Bridging the Cyber Gap: Mapping Misalignment Between Digital Adoption and Cybersecurity Capacity

Zakariya Belkhamza
Ahmed Bin Mohammed Military College, Doha, Qatar

zbelkhamza@abmmc.edu.qa

Abstract: The rapid pace of digital transformation has revealed a structural asymmetry between technological expansion and protective capabilities. As digital adoption speeds up across economies, cybersecurity frameworks tend to develop more slowly, creating what this paper calls *the cyber gap*: a persistent misalignment between the trajectories of digital adoption and cybersecurity readiness. This gap is not a temporary delay but an institutional condition that arises when digitalisation advances faster than the laws, institutions and technical competencies required to secure it. This imbalance transforms cybersecurity from a discrete technical function into a systemic feature of digital governance. Building on strategic alignment and socio-technical systems theory, this paper introduces the *cyber gap assessment* (CGA), a conceptual framework designed to make this misalignment visible through analysis. CGA considers digital adoption and cybersecurity capacity as parallel yet interdependent trajectories, distinguishing between two complementary dimensions: *level gaps*, which measure the magnitude of divergence at a given time, and *pace gaps*, which capture the difference in their rates of change. Together, these parameters form a two-dimensional diagnostic that indicates whether states are converging or diverging in their capacity to align technological growth with institutional protection. A typology based on this structure identifies four configurations: high adoption/low capacity; low adoption/high capacity; high adoption/high capacity; and low adoption/low capacity. Each configuration reflects a unique sequence of digital reform, institutional design and governance logic. This analysis demonstrates that high level gaps correspond to structural exposure, where digital systems extend beyond protective reach, while sustained pace gaps generate compounding vulnerabilities across cyber-physical sectors such as energy, transport and e-government. Conversely, convergence across both dimensions signals institutional agility and anticipatory governance. By formalising these relationships, CGA reframes cybersecurity capacity as a co-evolving dimension of digital transformation rather than an ex-post control mechanism. This paper concludes that narrowing the cyber gap requires synchronised governance, adaptive regulation, secure-by-design infrastructures and investment in human capital. This study offers policymakers and researchers a reproducible framework to diagnose structural imbalances and align digital ambitions with resilience.

Keywords: Digital transformation, Cybersecurity, National cybersecurity, Cybersecurity capacity, Cyber gap, Digital adoption, Cybersecurity governance

1. Introduction

Digital transformation has become a defining feature of national development strategies. Governments are digitising services, firms are restructuring around data, and societies are becoming more dependent on interconnected digital infrastructures (Mettler et al, 2024). These changes have resulted in significant improvement in efficiency, accessibility and innovation (Xu et al, 2025). However, the rapid expansion of digital systems has not been matched by improvements in cybersecurity capacity, which have created a systemic imbalance that makes vulnerabilities structural rather than incidental (Forscey et al, 2022).

Many studies demonstrate that while governments and firms rapidly digitise, cybersecurity maturity remains formative, with institutional and social constraints inhibiting progress (Creese et al, 2021). Empirical research shows that although digital transformation boosts efficiency and innovation, it also expands the attack surface faster than technical preparedness can adapt (Catal et al, 2023; Saeed et al, 2023; Fan, 2024; Mirzaei, 2024; Balarabe, 2025; Brezavšček & Baggia, 2025).

This paper addresses this persistent misalignment by introducing the concept of the cyber gap, which captures the structural divergence between the pace of digital adoption and the evolution of cybersecurity capacity. Unlike measures of cyber readiness or maturity, the cyber gap emphasises the relational misfit between digital adoption and cybersecurity capacity. A state may advance rapidly in digitalisation yet remain insecure if protective institutions and practices fail to evolve at the same pace. Digital agendas often prioritise adoption while sidelining cybersecurity (Hurel 2022; Stewart, 2023), undermining resilience and trust at the organisational level and generating systemic risks at the national level that adversaries can exploit (Nye, 2022). To address these challenges, this paper pursues two objectives. First, it develops a conceptual framework and typology for understanding the cyber gap as a structural misalignment between digital adoption and cybersecurity capacity. Second, it proposes an operational diagnostic tool – the *cyber gap assessment* (CGA) – that translates this framework into measurable dimensions.

2. Conceptual Foundations

Studies on cybersecurity have long examined the imbalance between digital adoption and cybersecurity capacity through related concepts such as cyber readiness, maturity and resilience (Büyüközkan & Güler, 2025). Cyber readiness refers to the ability of states or organisations to prevent, detect and respond to cyber threats, often evaluated using indices or staged models (Von Solms & Van Niekerk, 2013; Lee et al, 2025). Cyber maturity frameworks conceptualise progression through predefined stages of institutional development, assuming a linear trajectory of improvement in protective capabilities (Brezavšček & Baggia, 2025). Cyber resilience frameworks often emphasise adaptive capacity following incidents, primarily focusing on post-incident response and recovery, with limited attention to proactive alignment or co-evolution (Dupont et al, 2023; Araujo et al, 2024; Teichmann & Sergi, 2025). They do not sufficiently explain how digital adoption can outpace cybersecurity capacity, leaving systemic vulnerabilities unaddressed. Table 1 summarises the primary cybersecurity constructs discussed in this section, highlighting how the cyber gap surpasses existing frameworks of readiness, maturity and resilience.

