Received 22 April 2025
Revised 21 September 2025
22 December 2025
Accepted 29 March 2026

How the Finnish governance networks enhance digital resilience under hybrid threats and economic uncertainty?

Jukka Keinänen
School of Management, University of Vaasa, Vaasa, Finland

Abstract

Purpose – This study examines how Finnish governance networks enhance resilience in the face of digital transformation and hybrid threats. Specifically, it explores how multi-level governance, institutional coordination, and public–private collaboration shape digital resilience, hybrid threat management, and economic security by fostering adaptive and proactive resilience strategies.

Design/methodology/approach – The study employs a qualitative research design based on 36 thematic interviews with public-sector actors, nongovernmental organisations, and small and medium-sized enterprises involved in trade and economic governance. Using a governance resilience framework, it examines how networked governance structures adapt to digital and geopolitical disruptions.

Findings – Governance resilience rests on institutional coordination, regulatory adaptability, and strategic foresight. Additionally, effective digital transformation depends on the alignment of governance structures across multiple levels, from global to regional. Hybrid threats and economic dependencies require proactive risk management, including scenario planning, resilience audits, and foresight practices. Public–private collaboration emerges as a critical mechanism when institutionalised — through structured dialogue, shared data practices, and joint investment — rather than short-term or ad hoc initiatives.

Originality/value – This study refines governance resilience research by demonstrating how digital sovereignty, hybrid threat mitigation, and regulatory coordination interact within a multi-level economic governance framework. It highlights the significance of institutionalised collaboration and anticipatory policymaking in ensuring long-term resilience. The findings provide policymakers and governance actors with actionable insights to strengthen digital resilience in an era of geopolitical and technological volatility.

Keywords Governance resilience, Digital transformation, Hybrid threats, Multi-level governance, Public-private collaboration, Finland

Paper type Research article

Introduction

Amid rising geopolitical tensions worldwide, governance resilience has become a critical framework for understanding how institutions withstand, adapt to, and recover from systemic disruptions (Boin *et al.*, 2021; Linkov and Trump, 2019). However, resilience in the digital age requires proactive strategies, adaptive governance, and the integration of technological solutions within institutional networks (Linkov *et al.*, 2013).

Network-based governance has emerged as a key mechanism for managing complexity in modern policymaking, emphasising multi-actor collaboration, flexible decision-making, and adaptive coordination across different governance levels (Ansell and Gash, 2008; Klijn and Koppenjan, 2016). These principles are particularly relevant in governance systems with ingrained decentralised decision-making, such as the Nordic countries, where regional actors play a key role in fostering resilience and policy innovation (Van Well *et al.*, 2018). Owing to the increasing reliance on digital infrastructures, governance structures must balance adaptability with institutional stability (Ansell *et al.*, 2021).

Public Administration and Policy
Vol. 29 No. 2, 2026
pp. 170-184
Emerald Publishing Limited
e-ISSN: 2517-679X
p-ISSN: 1727-2645
DOI 10.1108/PAP-04-2025-0061

This study examines the Team Finland network, a multi-scalar governance system that operates across regional, national, and international levels to support export promotion, small and medium-sized enterprises (SME) internationalisation, and investment facilitation. While administratively coordinated from Finland, the network's activities span over 80 country teams worldwide, making it an illustrative example of internationally embedded governance.

Existing research on resilience and governance emphasises either technological infrastructures and digital transformation (Dunleavy *et al.*, 2006) or institutional adaptation and sovereignty concerns (Dunn Cavelty and Wenger, 2020), with less attention given to the interconnections between these dimensions and how they jointly shape governance responses. This study examines how governance networks adapt to digital transformation and strengthen resilience amid hybrid threats and economic uncertainty.

Digital resilience is defined as the capacity of governance systems to anticipate, withstand, and adapt to digital disruptions (Mahmood *et al.*, 2024). *Digital sovereignty* refers to the ability of a state or governance network to maintain legitimate control over its digital infrastructure, data governance, and technological standards in line with strategic interests (Roberts, 2024). *Regulatory fragmentation* describes the lack of coherence across jurisdictions or governance levels, leading to gaps in digital policy design and implementation (OECD, 2025). Governance networks refer to collaborative arrangements linking public institutions, businesses, and other stakeholders across governance levels to coordinate strategies and resources in response to shared challenges (Ansell and Gash, 2008; Klijn and Koppenjan, 2016).

This study draws on resilience theory to examine the following research questions:

1. In what ways do hybrid threats and economic vulnerabilities challenge governance networks' capacity to respond and coordinate under uncertainty?
2. How do governance networks adapt institutional practices to overcome strategic challenges?
3. How is inter-organisational coordination leveraged across governance levels in relation to digital resilience?

This study contributes to debates on governance resilience and digital transformation, offering insights for policymakers, businesses, and governance actors.

Governance resilience: conceptual framework

This study conceptualises governance resilience as a multidimensional construct, integrating insights from multiple literature strands. Multi-level governance provides the structural background, networked coordination offers the operational logic, and digital infrastructures create enabling conditions for institutional adaptability.

Resilience theory has been applied across various disciplines, including governance structures (Linkov and Trump, 2019). Resilience refers to the ability of systems to absorb shocks, adapt, and transform in response to external pressures. Hence, this study adopts a governance resilience perspective to examine how hybrid threats challenge institutional stability and how governance networks respond through digital governance and cross-sectoral collaboration to strengthen strategic adaptability. By integrating resilience into the governance framework, this study reveals how organisations and regions manage uncertainty, reduce vulnerabilities, and enhance strategic foresight.

