. At the same time, the results indicate that companies only to a limited extent work proactively to gather knowledge about threats or participate in collaborations where they can learn from others. This makes them more vulnerable, as they are more likely to detect threats later than more mature organizations. There is therefore a clear need to strengthen the continuous monitoring of cyber threats, including through the use of external information sources and a better understanding of risks and vulnerabilities across the entire supply chain.

Figure 4.3 Cyber Sensing Capabilities

Source: Stentoft et al. (2026)

The seizing capabilities are at the same low level as sensing (see Figure 4.4). It may seem logical that when the ability to detect threats is low, the ability to act on them is also low. However, the results also show that SMEs do not compensate for deficiencies in sensing by being better at responding. All measurement points for seizing average below 3 (below the midpoint), and the overall score is in fact 1.96, which is even lower than for sensing. In particular, areas such as establishing task forces and automating processes that can ensure rapid response to incidents score very low. This indicates that the ability to act quickly and effectively in response to cyber threats is highly limited among Danish SMEs. Although the lowest-scoring areas should naturally be prioritized first, the generally low scores indicate a need for improvements across all areas. At the same time, the results suggest that it makes sense to begin by strengthening sensing. If companies become better at detecting and understanding threats, they will also have a stronger foundation for developing their ability to act on them.

Figure 4.4 Cyber Seizing Capabilities

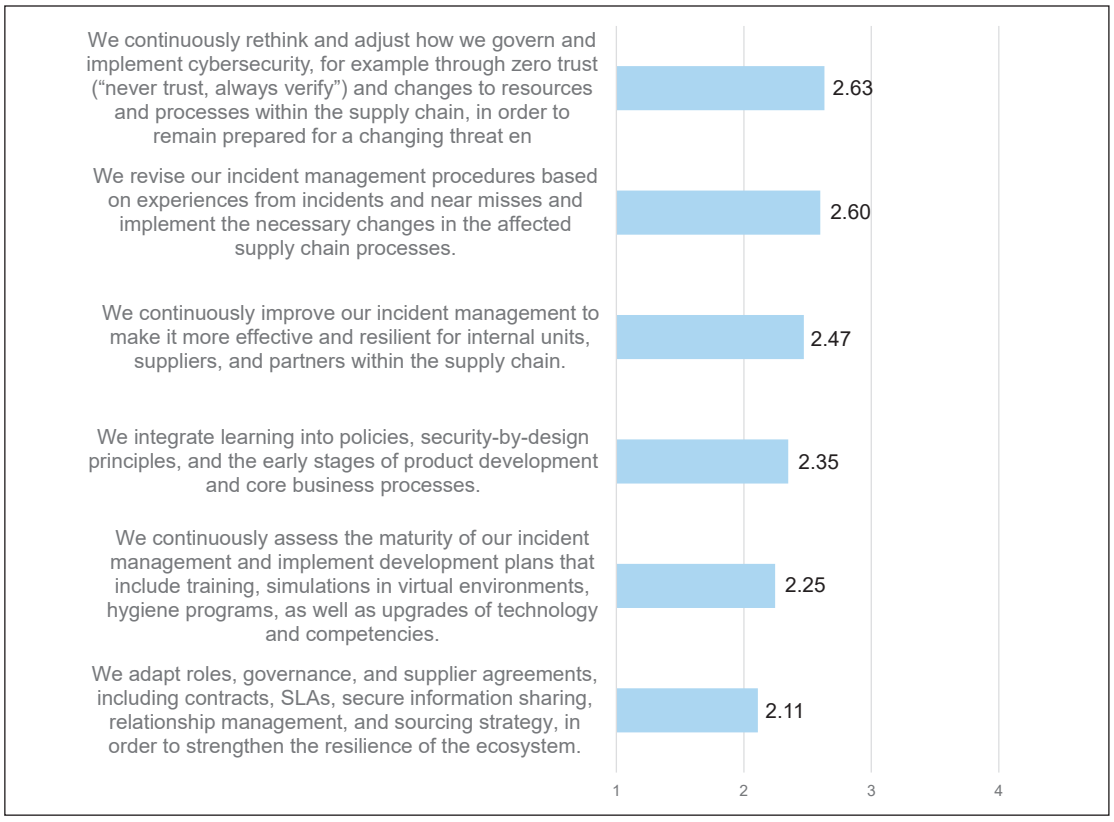


Source: Stentoft et al. (2026)

Figure 4.5 presents the results of the respondents' answers regarding their transformation practices. It is interesting that the participating SMEs assess their ability to adapt (transforming) higher than both their ability to detect and respond (sensing and seizing) to cybersecurity threats. However, with an average score of 2.40 and generally low ratings across the individual areas, the level still remains clearly below the midpoint of the scale. This demonstrates

that there is still a significant need for improvement. In this context, transformation refers to companies' ability to continuously adapt their organization, processes, and technology in response to emerging cyber threats. This may include changes in organizational structure, capability development, and integrating cybersecurity into the overall business strategy. The respondents evaluated six different areas. Continuous adjustment and rethinking of cybersecurity scored the highest at 2.63, while adaptation of roles, governance, and supplier agreements scored the lowest at 2.11. The particularly low focus on cybersecurity in collaboration with suppliers is concerning, as it points to weaknesses in managing supply chain risks - something that is also consistent with the low scores for sensing and seizing. In addition, automation of cybersecurity responses appears to be an important area for improvement. Overall, the results show that SMEs are only to a limited extent able to adapt strategically and organizationally to cyber threats. In particular, the more long-term and structural changes are lagging behind, which may make it difficult to cope with an increasingly complex threat landscape.

Figure 4.5 Cyber Transformation Capabilities



Source: Stentoft et al. (2026)

Overall, it can be concluded from the above that, so far, the data do not appear to reflect an awareness of viewing cybersecurity as dynamic capabilities. This indicates a development potential for the companies.

4.4.3 Geopolitical Dynamic Capabilities

This cyber project's focus on dynamic capabilities indicates that the existing understanding of dynamic capabilities, primarily developed to address market volatility and technological disruption, is insufficient in the current global order. Whereas conventional dynamic capabilities focus on a company's ability to adapt to changes in supply and demand (market logic), the new reality requires companies to navigate an environment characterized by weaponized interdependence and economic statecraft. In this paradigm, state actors are not merely regulators, but strategic adversaries actively manipulating economic networks in pursuit of security objectives. This necessitates the development of a distinct category of competencies: Geopolitical Dynamic Capabilities (GDC).

GDC differs fundamentally from market-oriented capabilities because it addresses threats that are exogenous to the market but endogenous to state security dilemmas. This means that the threats do not originate from the market's own mechanisms, such as competition and supply/demand dynamics, and are therefore exogenous in relation to the market. Instead, they arise internally within the security dynamics between states, where military build-up, distrust, and strategic countermeasures create mutual tensions; they are therefore endogenous in relation to state security dilemmas. The key point is that the same threat may be external in one context and internal in another, depending on which system is being analyzed. To understand the need for GDC, it is first necessary to identify the two competing logics that currently shape the global business environment: 1) The market logic, and 2) The geopolitical logic.