Governance resilience is critical for understanding how institutions manage uncertainty, adapt to disruptions, and maintain operational stability (Boin *et al.*, 2021; Martin and Sunley, 2020). Traditionally, resilience in governance has been linked to crisis management and institutional robustness (Boin *et al.*, 2021; Linkov and Trump, 2019). However, digital transformation has introduced new resilience dimensions, necessitating governance structures that integrate digital infrastructures, adaptive policymaking, and strategic coordination mechanisms (Linkov *et al.*, 2013). Moreover, governance resilience is inherently linked to networked governance, as institutional adaptability depends on inter-organisational coordination and regulatory flexibility (Ansell *et al.*, 2021; Rhodes, 1996).

Multi-level governance (Hooghe and Marks, 2003) emphasises the distribution of governance authority across different levels, requiring effective coordination between international, national, and regional actors. Digital resilience is closely linked to effective multi-level coordination, which supports institutional adaptability and coherent governance responses (Dunn Cavelty *et al.*, 2023). Geels (2018) emphasises that multi-level governance fosters flexibility in institutional responses to technological and policy shifts. However, digital governance does not inherently guarantee resilience; rather, it introduces new vulnerabilities (Dunn Cavelty and Wenger, 2020). The extent to which governance actors can mitigate these risks depends on institutional coordination, regulatory adaptability, and strategic foresight (Martin and Sunley, 2020; Boin *et al.*, 2020). Thus, multi-level governance enhances governance resilience by organising authority, resources, and decision-making responsibilities in response to uncertainty.

Hybrid threats, digital vulnerabilities, and economic security

Hybrid threats encompass tactics such as disinformation campaigns, cyberattacks, economic coercion, and the manipulation of strategic dependencies. These exploit vulnerabilities in governance systems and market structures (Dunn Cavelty and Wenger, 2020; Dunn Cavelty *et al.*, 2023). These tactics blur the lines between traditional security threats and economic strategies, as seen in the increasing use of regulatory and digital tools as instruments of geopolitical influence (Farrand and Carrapico, 2022).

Regional governance networks with strong digital dependencies but limited cybersecurity expertise is particularly vulnerable to hybrid threats. In digitally advanced economies, regulatory fragmentation may create loopholes that could be exploited by foreign actors. Conversely, in digitally underdeveloped regions, the lack of digital governance mechanisms can hinder rapid responses and coordination efforts. Hybrid threats not only disrupt economic stability but also test the adaptive capacity of governance networks. In an era of interconnected crises, governance resilience depends on multi-level coordination and adaptive governance structures (Boin *et al.*, 2020; Dunleavy *et al.*, 2006). Similarly, in the realm of digital security, governance frameworks must integrate cross-sectoral responses to emerging threats (OECD, 2019).

Economic interdependencies, particularly in critical technology sectors, have become strategic leverage points in global governance resilience. The ability of governance networks to manage these dependencies influences their capacity to reduce external pressures and maintain stability (Baldwin and Evenett, 2020).

Networked governance, regulatory adaptation, and cross-sector collaboration

Effective resilience strategies require structured inter-organisational coordination that allows for regulatory flexibility and rapid adaptation (Morsut *et al.*, 2021; Keinänen *et al.*, 2026). Governance networks play a fundamental role in resilience-building by bridging institutional gaps, aligning economic and security objectives, and fostering adaptive policymaking (Klijn and Koppenjan, 2016; Christensen and Lægreid, 2020). These networks must create institutionalised engagement mechanisms that facilitate direct cooperation between public authorities, private enterprises, and regional development agencies to ensure that resilience strategies remain both proactive and actionable (Ansell and Gash, 2008; Mizrahi *et al.*, 2021).

Sustained public-private collaboration requires structured mechanisms that ensure continuity. Intermediary institutions, such as cybersecurity councils or industry task forces, facilitate knowledge exchange, regulatory alignment, and investment in digital resilience. These mechanisms help sustain public-private cooperation and reduce governance fragmentation (Ansell and Gash, 2008; Provan and Kenis, 2007; World Economic Forum, 2017).

Networked governance serves as a critical intermediary in regulatory adaptation, ensuring flexible policies while maintaining consistency across governance levels (Martin and Sunley, 2020; Keinänen and Luoto, 2025). This is particularly relevant in digital governance, where interoperability challenges and regulatory fragmentation can weaken the institutional capacity to implement resilience strategies (Dunn Cavelty and Wenger, 2020). By embedding resilience strategies within institutional structures, fostering long-term digital security partnerships, and integrating adaptive economic policies, governance networks can ensure that resilience remains a foundational principle. A structured collaboration between governance actors enhances resilience at the institutional level and supports sustainable, innovation-driven regional development.

By examining how governance networks address hybrid threats and digital dependencies through multi-level coordination and cross-sector collaboration, this study clarifies how governance resilience is enacted in digitally dependent policy environments.

Research methods

Based on a theory-informed and empirically grounded conceptual framework, this qualitative study examines how governance networks respond to digital transformation, hybrid threats, and economic uncertainty through policy coordination, cross-sector collaboration, and institutional adaptation to enhance resilience. It employs a single case study approach (Yin, 2018), examining the Team Finland governance network to explore the complexity of governance resilience.