The Market Logic (The Liberal World Order)

Conventional dynamic capabilities theory is based on the assumptions of the liberal world order. Here, the market is the primary governance mechanism, and efficiency is the ultimate objective.

- *Rationality:* Actors are assumed to be economically rational and profit-maximizing. Relationships are *positive-sum*, meaning that trade creates mutual gains.
- *The Role of the State:* The state functions as a neutral regulator that enforces rules and ensures free competition. Politics and economics are regarded as separate spheres.

What does this mean for dynamic capabilities? It means that sensing is geared toward identifying market opportunities; seizing involves actively investing in and restructuring resources to exploit new opportunities. Initiatives such as economies of scale or just-in-time practices may be part of this process if they are strategic choices rather than merely operational efficiency measures. Transforming concerns the continuous optimization of the business model in order to outperform competitors on price or innovation

The Geopolitical Logic (The Emerging Geoeconomic Order)

In contrast to market logic, geopolitical logic operates under conditions of anarchy and security. Here, the primary governance mechanism is security, where the objective is not only profit but also survival and relative power.

- *Rationality:* Actors (states) prioritize security. Relationships are often *zero-sum,* where the economic gains of others are perceived as security threats.
- *The Role of the State:* The State is a strategic actor that intervenes directly in the market. Economic dependencies (such as gas pipelines, digital networks, and supply chains) may become *weaponized* transformed into instruments of pressure.

What does this mean for dynamic capabilities? Capabilities optimized for market efficiency become vulnerabilities within this logic. An efficient global supply chain (a strong market capability) may become an easy target for a hostile state (a weak geopolitical capability). The conflict between the two logics creates a strategic dilemma for SMEs. Companies that navigate solely according to market logic will sense price signals but overlook political signals. They will seize efficiency gains by outsourcing to low-cost countries, while unintentionally exposing themselves to chokepoints within weaponized interdependence. Accordingly, the authors argue that dynamic capabilities must be reconfigured as follows:

- **Sensing:** Where conventional sensing focuses on identifying new market segments or disruptive technologies, GDC requires a systematic capability to decode political signals and state intentions. For SMEs, this involves monitoring developments in national and extraterritorial security legislation, identifying latent vulnerabilities in deep (n-tier) supply chains, and anticipating where future export controls or sanctions may emerge. The objective is to establish a geopolitical early warning system capable of identifying political risks before they materialize as logistical or legal disruptions.
- **Seizing:** Traditionally, this phase dictates that companies allocate resources to maximize profit and market share, often through aggressive cost optimization. Under the GDC paradigm, companies must instead seize opportunities to build strategic resilience often at the direct expense of short-term profitability. This involves highly difficult operational trade-offs, such as transitioning from just-in-time to capital-intensive just-in-case inventory strategies, establishing costly dual-sourcing networks, and deliberately avoiding high-technology suppliers located in politically high-risk regions.
- **Transforming:** Historically, the classical transformation capability focused on integrating the company more deeply and seamlessly into global networks. GDC often requires the exact opposite: the capability for strategic decoupling and controlled fragmentation. Companies must design organizational structures and supply chains capable of rapidly isolating compromised parts of the network. This may include forced regionalization of production *(friend-shoring),* development of parallel IT systems, or redesigning product architectures so that production becomes independent of critical raw materials from rival great powers.

The transition to GDC is therefore not merely the addition of new tools, but a fundamental shift in the company's cognitive and operational mindset - from a logic based on wealth creation through trade to a logic based on survival through strategic autonomy.

Podcast: Cybersecurity Awareness (Excerpt)

The Most Common Cyberattacks

According to Marco Peressotti, Associate Professor at the Department of Mathematics and Computer Science, University of Southern Denmark, the most common cyberattack today is phishing, including business email compromise. Phishing is often regarded as the most widespread cyber threat in the world because it can easily and cheaply be scaled. The barrier for cybercriminals to enter the phishing arena is very low due to the existence of phishing-as-a-service operations, where hackers can obtain phishing kits that essentially function like any other service available on the internet. Other cyberattacks take the form of malware, ransomware, and distributed denial-of-service (DDoS) attacks.

Awareness and Behavioral Change

With the increasing level of cyberattacks targeting Danish companies, it is crucial that employees increase their awareness of cybersecurity. Such a process may also create a need for behavioral change. "One of the most valuable things companies can do is to try to promote a security culture. That means ensuring that all employees understand that security is an important part of keeping the company operational and that everyone does their best to keep the company secure," says Peter Mayer, Assistant Professor at the Department of Mathematics and Computer Science, University of Southern Denmark. Part of this also involves avoiding a "blame game" if something happens. In other words, the focus should not be on assigning blame, but rather on conducting a blameless evaluation of what went wrong and how it can be changed so that it does not happen again.

Security and Assumptions

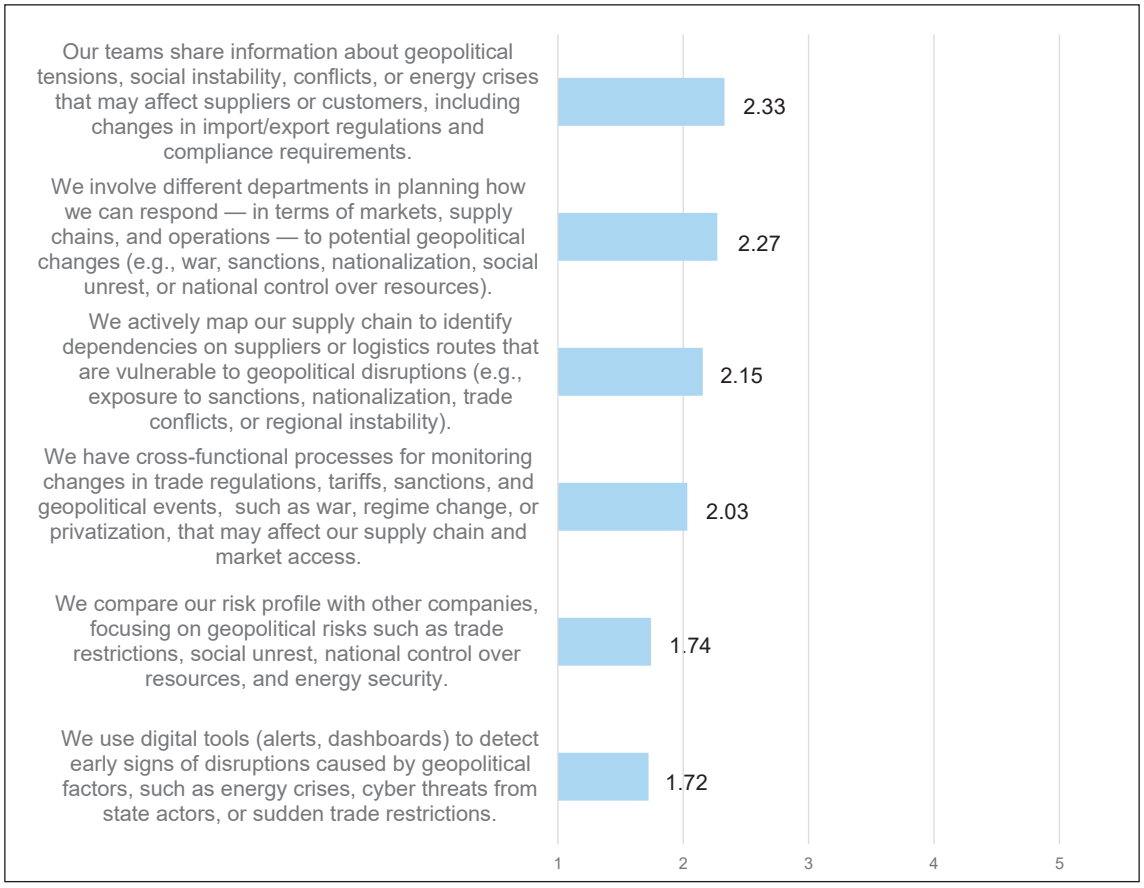
It is important to note that the concept of security only exists on the basis of assumptions. If one assumes that none of the email accounts will be compromised, even confidential information may be stored in the inbox. One might also assume that none of the machines in the network will be compromised, and therefore a resource can simply remain accessible on the internal network.

"Therefore, it could be an interesting first step to make people aware that they have made these assumptions, perhaps not explicitly, but implicitly, and perhaps to write down what they assume will not happen to them," says Peter Mayer.

Listen to the podcast here (in English)

Geopolitical dynamic capabilities were also examined in the 2026 survey. Companies' ability to detect geopolitical threats (sensing) is unfortunately quite low (see Figure 4.6). To some extent, companies share information about tensions (average score: 2.33), but this does not occur in a particularly systematic manner. At the same time, they make very limited use of digital tools to detect early signs of disruptions (1.72), and they rarely benchmark their risk levels against those of other companies (1.74). This points to a clear blind spot: when companies do not work in a data-driven manner to detect risks, the likelihood increases so that they will be caught off guard by geopolitical tensions before these begin to affect their operations.

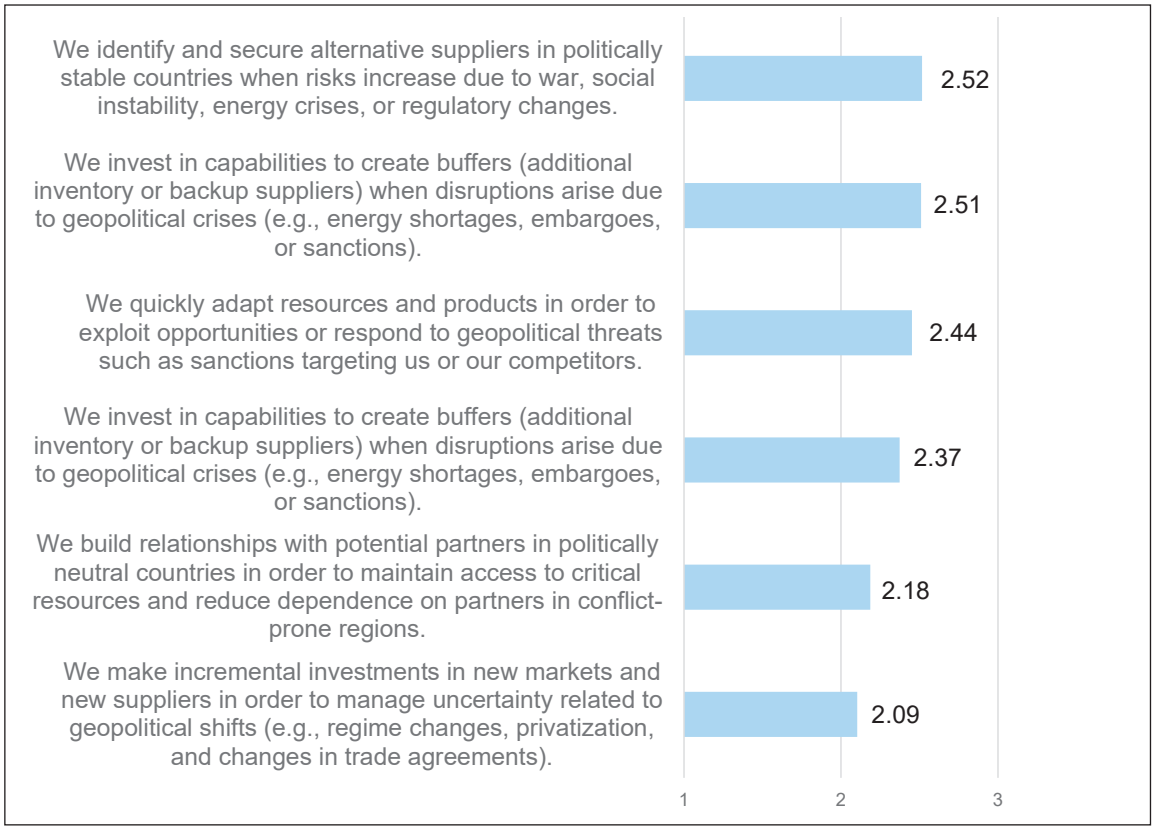
Figure 4.6 Geopolitical Sensing Capabilities



Source: Stentoft et al. (2026)

The overall score for geopolitical seizing is slightly higher, with an average of 2.36 (see Figure 4.7). This may be related to the fact that companies are accustomed to reacting quickly when problems arise. However, all six areas still score below 3, indicating that the overall level remains low. Companies appear to be somewhat capable of identifying alternative suppliers in stable countries (2.52) and building additional inventory during crisis situations (2.51). Performance is weaker when it comes to more long-term and strategic investments in new markets and suppliers, which score only 2.37. This suggests that efforts are often characterized by short-term crisis management rather than a more planned and long-term approach to building resilience.