This case study focuses on how governance institutions, business associations, and internationally active SMEs interact within governance mechanisms to strengthen digital resilience and economic security. The analysis clarifies these dynamics across governance levels and regional contexts, rather than generalising from the specific case itself. Overall, 36 thematic interviews were conducted with key actors involved in export promotion, internationalisation support, and economic governance. The interviewees represented public-sector actors, non-governmental business organisations, and internationally active SMEs. They were selected based on their roles and expertise in these domains. Most public-sector and business-organisation participants held senior-, expert-, or executive-level positions, with extensive professional experience in public administration, trade promotion, and internationalisation policy. NGO representatives and SME owners or executives were included due to their direct experience with export activities, cross-border business operations, and collaboration with governance institutions. Several participants had been involved in the Team Finland network since its formation, providing institutional memory and strategic perspectives. Public sector representatives were recruited from ministries involved in economic and trade governance (e.g., the Ministry of Economic Affairs and Employment, the Ministry for Foreign Affairs) and key agencies (Business Finland, Finnvera, ELY Centres). Business organisations, such as the Confederation of Finnish Industries, the Central Chamber of Commerce, and the Federation of Finnish Enterprises, provided perspectives on regulatory challenges and intermediary roles, while internationally active SMEs offered firm-level insights into export dynamics and institutional coordination. The interview data highlight the multi-scalar nature of the Team Finland network (Team Finland, 2019): while some organisations operate across international, national, and regional levels (e.g., ministries, missions abroad, Business Finland), others — such as ELY Centres — focus on subnational implementation. These variations reflect the networked governance structure analysed in this study.

The selection process ensured diverse and multi-scalar perspectives on governance adaptation. A snowball sampling approach (Noy, 2008; Patton, 2002) was used to identify key informants through expert referrals, allowing access to relevant expertise across different levels of governance and private-sector networks. Thematic interviews were conducted to capture in-depth perspectives on governance adaptation (Braun and Clarke, 2021). Data collection continued until theoretical saturation was reached (Hennink *et al.*, 2017), ensuring that all major themes were captured while avoiding redundancy.

The interviews were conducted between December 2022 and December 2023. To maintain confidentiality, interviewees were pseudonymised as R1-R36. The interviews were guided by a thematic structure, focusing on three key dimensions: governance and networks, disruptions and transitions, and regional perspectives. In addition to the interview data, secondary sources, such as national policy documents, Team Finland strategy papers, organisational reports from trade and innovation agencies, and official evaluations of the network's governance and coordination, were utilised to provide contextual background and support the interpretation of findings (Creswell and Poth, 2018). This additional material helped position the interview insights within broader governance structures and policy developments. These sources complemented the interview findings by clarifying governance structures and regulatory frameworks. The study followed the Standards for Reporting Qualitative Research (SRQR) guidelines (O'Brien *et al.*, 2014) to ensure clarity and transparency in reporting.

The study employed a theory-informed approach, with resilience theory providing the core conceptual foundation. The conceptual framework was grounded in existing governance resilience literature but applied iteratively to the empirical material. While the main categories were informed by theoretical concepts, subcodes and thematic patterns were refined during the coding process to capture nuances emerging from the data. The framework comprises three components: a conceptual grounding that links governance resilience theory to established frameworks, theory-based subcodes that bridge theoretical and empirical dimensions, and overarching thematic codes that structure the analysis around governance resilience in the digital age. Table 1 presents the coding framework for analysing governance resilience in the digital age.

Table 1. Coding framework for analysing governance resilience in the digital age

Theory	Theory-based Subcode	Main Category of Governance Resilience in the Digital Age
Governance Resilience (Boin *et al.*, 2021; Linkov and Trump, 2019)	Institutional adaptation; anticipation and crisis response	Digital Resilience and Multi-Level Governance Framework
Multi-Level and digital Governance (Hooghe and Marks, 2003; Geels, 2018; Dunn Cavelty and Wenger, 2020; Martin and Sunley, 2020; Dunn Cavelty *et al.*, 2023)	Coordination across governance levels; ICT integration and interoperability; uneven access to digital infrastructure and policy implementation	Digital Resilience and Multi-Level Governance
Hybrid Threats and Economic Security (Dunn Cavelty and Wenger, 2020; Baldwin and Evenett, 2020; Farrand and Carrapico, 2022)	Strategic dependencies; cybersecurity; supply chain vulnerabilities	Hybrid Threats and Economic Vulnerabilities
Networked Governance and Public-Private Collaboration (Ansell and Gash, 2008; Ansell *et al.*, 2021)	Collaborative models; intermediary roles; institutionalised partnerships	Networked Governance and Digital Sovereignty
Regulatory Governance (Martin and Sunley, 2020; OECD, 2025)	Balancing digital sovereignty; regulatory fragmentation; market openness	Networked Governance and Digital Sovereignty
Resilience and Governance Networks (Klijn and Koppenjan, 2016; Morsut *et al.*, 2021; Keinänen *et al.*, 2026)	Crisis management; proactive adaptation and organisational learning	Cross-cutting themes in Governance Resilience

Source: By author

Findings

Digital resilience and multi-level governance

Digital resilience is shaped by technological advancements and unequal access to digital resources (Dunn Cavelty and Wenger, 2020; Boin and Rhinard, 2022). The Team Finland network illustrates how capacity varies across regions, with disparities in infrastructure, coordination, and expertise undermining resilience.

A respondent from the international Team Finland network highlighted the difficulty of accessing crucial information in some countries:

> The regional availability of information and its consideration in operational and service planning are crucial. In some countries, accessing information is not easy — there are no readily available details on websites. You can't just Google them. (R24)

In digitally constrained regions, outdated service structures and governance delays exacerbate resilience disparities between advanced and lagging areas, restricting access to information and reducing the ability to respond to crises effectively, thereby weakening governance resilience. This corresponds to the governance and coordination challenges in Table 1, where fragmented structures and uneven digital infrastructures reduce the capacity for timely adaptation.

Some respondents emphasised that digitalisation efforts remain inconsistent across governance levels, affecting both internal processes and service delivery. One public official noted:

> Digital development varies across organisations, with deficiencies evident in places like [–]. This affects transformation capacity, especially in data management and expertise — both of which directly shape the network. (R16)

These differences reflect the coordination challenges across governance levels (Table 1), where uneven infrastructures and expertise constrain adaptation capacity. Regional governance capacity shapes digital resilience: while some regions integrate emerging technologies, others rely on outdated systems, increasing vulnerability to disruptions.

Beyond infrastructure disparities, governance structures shape digital resilience. Regions with well-coordinated governance networks and integrated digital strategies exhibit greater adaptability to crises, whereas fragmented governance environments struggle to implement cohesive digital policies.

In particular, the misalignment between administrative levels and agencies hampers the efficient deployment of digital solutions. A respondent from an SME operating in international markets highlighted the challenges created by governance fragmentation:

> At the [–] level, working with individuals is straightforward, but when you factor in the systemic aspects, such as the overhaul of administrative systems, things become unnecessarily complicated, sometimes even deliberately so. (R2)

Similar tensions were observed internationally, where the integration of local knowledge and digital tools into centralised strategies remains fragmented (R34). These coordination problems weaken digital resilience by creating inconsistencies in digital tool deployment and policy implementation. Fragmented governance structures and inconsistencies between administrative levels create delays in the implementation of digital resilience strategies.

Nevertheless, the respondents highlighted that the Team Finland network provides an essential framework for structuring strategic foresight and aligning regional and national priorities. Through collaborative planning processes, the network facilitates the early identification of emerging transitions, sustainability goals, and security concerns. A public actor emphasised how this shared agenda-setting accelerates adaptation and improves network-wide responsiveness:

> Within the network, we create local strategic plans in which these transitions are collectively addressed — digitalisation, the green transition, and security. [–] This process embeds these themes into joint operations rather than leaving them to individual organisations. While network-based implementation can take longer due to organisational differences, it ultimately accelerates adaptation by fostering a shared understanding and improving coordination. (R33)

In practice, this fragmentation manifests in inconsistent digital support structures, where some regions have access to streamlined market-entry mechanisms while others lack coordinated digital facilitation. This disparity means that companies in digitally advanced regions benefit from integrated tools and governmental support, whereas firms in less developed digital environments suffer from limited digital infrastructure and a lack of tailored guidance on international expansion. Without structured cooperation between governance levels, these discrepancies could reinforce regional inequalities in digital resilience.

Additionally, digital literacy and cybersecurity preparedness play a vital role in enhancing digital resilience. The interview data underscores concerns about the preparedness levels in different sectors, particularly among SMEs and regional governance structures.

Governance actors often frame cybersecurity as a systemic concern, whereas non-governmental organisation representatives underscore specific vulnerabilities businesses face in practice. One respondent noted that companies often assume cloud-based systems provide sufficient security, without considering contingency measures:

> In our organisation, we actively discuss supply chains and dependencies with businesses — are they too reliant on a single supplier or a specific logistics route? Recently, the security perspective has become increasingly important. Companies don't always prepare for worst-case scenarios. I was quite concerned when, in one discussion, a company's customer records and critical business data were stored only in the cloud — if these disappeared, they would have nothing. Contingency planning is often taken for granted, but systematic investments in it are lacking. (R11)

These findings reveal a dual challenge: while national-level digital infrastructure may be robust, regional and organisational vulnerabilities persist, particularly in sectors that have not traditionally prioritised cybersecurity. The data suggest that improving digital literacy across different governance and business sectors is essential for enhancing digital resilience.

Moreover, discrepancies in cybersecurity preparedness persist across governance and business sectors. As one respondent emphasised:

> Being cyber-resilient is already a selling point today [. . .]. However, at the organisational or SME level, I'm not sure how truly cyber-resilient we are. (R34)

The respondents further warned that a lack of incentives would leave SMEs and local governance structures exposed to evolving digital threats, highlighting the need for cybersecurity strategies that integrate governance and business actors.

The findings indicate that digital resilience is shaped by regional disparities in infrastructure, governance coordination, and cybersecurity preparedness, resulting in uneven capacities to withstand and adapt to digital disruptions.

Hybrid threats and economic vulnerabilities

Disinformation and information warfare threaten transparency in decision-making and institutional credibility. As one respondent described:

> Narrative warfare — whether it is about 'denazification' or the idea that Western sanctions are the reason the world is starving. (R20)

The respondents highlighted the key role of official channels in countering these campaigns that seek to redefine geopolitical realities and erode trust in institutions. As one governance actor noted:

> Business Finland and the Ministry for Foreign Affairs have played a key role in sharing information and forming an overall understanding of how the operating environment is changing. (R25)

SMEs also valued the network as a source of otherwise inaccessible expertise:

> Country-specific knowledge is practically very difficult to obtain from elsewhere. (R6)

These insights show how governance networks strengthen legitimacy by providing credible information and trusted local knowledge and foresight on risks.

These uncertainties reshape global value chains, compelling businesses and governance structures to reassess dependencies, regulatory risks, and market positioning. One respondent emphasised that companies are now required to assess which partners they can safely engage with, while another highlighted how political risks have already reshaped global market positions, with some firms benefiting from shifting alliances:

> Some technology firms have been excluded from key markets, whereas others have found new market opportunities due to shifting geopolitical alliances. Political risks and the broader global environment are now deeply interconnected. (R24)

This illustrates how businesses have become active participants in shifting geopolitical alliances. Policy mechanisms must offer adaptive regulatory frameworks to help businesses navigate a kind of fragmented economic order. Governance resilience in this context requires scenario-based risk assessments, ensuring that both policymakers and businesses have structured frameworks for adapting to the rapidly shifting geopolitical realities.