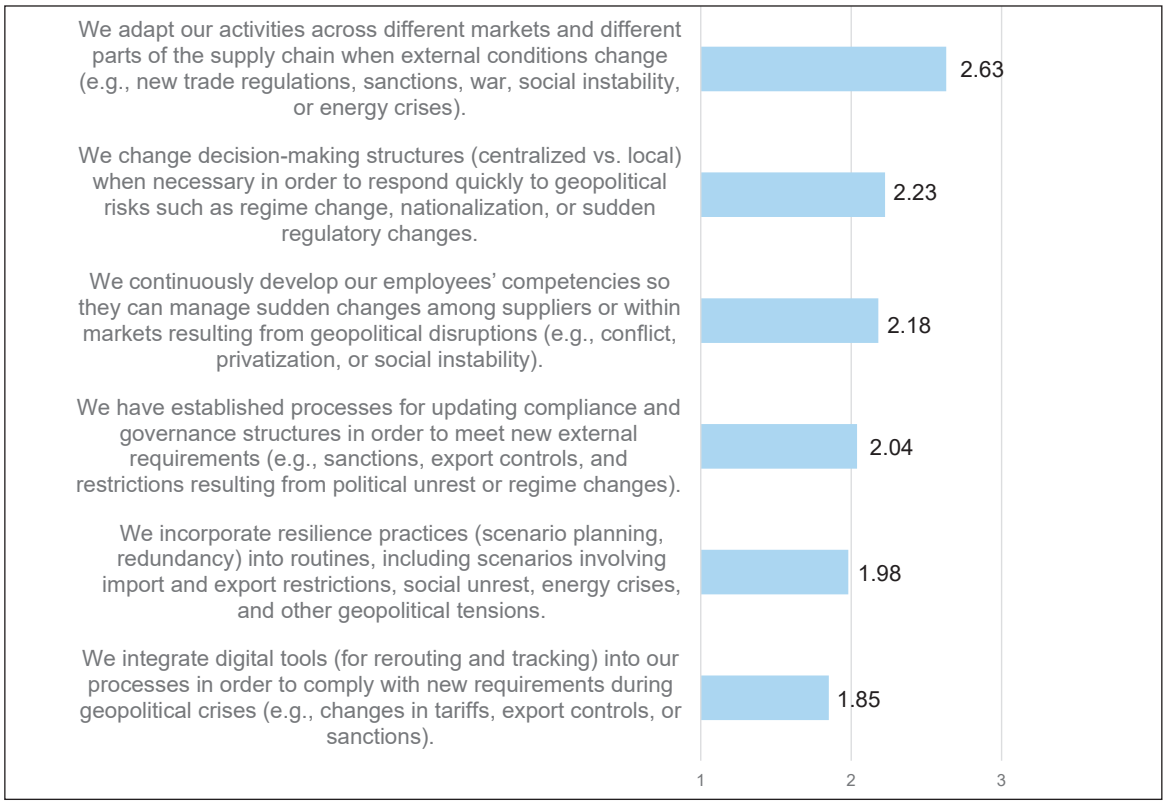
Figure 4.7 Geopolitical Seizing Capabilities



Source: Stentoft et al. (2026)

The ability to transform operations is also quite limited, as shown in Figure 4.8. SMEs do adapt their activities when changes occur in the external environment (2.63), but this takes place without clear and established procedures. At the same time, there are challenges in integrating more structured measures into daily operations. For example, the use of scenario planning remains low (1.98), and there is a lack of digital tools for monitoring and complying with new export regulations (1.85). This suggests that many SMEs still work rather informally with risk management instead of having clear systems and processes in place.

Figure 4.8 Geopolitical Transformation Capabilities



Source: Stentoft et al. (2026)

5.
Conclusion

This three-year research project on Cybersecurity and Business Continuity, supported by the Danish Industry Foundation, aimed to strengthen awareness and practical implementation of cybersecurity from a supply chain perspective. The project placed a strong emphasis on practically relevant research. This means that companies were heavily involved in the project in order to develop tools capable of strengthening cybersecurity and competitiveness, not only for the participating companies, but also for the broader industry, which can access the developed tools and software supporting the implementation of a supply chain resilience process model available on the project website: **www.cyber-smv.dk**.

The project consisted of several work packages, including nationwide questionnaire surveys, development of future scenarios, and mapping of mental models related to the understanding of cybersecurity (political level), evaluation of the future scenarios (industry level), practical application of the future scenarios (company level), and dissemination of the project's findings through articles, podcasts, conference presentations, presentations for business organizations and Danish business hubs, as well as presentations for the public and private consulting market.

Tools

A comprehensive package of 30 practical and applicable tools has been developed to help manufacturing companies strengthen their cybersecurity - not only technically, but also organizationally, strategically, and behaviorally. The tools were developed based on the realities faced by SMEs, including:

- Limited resources
- Complex supply chains
- Increasing pressure from both digital and geopolitical risks

The toolkit helps manufacturing SMEs to:

- Understand their actual cyber risks
- Strengthen supply chains and continuity
- Combine technology, organization, and human behavior
- Translate cybersecurity into concrete action

The term tools refer to practically applicable methods in the form of templates, checklists, and processes with concrete steps. Each tool is accompanied by a description of its purpose, participants, and application.

The complete toolkit consists of 30 tools distributed across the following categories:

1. Supply Chain Resilience Process Model
   a. Open-source software supporting Phases 2 and 3 of the process model
   b. Cyber-related vulnerabilities and capabilities

2. Future Scenarios
   a. U.S. withdrawal from Europe
   b. U.S.–China confrontation over Taiwan
   c. Climate change
   d. Economic polarization
   e. When AI Goes Rogue

3. Cyber Risk Management in Supply Chains
   a. Overview
   b. Risk management strategy and stakeholder analysis
   c. Cybersecurity roles and responsibilities
   d. Integration of cybersecurity into risk management and improvement processes
   e. Supplier prioritization
   f. Cybersecurity in contracts
   g. Cybersecurity due diligence for new customers
   h. Cybersecurity due diligence for new suppliers
   i. Cybersecurity register
   j. Involvement of partners during cyber incidents
   k. Integration of supply chain cybersecurity throughout the product lifecycle
   l. Checklist for termination of collaboration

4. Business Continuity
   a. Business Impact Analysis (BIA)
   b. Risk and vulnerability analysis
   c. Supplier criticality analysis
   d. Continuity plans
   e. Scenario planning
   f. Cyber contingency planning
   g. Tabletop exercises

5. Cyber Mindset
   a. Assume compromise
   b. The attacker's perspective
   c. Defense in Depth
   d. The Pause Button (Slow Down)
   e. Normalization of mistakes (Just Culture)
   f. Signal vs. Noise (Attention Economics)

6. Cyber Resilience
   a. Protection of intellectual property rights
   b. Risk reduction when entering supplier or other third-party relationships
   c. Supply chain security practices from a product and service lifecycle perspective

Questionnaire Surveys

The two questionnaire surveys conducted in 2024 and 2026 showed that 20% of respondents reported cyberattacks in the 2024 survey, while this had increased to 25% in the 2026 survey. This demonstrates the relevance of maintaining a focus on cybersecurity. The comparison between the 2024 and 2026 surveys also shows that companies generally have a high awareness of cybersecurity and a relatively solid internal foundation - particularly in terms of good internal integration and strong control over technical conditions such as IT/OT integration and system visibility. At the same time, cybersecurity is no longer perceived as technically complex, indicating a certain degree of maturity at the operational level. Despite this development, significant structural and strategic challenges remain. Cybersecurity is still primarily anchored internally within companies, and only limited requirements are imposed on suppliers and customers. This points to a low level of maturity in managing cybersecurity across the value chain, which is further supported by the persistently low level of cybersecurity supply chain risk management identified in both surveys. Furthermore, only limited progress has been made regarding strategic anchoring. Board engagement remains moderate, and the work is driven primarily by management. At the same time, the 2026 results show that companies' dynamic capabilities, both in relation to cybersecurity and geopolitics, remain low. This means that companies have only a limited ability to identify, exploit, and adapt to new threats and opportunities.

Work on geopolitical risk management also remains weakly developed, and many companies lack a strategic focus on external risk factors, including regulation and global tensions. Overall, the findings point to a clear development need: companies must increasingly elevate cybersecurity from an internal operational concern to a strategic and supply-chain-oriented issue. This requires stronger management and board engagement, greater focus on suppliers and partners, and the development of dynamic capabilities that enable companies to manage both cyber and geopolitical risks over.

6.
Perspectives

A relevant perspective on the project points to several obvious directions for further research and development. First, it would be relevant to investigate how cybersecurity in supply chains is managed in other countries, particularly in economies with a high level of digital maturity similar to Denmark. Such a comparative analysis could reveal whether the challenges experienced by Danish SMEs, for example, lack of strategic anchoring and limited supplier integration, are general or context-specific.

In addition, further research could beneficially focus on sectors other than manufacturing, such as healthcare, finance, or critical infrastructure, where the consequences of cyberattacks are often even more severe and where regulatory requirements play a greater role. The approach used in this project could be replicated across other sectors. This could contribute to a more nuanced understanding of how sector differences influence cybersecurity and business continuity.

Another important direction is to examine how companies can concretely develop their dynamic capabilities, particularly in relation to managing emerging threats such as artificial intelligence, geopolitical instability, and increasing regulatory requirements (e.g., the NIS 2 Directive). Future research could focus on identifying which management practices and organizational structures support a more strategic approach to cybersecurity.

Finally, it may be relevant to analyze the implementation and long-term effects of the developed tools. This could involve examining the extent to which companies actually change their behavior, improve their security levels, and achieve greater resilience within their supply chains. Longitudinal studies or case studies could provide deeper insight into what works in practice and which barriers still exist. Overall, this perspective suggests that cybersecurity should increasingly be understood as a strategic and cross-organizational issue that extends beyond the individual company and requires international, sectoral, and organizational attention.

The Project's Interdisciplinary Nature: Advantages and Challenges

This project represents a complex interdisciplinary collaboration integrating supply chain management and business understanding (Department of Business and Sustainability), political science and international relations (Center for War Studies), and computer science and cybersecurity (Department of Mathematics and Computer Science). This constellation proved essential, as today's security challenges in global supply chains constitute a problem that is too multidimensional to be adequately addressed within the framework of a single academic discipline.

Advantages of the Interdisciplinary Integration

The combination of these three research fields creates unique synergies that structurally expand the traditional understanding of business operations and threat management.

- The integration of political science with supply chain management and business understanding makes it possible to translate macro-political tensions into supply chain strategies at the company level. Whereas traditional supply chain research may adopt a narrower, market-driven, and disciplinary perspective, political science adds a fundamental understanding of the exercise of state power. This enables companies to navigate an environment characterized by politically driven market disruptions rather than merely economic fluctuations. Political science contributes new concepts and understandings that can strengthen work with actors across supply chains, while supply chain management and business understanding provide the concrete empirical insights at the company level.
- The intersection between computer science and supply chain management and business understanding builds a critical bridge between technical infrastructures and organizational processes within companies. Computer science can provide advanced solutions for securing the information flows on which supply chains depend - an area that traditional supply chain experts often lack the technical foundation to address holistically. Conversely, this interaction also provides insights into what actually occurs in practice, enabling efforts to focus more precisely on what is practically relevant.
- The collaboration between political science and computer science enables a significantly deeper understanding of cyber threats. Within this intersection, cyberattacks are analyzed not merely as technical anomalies that must be patched, but to a large extent as political instruments and integrated elements within an asymmetric geopolitical power struggle.

Challenges and Inherent Risks of Interdisciplinary Integration

Despite the cross-disciplinary benefits, interdisciplinary work is fundamentally challenging and carries significant inherent risks that must be actively identified and managed in order to avoid analytical weaknesses.

- The traditional methodological clash between the formal, quantitative system logics of computer science and the systemic and interpretive approaches of the social sciences was significantly minimized in this project. This was primarily because the participating computer scientists were research-oriented toward the sociology of cybersecurity and the mental models of end users. This shared interest in the human and behavioral dimension substantially facilitated epistemological integration. However, within this partially overlapping field, a new analytical challenge emerges: Balancing the micro-perspective (the individual user's interaction with security systems) against the macro-perspective (the strategic behavior of organizations and states within supply chains). If these levels are uncritically merged, the analysis risks losing explanatory power.
- Despite the strong methodological convergence, temporal and institutional framework conditions remain a universal challenge. **Fully synthesizing knowledge across supply chain management, security policy, and human-centric computing requires an iterative and time-consuming translation process.** Under fixed project deadlines, the risk of instrumental interdisciplinarity remains present, where research groups, despite shared interests, may be pushed back into disciplinary silos in order to ensure timely deliverables, which ultimately may reduce the holistic value creation of the project.

References

Barney, J.B. (1991), “Firm resources and sustained competitive advantage”, *Journal of Management*, Vol. 17 No. 1, pp. 99–120.

Christopher, M. & Peck, H. (2004), “Building the resilient supply chain”, *The International Journal of Logistics Management*, Vol. 15 No. 2, pp. 1-13.

Crask, J. (2024), *Business Continuity Management: A Practical Guide to Organization Resilience and ISO 22301*, Kogan Page Ltd., London.

Espersen, I.N., Sjøberg, M. & Kaastrup, J. (2026), *Usynlig fjende - Hackerangreb og hemmelige netværk,* Politikens Forlag, København V.

Europa-Kommissionen (2003), https://eur-lex.europa.eu/legal-content/DA/TXT/?uri=CELEX%3A32003H0361, tilgået 12. februar 2026.

Fan, Y. & Stevenson, M. (2018), ”A review of supply chain risk management: definition, theory, and research agenda”, *International Journal of Physical Distribution & Logistics Management*, Vol 48 No. 3, pp. 205-230.

Farrell, H. & Newman, A.L. (2019), “Weaponized interdependence: How global economic networks shape state coercion open access”, *International Security*, Vol. 44 No. 1, pp. 42-79.

Hiles, A. (2014), *Business Continuity Management: Global Best Practices*, 4. udg. Rothstein Publishing, Brookfield.

Kankam-Boateng, J., Peressotti, M., Stentoft, J., Wickstrøm, K.A., Keating, V.C., Tumchewics, L.A., Schmitt, O., Theussen, A. & Mayer, P. (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 (CHI ‘26),* Barcelona, Spain. ACM. Association for Computing Machinery, New York, Article 76, 1-26.

Mayer, P., Zou, Y., Lowens, B.M., Dyer, H.A., Le, K., Schaub, F. & Aviv, A.J. (2023), “Awareness, intention, (in)action: Individuals’ reactions to data breaches”, *ACM Transactions on Computer-Human Interaction*, Vol. 30 No. 5, pp.1-53.

Melnyk, S.A., Schoenherr, T., Speier-Perob, C., Peters, C., Chang, J.F. & Friday, D. (2022), “New challenges in supply chain management: Cybersecurity across the supply chain”, *International Journal of Production Research,* Vol. 60 No.1, pp. 162-183.

Narasimhan, R., Nair, A., Griffith, D.A., Arlbjørn, J.S. & Bendoly, E. (2009), “Lock-in situations in supply chains: A social exchange theoretic study of sourcing arrangements in buyer–supplier relationships”, *Journal of Operations Management*, Vol. 27 No. 5, pp. 374-389.

NIST (National Institute of Standards and Technology) (2024), *The NIST Cybersecurity Framework (CSF) 2.0.*, National Institute of Standards and Technology, Gaithersburg, MD.

NIST (National Institute of Standards and Technology) (2026), https://csrc.nist.rip/glossary/term/cybersecurity?utm_source=chatgpt.com (tilgået 18. marts, 2026).