The digital dependencies and supply chain fragility further complicate resilience-building. Global reliance on key raw materials, microchips, and digital infrastructures creates structural vulnerabilities, making supply chains highly susceptible to external disruptions. A business respondent emphasised how these uncertainties shape investment decisions:

> Supply chains and the challenges related to them are currently among the most significant uncertainties. Investments are being delayed because it is unclear how materials will move and what the global political impacts on supply chains will be. (R3)

This reflects how geopolitical shifts and evolving trade regulations directly affect supply chain security. The increasing weaponisation of trade policies and technological decoupling force businesses to reconsider their operational resilience. Companies must navigate evolving standards and export regulations, which further complicate long-term planning and risk management.

In this context, ensuring policy coherence and strategic foresight remains challenging. To maintain economic stability, policy frameworks must foster structured collaboration between public organisations and private actors in supply chain risk management. Institutionalised preparedness frameworks, including resilience audits and scenario-based adaptation strategies, are essential for safeguarding supply chain continuity.

These findings highlight governance networks' critical role in mitigating hybrid threats and economic vulnerabilities.

Networked governance and digital sovereignty

As governance structures become increasingly digitalised, networks must adjust how they coordinate, share knowledge, and respond to disruptions. Although digital coordination tools create opportunities for strategic alignment, their effectiveness depends on integration into governance frameworks.

A public official emphasised that while digital tools create new opportunities, they do not inherently resolve the complexities of network coordination:

> The strength of the network lies in its strategic goals and the ability to align them with organisational objectives. Clarity, communication with businesses, and integrating regional partners into the broader

> structure are critical. However, coordination is not always straightforward; it involves multiple ministries and departments, each with its own processes and objectives. (R25)

This highlights that while digital coordination mechanisms can enhance operational efficiency, their effectiveness is contingent on clear strategic alignment. Fragmented governance structures may hinder collaboration, particularly when actors operate in separate administrative silos.

Another respondent noted that inconsistent data exchange remains a challenge:

> Within the network, different actors have various strengths. Some are relatively easy to approach, while others are more challenging. Information sharing is key, yet in practice, a lack of seamless data exchange can create inefficiencies and friction. (R10)

Despite efforts to streamline operations, these structural barriers lead to inconsistencies in decision-making and limit adaptability. As another respondent pointed out:

> Data-driven management must be further developed; it is a prerequisite for responsiveness and adaptability. Too often, decisions rely on intuition rather than structured insights. (R15)

These insights underscore the evolving role of digital infrastructures in governance. Digital governance depends on effectively using data for decision-making. Without structured mechanisms to do so, governance networks risk fragmentation, ultimately weakening their capacity to respond to rapid changes.

Digital coordination mechanisms present both opportunities and challenges. While they can improve governance efficiency, they reveal tensions between technological capabilities and institutional realities. Bridging this gap requires a data-driven governance model that fosters transparency, adaptability, and cross-sectoral collaboration.

In today's world, governments must treat data governance and technological dependencies as strategic imperatives, balancing open markets with national and regional security to establish new digital regulatory frameworks.

One interviewee highlighted the growing complexity of today's environment, particularly in relation to global partnerships and technological competition:

> What are our global strengths, and where is the demand for them? And with which countries can we dare to cooperate in this global technology competition? (R25)

This statement underscores the dilemma faced by national and regional actors as they seek to engage in international collaboration without compromising strategic autonomy. Regulatory fragmentation, where major economic blocs implement divergent technological standards, further complicates decision-making. In particular, small highly digitalised economies, must comply with evolving regulations and position themselves within shifting global alliances to maintain technological resilience.

Another respondent underscored cybersecurity as a major concern for smaller states:

> Cybersecurity is the biggest emerging security threat for small nations. (R34)

This insight highlights how digital regulation and national security are increasingly intertwined. Beyond risk management, regulatory frameworks serve as proactive tools for economic positioning. As one interviewee noted, regions with sensitive technological assets face unique pressures:

> There are specific sensitivities in this region, such as the need to safeguard technology. (R30)

This observation reflects that digital sovereignty also involves mitigating external dependencies and leveraging technological capabilities. Regulatory approaches must address domestic priorities and external geopolitical pressures.

Hence, networked governance should balance regulatory adaptability with long-term stability. The respondents emphasised that digital sovereignty drives economic and technological competitiveness, enabling actors to shape digital futures more autonomously. Additionally, the respondents called for proactive governance mechanisms to anticipate risks, manage dependencies, and support regional autonomy through strategic positioning.

In networked governance, integrating private sector insights into policy frameworks is essential for enhancing digital resilience. Public-private collaboration actively shapes long-term strategic trajectories. The effectiveness of governance networks in supporting businesses, particularly SMEs, depends on how well they facilitate structured dialogue, foster partnerships, and align with industry needs.

One business respondent highlighted the role of companies as the primary drivers of economic transformation:

> The role of businesses is fundamental, whereas the public sector has its own limited sphere of influence. In practice, businesses create new pathways, jobs, and opportunities. (R3)

While businesses drive resilience and innovation, governance networks provide policy direction, funding mechanisms, and a stable framework for long-term transformation. This dynamic illustrates the complementary roles of public and private actors in sustaining economic and regional development. Effective governance systems enable transformation through open communication and adaptive support mechanisms rather than rigid structures.

Another business respondent highlighted the practical value of structured public-private engagement, particularly in fostering direct communication between governance actors and businesses:

> I would appreciate more joint meetings within the Team Finland network. [. . .] We had one such event in our region, and it led to many productive initiatives. (R4)

This observation highlights that while governance networks offer structured support, their impact is amplified when businesses have direct access to decision-makers. The ability to exchange insights, align strategies, and co-develop solutions ensures that governance structures remain responsive.