Peressotti, M., Mayer, P., Kjær, T.B.H. & Stentoft, J. (2024), "SCM Agendaen – Cybersecurity Awareness", podcast publiceret på: https://www.scm.dk/scm-agendaen, tilgået 8. april 2026.

Pettit, T.J., Croxton, K.L. & Fiksel, J. (2013), "Ensuring supply chain resilience: Development and implementation of an assessment tool", *Journal of Business Logistics*, Vol. 34 No. 1, pp. 46-76.

Pettit, T.J., Fiksel, J. & Croxton, K.L. (2010), "Ensuring supply chain resilience: Development of a conceptual framework", *Journal of Business Logistics,* Vol. 31 No. 1, pp. 1-21.

Schmitt, O., Keating, V., Kjær, T.B.H. & Stentoft, J. (2024), "SCM Agendaen – Geopolitiske spændinger og cybersikkerhed", podcast publiceret på https://www.SCM.dk, tilgået 8. april 2026.

SMVdanmark, https://smvdanmark.dk/analyser/temaanalyser/smver-erygraden-i-dansk-erhvervsliv?utm_source=chatgpt.com, tilgået 14. februar 2026.

Stentoft, J. & Mikkelsen, O.S. (2024), "Towards Supply Chain Resilience: A Structured Process Approach", *Operations Management Research,* Vol. 17, pp. 1421-1443.

Stentoft, J., Keating, V., Peressotti, M. & Mayer, P. (2025), "Hvordan sikrer vi, at cybersikkerhed bliver taget alvorligt?", kronik, *Erhverv+ Fyn*, 6. februar, p. 16.

Stentoft, J., Mikkelsen, O.S. & Kjær, T.H. (2023), *Supply Chain Resilience i små og mellemstore danske produktionsvirksomheder,* Institut Entreprenørskab og Relationsledelse, Syddansk Universitet.

Stentoft, J., Mikkelsen, O.S. & Rajkumar, C. (2018), *Supply Chain Management: Sources for Competitive Advantages*, Hans Reitzels Forlag, Copenhagen.

Stentoft, J., Mikkelsen, O.S. & Wickstrøm, K.A. (2025a), "Et svagt led kan lamme os alle – derfor kræver forsyningskæder stærk cybersikkerhed", Kronik, *Erhverv+ Sydjylland*, 9. oktober, p. 20.

Stentoft, J., Mikkelsen, O.S. & Wickstrøm, K.A. (2025b), "Reshoring manufacturing: The influence of industry 4.0, Covid 19, and made in effects", *Operations Management Research*, Vol. 18 No. 1, pp. 353-372.

Stentoft, J., Mikkelsen, O.S., Schmitt, O., Keating, V., Theussen, A., Peressotti, M., Mayer, P., Kankam-Boateng, J. & Tumchewics, L. (2024), *Cybersikkerhed i små og mellemstore danske produktionsvirksomheder*, Institut for Erhverv og Bæredygtighed, Syddansk Universitet, Center for War Studies, Syddansk Universitet, Institut for Matematik og Datalogi, Syddansk Universitet samt Forsvarsakademiet.

Stentoft, J., Mikkelsen, O.S., Wickstrøm, K.A., Keating, V., Tumchewics, L., Theussen, A., Peressotti, M., Mayer P. & Kankam-Boateng, J. (2026), *Cybersikkerhed i praksis: Indsigter fra danske produktionsvirksomheder*, Institut for Erhverv og Bæredygtighed, Syddansk Universitet, Center for War Studies, Syddansk Universitet, Institut for Matematik og Datalogi, Syddansk Universitet samt Forsvarsakademiet.

Stentoft, J., Peressotti, M. & Mayer, P. (2024), "Derfor skal NETOP DU være ekstra på vagt", kronik, *Business Danmark*, 10. januar.

Stentoft, J., Peressotti, M., Mayer, P., Wickstrøm, K.A., Schmitt, O., Keating, V.C., Theussen, A., Tumchewics, L.A. & Kankam-Boateng, J. (2025), "The relationship between cybersecurity awareness, cybersecurity supply chain risk management and firm performance", *Supply Chain Management: An International Journal,* Vol. 30 No. 5, pp. 497-517.

Stentoft, J., Schmitt, O. & Keating, V. (2024), "Supply chain risk management and geopolitics: A new research agenda", artikel præsenteret på den 36. NOFOMA conference organiseret af Swedish Defence University and KTH Royal Institute of Technology, Gøteborg, den 13-14. juni.

Styrelsen for Samfundssikkerhed (2024), https://www.sikkerdigital.dk/virksomhed, tilgået 12. februar 2026.

Styrelsen for Samfundssikkerhed (2025), *Trusselsvurdering: Cybertruslen mod Danmark 2025,* Styrelsen for Samfundssikkerhed, Birkerød.

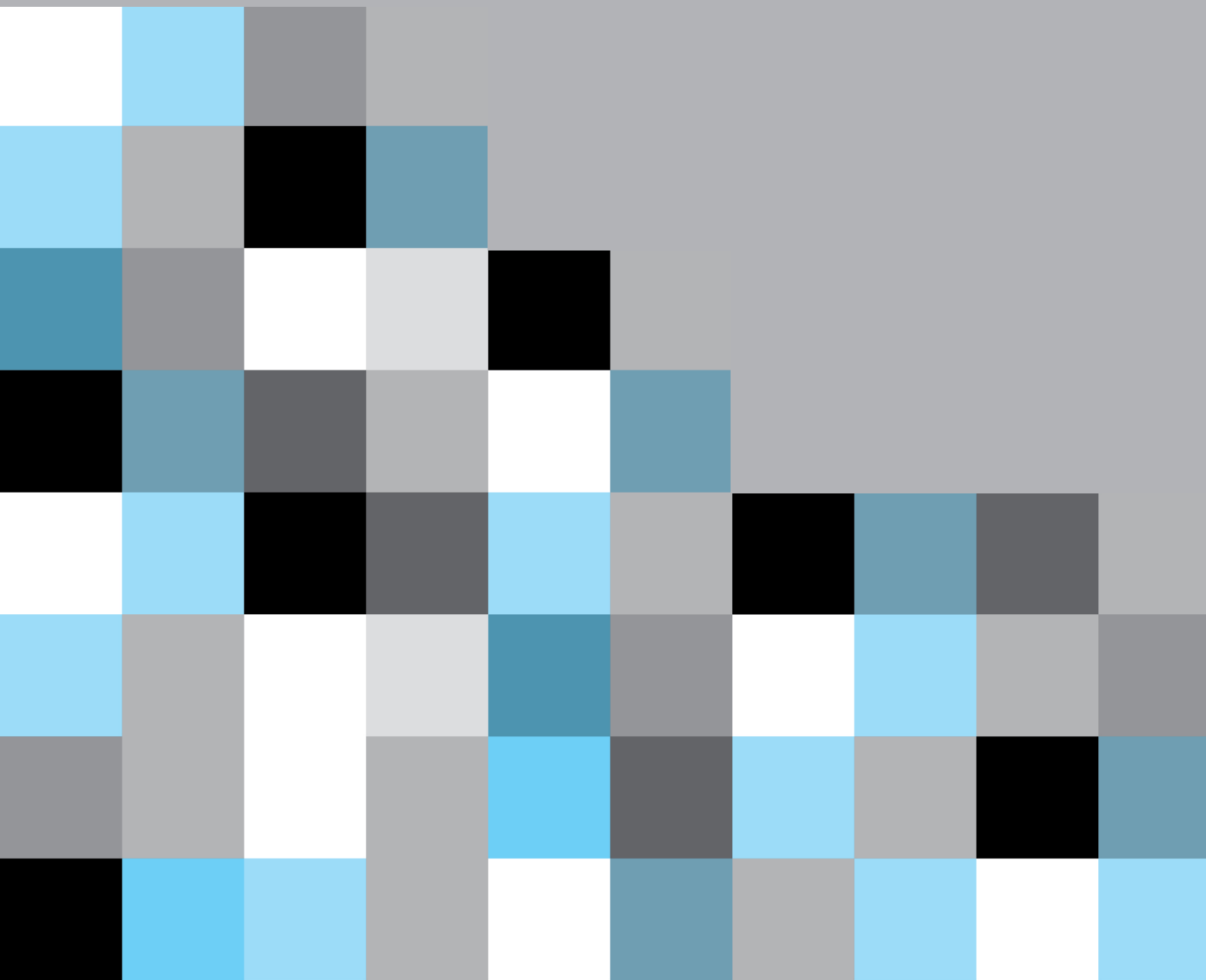
Teece, D.J. (2007), "Explicating dynamic capabilities: The nature and micro-foundations of (sustainable) enterprise performance", *Strategic Management Journal,* Vol. 28 No. 13, pp. 1319-1350.

Teece, D.J., Pisano, G. & Shuen, A. (1997), "Dynamic capabilities and strategic management", *Strategic Management Journal*, Vol. 18 No. 7, pp. 509–533.

Woods, M. (2022), *Risk Management in Organisations: An Integrated Case Study Approach*, Routledge, New York.

Zach, O., Munkvold, B.E. & Olsen, D.D. (2014), "ERP system implementation in SMEs: Exploring the influences of the SME context", *Enterprise Information Systems*, Vol. 8 No. 2, pp. 309-335.

About the Authors



Jan Stentoft, PhD, is Professor of Supply Chain Management at the Department of Business and Sustainability at the University of Southern Denmark. His research is application-oriented, and his research interests and teaching relate to supply chain management, supply chain resilience, cybersecurity, geopolitics, supply chain innovation, lean philosophy, sales and operations planning, and production location decisions from a global perspective with an emphasis on the use of new digital technologies. Jan has practical industry experience from positions at Dandy, Gumlink, and LEGO, as well as from ongoing assignments as a management consultant.

Ole Stegmann Mikkelsen, PhD, is Associate Professor of Supply Chain Management at the Department of Business and Sustainability at the University of Southern Denmark. His research interests and teaching are within supply chain management, supply chain resilience and risk management, strategic and global sourcing, supply chain innovation, sales and operations planning, and production location decisions from a global perspective. Ole has practical industry experience from positions at Milliken Denmark A/S and Danfoss A/S.

Kent Adsbøll Wickstrøm, PhD, is Associate Professor at the Department of Business and Sustainability within the field of organization theory. His research interests and teaching focus on organizational design, organizational behavior, digital transformation, digital strategy, technology management, knowledge management, and supply chain resilience. Kent is Head of the Supply Chain and Technology Management research group and is responsible for the MSc program specialization in Data Driven Business Development at the University of Southern Denmark.

Vincent Keating, PhD, is Associate Professor at the Center for War Studies, University of Southern Denmark. His research falls within security studies from the perspectives of political sociology and political theory. Vincent's previous research has examined how states and non-state organizations maintain trust and legitimacy, how the ideological appeal of Russian values leads Western populist groups to support Russian foreign policy, and how states make choices between human rights and security.

Louise Tumchewics, PhD, is a Postdoctoral Researcher at the Center for War Studies, University of Southern Denmark. Louise holds a PhD in War Studies from King's College London. Her research focuses on war and technology, economic warfare, and civil-military relations. Before joining the University of Southern Denmark, Louise was a Senior Researcher at the British Army's Centre for Historical Analysis and Conflict Research (CHACR), Assistant Professor at Rabdan Academy in the United Arab Emirates and Visiting Research Fellow at King's College London. Louise is editor of *Small Armies, Big Cities* — a study of modern urban warfare — and is the author of two forthcoming books.

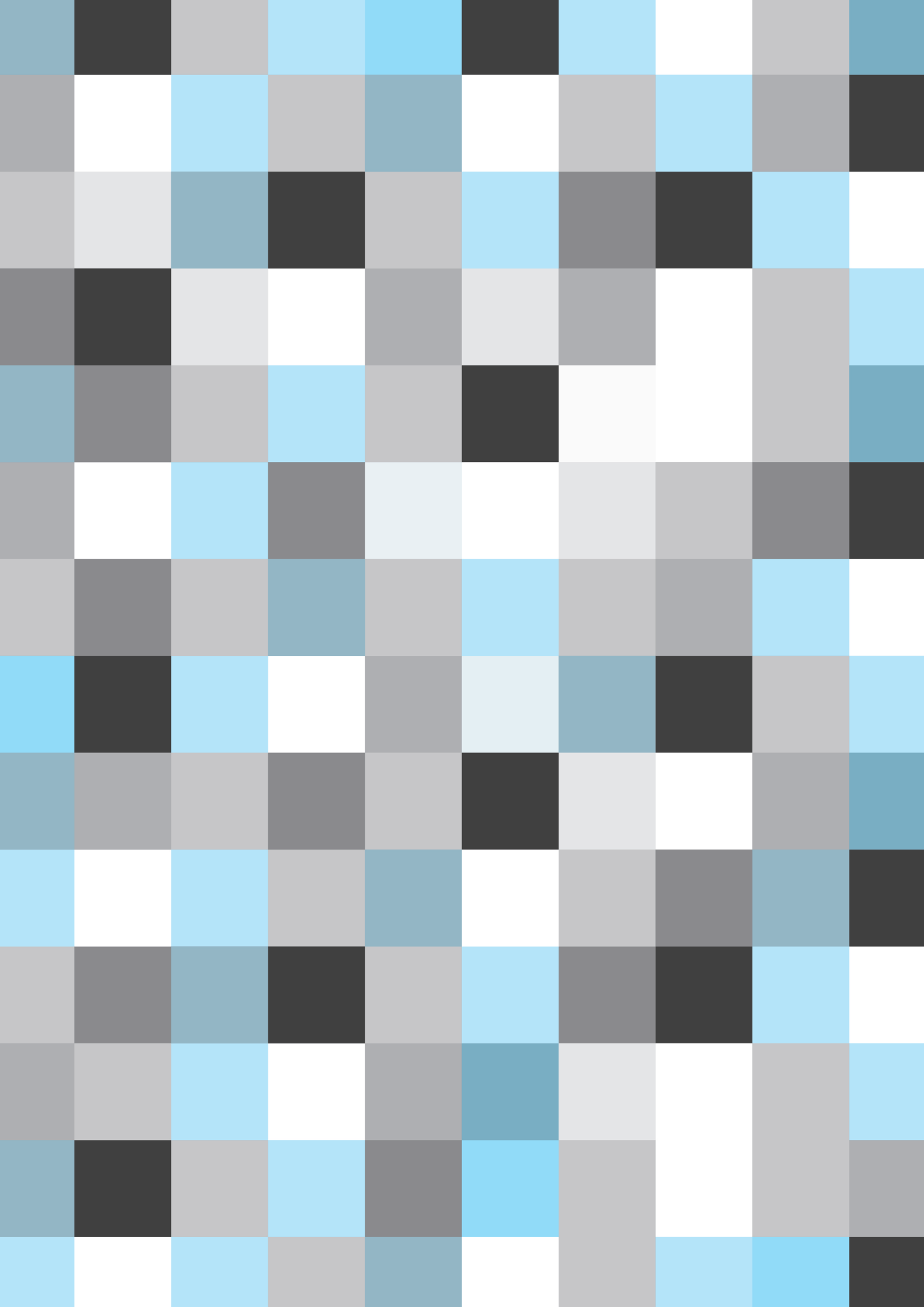
Olivier Schmitt, PhD, is Professor and Head of Research at the Department of Military Operations at the Royal Danish Defence College. He is also Senior Non-Resident Associate Fellow at the NATO Defence College and Associate at RAND Europe. His research focuses on European security, military transformation, and the changing character of warfare.