A governance respondent further emphasised that resilience-building extends beyond businesses and requires contributions from research institutions and policy actors, particularly in the context of digital transformation:

> This is a joint effort [. . .] companies, universities, research institutions, and public actors all play a role. (R24)

This underscores that resilience is built at the intersection of public, private, and academic collaboration. Public sector initiatives provide policy direction, regulatory stability, and funding mechanisms, while private sector actors translate these frameworks into tangible innovations and economic activity.

Effective public-private collaboration relies on structured engagement, clear regulations, and direct communication channels. When these elements align, governance networks enhance digital resilience through adaptive policies. Crucially, these challenges are deeply interconnected: digital divides hinder multi-level governance coordination, which in turn undermines the consistent implementation of cybersecurity practices, thereby producing uneven resilience outcomes across regions and sectors.

Overall, the findings reveal three interrelated yet analytically distinct dimensions of governance resilience (Table 2). First, digital resilience is shaped by uneven infrastructures, coordination challenges, and gaps in cybersecurity capacity. Second, hybrid threats and economic vulnerabilities expose governance actors and firms to systemic risks across markets and supply chains. Third, networked governance and digital sovereignty highlight both opportunities and tensions in data governance, regulation, and public–private collaboration.

Table 2. Governance resilience in the digital age

Main Category	Subcategory	Description
Digital Resilience and Multi-Level Governance	Regional Digital Divides	Uneven access to digital infrastructure and technology, leading to disparities in governance resilience across regions.
	Governance and Coordination Challenges	Fragmented governance structures hinder the efficient implementation of digital resilience strategies.
	Digital Competence and Cybersecurity Gaps	Variations in digital competence and cybersecurity awareness impact governance actors and businesses differently.
Hybrid Threats and Economic Vulnerabilities	Disinformation and Governance Legitimacy	The role of information warfare in undermining governance stability, institutional trust, and strategic foresight.
	Geopolitical Risks and Market Uncertainty	Increased economic and political polarisation forces businesses and governance actors to reassess strategic dependencies.
	Territorial Supply Chain Risks	Vulnerabilities in supply chain resilience due to external shocks, trade restrictions, and technological dependencies.
Networked Governance and Digital Sovereignty	Data-Driven Decision-Making and Institutional Alignment	The role of data governance, interoperability, and cross-sectoral coordination in governance resilience.
	Regulatory Fragmentation and Digital Sovereignty	Tensions between regulatory adaptability and digital sovereignty impact governance coherence and market stability.
	Public-Private Collaboration in Digital Resilience	Public-private partnerships to strengthen digital resilience and cybersecurity strategies.

Source: By author

Discussion

This study explored how governance networks adapt to digital transformation and hybrid threats through multi-level coordination and cross-sector collaboration. The findings indicate digital governance is marked by three interrelated challenges: uneven infrastructures and capacities, vulnerabilities from hybrid threats and economic dependencies, and tensions between regulatory adaptability and digital sovereignty. Hence, governance resilience depends not only on institutional coordination and regulatory adaptability, but also on anticipating systemic risks across digital, economic, and geopolitical domains.

The Finnish case, as a small, export-dependent, and highly digitalised economy, underscores the heightened vulnerability to hybrid threats and reliance on international coordination faced by small economies, offering broader insights for similar states.

Specifically, this study shows how regional digital disparities constrain the resilience of internationalisation services, an aspect overlooked in resilience studies, particularly with regard to their role in supporting SMEs. In practice, uneven access to digital infrastructure and expertise means that Team Finland's support mechanisms function effectively in some regions but remain weak or inaccessible in others, demonstrating how gaps in digital capacity translate into uneven business resilience. Additionally, the findings highlight a critical gap: while effective in facilitating economic collaboration, governance networks such as Team Finland lack the means to address hybrid threats, necessitating new coordination mechanisms that integrate security concerns alongside traditional economic support.

The results indicate that governance resilience is deeply linked to multi-level governance structures. Effective digital adaptation relies not only on technological capacity but also on well-coordinated governance mechanisms across national, regional, and international levels.

These findings align with those of Hooghe and Marks (2003) and Geels (2018). However, disparities in digital infrastructure and governance capacity reinforce existing regional inequalities, creating uneven resilience landscapes. This is consistent with Martin and Sunley's (2020) work on regional resilience, which demonstrates how differences in institutional capacity and policy environments can reinforce disparities in resilience outcomes across regions.

Furthermore, digital governance strategies must be embedded within governance frameworks that reflect both intra-national regional dynamics and the institutional diversity of international operating environments. In fragmented governance structures, digital transformation efforts remain reactive rather than proactive, limiting strategic foresight and weakening long-term resilience. Building on Martin and Sunley's (2020) framework, this study suggests that digital resilience is shaped by the quality of multi-level coordination and the ability of governance systems to align regulatory practices across levels. Regulatory inconsistencies can hinder institutional adaptation, highlighting the need for coherence across governance frameworks. Similarly, fragmented compliance requirements in critical mineral supply chains limit traceability and weaken coordinated governance (Bhamra *et al.*, 2025).

The increasing interconnection between digital vulnerabilities, economic security, and geopolitical risks presents a fundamental challenge for governance networks. Hybrid threats have redefined the resilience landscape, often outpacing governance actors' ability to develop proactive mitigation strategies. While governance frameworks incorporate cybersecurity regulations, their effectiveness is undermined by fragmented regulatory approaches and insufficient coordination across governance levels.

This requires integrated policy responses to address economic dependencies (Baldwin and Evenett, 2020) and regulatory coherence that embeds hybrid threat mitigation within broader governance frameworks. Public-private collaboration emerges as a crucial factor in governance resilience. Governance networks that effectively integrate private-sector expertise into resilience-building efforts exhibit greater adaptability and responsiveness. However, regulatory fragmentation and uneven digital capacities continue to hinder cross-sector collaboration, particularly in cybersecurity.