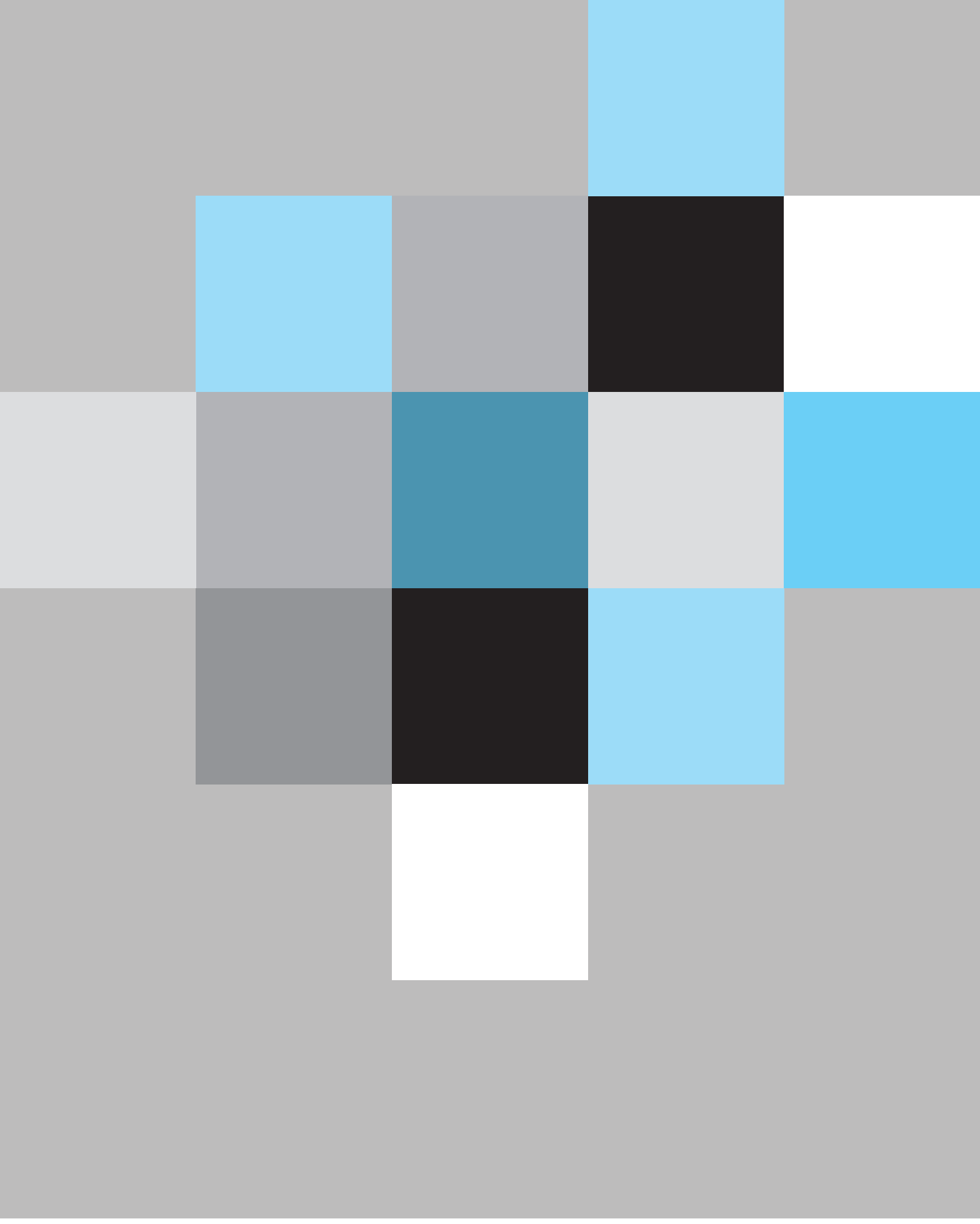
Amelie Theussen, PhD, is Associate Professor at the Royal Danish Defence College. Her research focuses on the security situation in the Arctic and the Baltic Sea region, Danish and German security and defense policy, and the question of how warfare is changing and what consequences this has for political and legal norms concerning the use of force. In addition, she designs and conducts award-winning simulation exercises for universities and military education programs.

Marco Peressotti, PhD, is Associate Professor at the Department of Mathematics and Computer Science, University of Southern Denmark. Marco's research mission is to make it more effective to program, analyze, and secure digital systems. He develops new methods and tools to support the development and maintenance of correct and secure software, particularly for interconnected systems that form the core of the digital transformation. An overarching theme in his research approach is the use of techniques from cybersecurity, artificial intelligence, and programming languages, as well as the ambition of creating a unified mathematical perspective.

Peter Mayer, PhD, is Associate Professor at the Department of Mathematics and Computer Science, University of Southern Denmark. Peter researches "End-user Viable Information Security & Privacy Solutions." His research is independent of whether the end user of a security solution is a layperson, administrator, or developer. The focus is on making security and privacy solutions viable for the target audience by considering their specific needs and competencies. An important aspect of this research is understanding end users' mental models, that is, how they believe cybersecurity affects them and how effective they perceive countermeasures to be.

Judith Kankam-Boateng is a PhD student at the Department of Mathematics and Computer Science, University of Southern Denmark. Judith holds a bachelor's degree in Information Technology and a master's degree in Law, Digital Innovation, and Sustainability with a focus on digitalization. She has a strong research interest in databases, programming, and software development. Judith has, among other things, worked as a teaching assistant for courses in artificial intelligence, machine learning, and blockchain technologies. She has expertise in ERP Microsoft Dynamics NAV 2018 and experience as a Business Analyst, Product Owner, and Scrum Master.





SDU

INDUSTRIENS FOND

ROYAL DANISH DEFENCE COLLEGE