These results reinforce the conclusions of Ansell and Gash (2008) and Baldwin and Evenett (2020), who highlight structured engagement mechanisms as essential for cross-sectoral governance. This study extends the discussion by demonstrating that governance resilience is most effective when public-private collaboration is institutionalised. Intermediary institutions enhance regulatory alignment, knowledge exchange, and investment in digital infrastructure, supporting Klijn and Koppenjan (2016) and Rhodes' (1996) arguments regarding networked governance.

This study identifies governance networks as facilitators of resilience. The findings indicate that governance actors must balance competing priorities while ensuring that digital infrastructure investments and cybersecurity measures do not exacerbate existing inequalities. Institutionalised public-private collaboration emerges as a critical mechanism for enhancing governance adaptability, as it strengthens strategic responsiveness in digital and economic security frameworks. However, persistent governance gaps continue to hinder cross-sector cooperation, resulting in delayed risk responses and uneven resilience outcomes.

This study refines governance resilience theory by demonstrating how insights from multi-level governance, digital sovereignty, and hybrid threat mitigation inform resilience in economic governance networks. Building upon previous studies (Hooghe and Marks, 2003; Boin *et al.*, 2021), it illustrates that governance resilience is shaped by institutional coordination and digital ecosystems' structural constraints (Farrand and Carrapico, 2022). Additionally, this study refines the role of public-private collaboration in governance resilience, demonstrating that adaptive policymaking depends on sustained engagement rather than short-term partnerships.

This study advances resilience research by identifying two underexplored dimensions within export-oriented economic governance networks: how regional digital disparities constrain the resilience of internationalisation services and the need for new governance coordination mechanisms to address hybrid threats. Moreover, it underscores how digital sovereignty tensions and regulatory fragmentation hinder the long-term adaptability of governance networks. These findings answer the three research questions by showing that resilience is shaped by systemic vulnerabilities, adaptive practices across governance levels, and the uneven effectiveness of coordination mechanisms.

Conclusion

Based on the above findings, three priorities stand out for policymakers and practitioners. First, bridging regional digital divides requires aligning transformation strategies with uneven capacities and ensuring that internationalisation services remain accessible across all regions. Second, governance networks must develop coordination mechanisms for hybrid threats, particularly cybersecurity preparedness and disinformation, alongside traditional economic collaboration. Third, institutionalising long-term public–private collaboration is essential for strengthening resilience. Finally, fostering regulatory coherence across governance levels will help avoid fragmented responses and enhance adaptability amid rapid technological and geopolitical change.

The qualitative, Finland-focused design constrains generalisability, underscoring the value of broader comparative analyses. Future research should examine how emerging technologies, such as artificial intelligence, reshape governance resilience strategies, how regional digital disparities affect resilience in other small, highly digitalised economies, and how governance networks address hybrid threats in practice.

About the author
Jukka Keinänen is a doctoral researcher at the School of Management, University of Vaasa, Vaasa, Finland. He holds a Master of Administrative Sciences. His research interests include governance networks, regional and organisational resilience, crisis management, digital governance, and SME internationalisation.

Acknowledgments
I would like to thank the interviewees for their valuable contributions and the reviewers for their constructive feedback.

References

Ansell, C. and Gash, A. (2008), “Collaborative governance in theory and practice”, *Journal of Public Administration Research and Theory,* Vol. 18 No. 4, pp. 543-571.

Ansell, C., Sørensen, E. and Torfing, J. (2021), “The COVID-19 pandemic as a game changer for public administration and leadership? The need for robust governance responses to turbulent problems”, *Public Management Review,* Vol. 23 No. 7, pp. 949-960.

Baldwin, R. and Evenett, S.J. (Eds.) (2020), *COVID-19 and Trade Policy: Why Turning Inward Won’t Work*, CEPR Press, London.

Bhamra, R., Small, A., Hicks, C. and Pilch, O. (2025), “Impact pathways: geopolitics, risk and ethics in critical minerals supply chains”, *International Journal of Operations & Production Management,* Vol. 45 No. 5, pp. 985-994.

Boin, A., Ekengren, M. and Rhinard, M. (2020), “Hiding in plain sight: conceptualizing the creeping crisis”, *Risk, Hazards and Crisis in Public Policy,* Vol. 11 No. 2, pp. 116-138.

Boin, A., McConnell, A. and ’t Hart, P. (2021), *Governing the Pandemic: The Politics of Navigating a Mega-crisis*, Springer International Publishing, Cham.

Boin, A. and Rhinard, M. (2022), “Crisis management performance and the European Union: the case of COVID-19”, *Journal of European Public Policy,* Vol. 30 No. 4, pp. 655-675.

Braun, V. and Clarke, V. (2021), *Thematic Analysis: A Practical Guide*, SAGE Publications, London.

Christensen, T. and Lægreid, P. (2020), "Balancing governance capacity and legitimacy: how the Norwegian government handled the COVID-19 crisis as a high performer", *Public Administration Review*, Vol. 80 No. 5, pp. 774-779.

Creswell, J.W. and Poth, C.N. (2018), *Qualitative Inquiry and Research Design: Choosing among Five Approaches*, Sage Publications, Thousand Oaks, CA.

Dunleavy, P., Margetts, H., Bastow, S. and Tinkler, J. (2006), "New public management is dead —long live digital-era governance", *Journal of Public Administration Research and Theory*, Vol. 16 No. 3, pp. 467-494.

Dunn Cavelty, M., Eriksen, C. and Scharte, B. (2023), "Making cyber security more resilient: adding social considerations to technological fixes", *Journal of Risk Research*, Vol. 26 No. 7, pp. 801-814.

Dunn Cavelty, M. and Wenger, A. (2020), "Cybersecurity meets security politics: complex technology, fragmented politics, and networked science", *Contemporary Security Policy*, Vol. 41 No. 1, pp. 5-32.

Farrand, B. and Carrapico, H. (2022), "Digital sovereignty and taking back control: from regulatory capitalism to regulatory mercantilism in EU cybersecurity", *European Security*, Vol. 31 No. 3, pp. 435-453.

Geels, F.W. (2018), "Disruption and low-carbon system transformation: progress and new challenges in socio-technical transitions research and the multi-level perspective", *Energy Research and Social Science*, Vol. 37, pp. 224-231.

Hennink, M.M., Kaiser, B.N. and Marconi, V.C. (2017), "Code saturation versus meaning saturation: how many interviews are enough?", *Qualitative Health Research*, Vol. 27 No. 4, pp. 591-608.

Hooghe, L. and Marks, G. (2003), "Unraveling the central state, but how? Types of multi-level governance", *American Political Science Review*, Vol. 97 No. 2, pp. 233-243.

Keinänen, J. and Luoto, I. (2025), "Contextualizing resilience within a mutable network organization", *Continuity & Resilience Review*, Vol. ahead-of-print No. ahead-of-print, pp. 1-15, doi: 10.1108/CRR-12-2024-0046.

Keinänen, J., Halonen, M. and Luoto, I. (2026), "What can we learn about crisis management in the polycrisis era? Insights from Finland's international public policy network", *International Journal of Public Sector Management*, Vol. 39 No. 1 pp. 80-95.

Klijn, E.H. and Koppenjan, J.F.M. (2016), *Governance Networks in the Public Sector*, Routledge, London.

Linkov, I., Eisenberg, D.A., Plourde, K., Seager, T.P., Allen, J. and Kott, A. (2013), "Resilience metrics for cyber systems", *Environment Systems and Decisions*, Vol. 33 No. 4, pp. 471-476.

Linkov, I. and Trump, B.D. (2019), *The Science and Practice of Resilience*, Springer, Dordrecht.

Mahmood, S., Chadhar, M. and Firmin, S. (2024), "Digital resilience framework for managing crisis: a qualitative study in the higher education and research sector", *Journal of Contingencies and Crisis Management*, Vol. 32 No. 2, pp. 1-17.

Martin, R. and Sunley, P. (2020), "Regional economic resilience: evolution and evaluation", Bristow, G. and Healy, A. (Eds.), *Handbook on Regional Economic Resilience*, Edward Elgar Publishing, Cheltenham, pp. 10-35.

Mizrahi, S., Vigoda-Gadot, E. and Cohen, N. (2021), "How well do they manage a crisis? The government's effectiveness during the COVID-19 pandemic", *Public Administration Review*, Vol. 81 No. 6, pp. 1120-1130.

Morsut, C., Kuran, C., Kruke, B.I., Orru, K. and Hansson, S. (2021), "Linking resilience, vulnerability, social capital and risk awareness for crisis and disaster research", *Journal of Contingencies and Crisis Management*, Vol. 30 No. 2, pp. 137-147.

Noy, C. (2008), "Sampling knowledge: the hermeneutics of snowball sampling in qualitative research", *International Journal of Social Research Methodology*, Vol. 11 No. 4, pp. 327-344.

O'Brien, B.C., Harris, I.B., Beckman, T.J., Reed, D.A. and Cook, D.A. (2014), "Standards for reporting qualitative research: a synthesis of recommendations", *Academic Medicine*, Vol. 89 No. 9, pp. 1245-1251.

OECD (2019), "Good governance for critical infrastructure resilience", available at: https://www.oecd.org/governance/good-governance-for-critical-infrastructure-resilience-02f0e5a0-en.htm (accessed 9 April 2025).

OECD (2025), "Regulatory environment for digital trade", available at: https://www.oecd.org/en/topics/regulatory-environment-for-digital-trade.html (accessed 16 August 2025).

Patton, M.Q. (2002), *Qualitative Research and Evaluation Methods*, Sage Publications, Thousand Oaks, CA.

Provan, K.G. and Kenis, P. (2007), "Modes of network governance: structure, management, and effectiveness", *Journal of Public Administration Research and Theory*, Vol. 18 No. 2, pp. 229-252.

Rhodes, R.A.W. (1996), "The new governance: governing without government", *Political Studies*, Vol. 44 No. 4, pp. 652-667.

Roberts, H. (2024), "Digital sovereignty: concepts, challenges, and implications", *Ethics and Information Technology*, Vol. 26 No. 4, pp. 1-15.

Team Finland (2019), "Team Finland network strategy", available at: https://www.team-finland.fi/4aaf24/siteassets/team-finland-subsite/documentation/team_finland_strategy_2019.pdf (accessed 14 March 2025).

Van Well, L., van der Keur, P., Harjanne, A., Pagneux, E., Perrels, A. and Henriksen, H.J. (2018), "Resilience to natural hazards: an analysis of territorial governance in the Nordic countries", *Environmental Science & Policy*, Vol. 85, pp. 1-9.

World Economic Forum (2017), "Cyber resilience playbook for public-private collaboration", available at: https://www3.weforum.org/docs/WEF_Cyber_Resilience_Playbook.pdf (accessed 19 March 2025).

Yin, R.K. (2018), *Case Study Research and Applications: Design and Methods*, Sage Publications, Thousand Oaks, CA.

Corresponding author
Jukka Keinänen can be contacted at: jukka.keinanen@uwasa.fi