Table 1: Comparative overview of cybersecurity constructs

Construct	Focus	Approach	Limitation
Cyber readiness	Ability to prevent, detect and respond to cyber threats	Assessed as the absolute level of preparedness through audits or composite indices	Ignores temporal dynamics and pace of digital adoption (Von Solms & Van Niekerk, 2013; International Telecommunication Union, 2021)
Cyber maturity	Staged development of institutions, policies and controls	Evaluated through level-based or staged capability models	Assumes linear, static progression of capacity building (Brezavšček & Baggia, 2025)
Cyber resilience	Capacity to absorb, adapt and recover from cyber incidents	Measured by recovery and continuity outcomes following disruption	Focuses on post-incident adaptation with limited proactive alignment (Dupont et al, 2023; Araujo et al, 2024; Teichmann & Sergi, 2025)
Cyber gap (this study)	Structural misalignment between digital adoption and cybersecurity capacity	Conceptualised as relative divergence between digital adoption and cybersecurity capacity trajectories	

The term *cyber gap* denotes a structural divergence between how fast nations digitise and how effectively they build and sustain cybersecurity capacity. The cyber gap arises from persistent patterns in digital governance, where the pursuit of digital adoption consistently outpaces the development of cybersecurity measures. In this context, the cyber gap is defined as a structural misalignment between two interdependent national trajectories: digital adoption and cybersecurity capacity. Digital adoption refers to the expansion of infrastructures and services such as broadband, e-government, digital payments and digital platforms, which are common benchmarks in digital development (International Telecommunication Union [ITU], 2021; Organisation for Economic Co-operation and Development [OECD], 2023). Cybersecurity capacity refers to the development of laws, institutions, incident response mechanisms, technical standards and a skilled cybersecurity workforce, as reflected in frameworks such as the ITU Global Cybersecurity Index and national capacity-building models (ITU, 2021; Collett et al, 2021; Lee et al, 2025). Instead of focusing on inequality in access or competence, the cyber gap highlights a relational imbalance that can also leave digitally advanced countries vulnerable to systemic threats.

Empirical evidence supports this observation. Mettler et al (2024) show that national digital-transformation policies evolve unevenly across infrastructural and governance sectors, while cybersecurity frameworks frequently lag behind the expansion of digital services, particularly in emerging economies. The ITU Global Cybersecurity Index (2021) demonstrates that high levels of digital adoption do not always match high cybersecurity capacity, revealing a persistent decoupling between technological diffusion and institutional preparedness.

As Craigen et al (2014) argued earlier, the dominance of a technical view of cybersecurity has constrained its development, limiting interdisciplinary integration across technological, organisational and policy areas. This helps explain why cybersecurity capacity often evolves reactively within broader digital-transformation efforts. In this context, the cyber gap redefines cybersecurity as a dynamic misalignment rather than a static deficit of capacity.

While the concept of the cyber gap explains why divergence emerges, its distribution across countries is highly uneven. Some states advance rapidly in digital adoption but lag behind in security, whereas others prioritise cybersecurity at the expense of innovation and digital progress. These contrasting trajectories underscore the need for a systematic way to classify how adoption and capacity interact in practice.

3. Mapping the Cyber Gap: A Conceptual Typology

Although the typology is conceptual, similar patterns can be observed in global indicators such as the ITU Global Cybersecurity Index (2021) and the United Nations E-Government Development Index (2022), which together reveal how states differ in digital progress and their ability to secure it. By mapping these configurations, the typology explains how different national trajectories of digitalisation and cybersecurity capacity produce distinct vulnerability profiles. Such typological reasoning has long been used to identify structural patterns that quantitative metrics alone might miss (Doty & Glick, 1994; Elman, 2005). This section proposes a typology with four categories, offering a conceptual framework for comparative analysis.

3.1 High Digital Adoption/low Cybersecurity Capacity

The first quadrant represents the archetypal expression of the cyber gap. States in this quadrant undergo rapid digitalisation through expanded digital transformation efforts, such as e-government platforms, fintech ecosystems and data-driven public services, while their cybersecurity institutions remain comparatively underdeveloped. Political and economic incentives to modernise often drive technological deployment faster than governance reforms can keep pace with, resulting in a systemic misfit between two interdependent trajectories: technological expansion and capacity building (Pérez-Nordtvedt et al, 2008).

The technical layer of transformation, such as networks, platforms and applications, can scale rapidly, whereas the corresponding layers of policy design, enforcement and professional expertise evolve more slowly (Ansari & Garud, 2009). This generates governance lag as digital infrastructures expand while the rules, safeguards and human capabilities required to protect them remain incomplete (Őri & Szabó, 2024). Cybersecurity capacity does not erode through neglect but through asymmetric modernisation, a condition where innovation progresses faster than governance can stabilise (Thierer, 2018).

3.2 Low Digital Adoption/High Cybersecurity Capacity

At the opposite end of the spectrum are states that prioritise cybersecurity over digital expansion. They establish legal frameworks and specialised agencies early in their development, creating a governance structure focused on caution and control (ITU, 2021). This sequencing typically emerges in states with strong administrative traditions and centralised governance, where they value policy consistency more than rapid market experimentation. While this approach improves state preparedness, it also embeds caution – a core principle of digitalisation – that influences how innovation is subsequently authorised and scaled.

Institutional and protective capacity outpace innovation, creating rigidity rather than fragility as controls harden faster than use cases mature (Henderson & Venkatraman, 1993). Before the deployment of new technologies, rigorous compliance, risk assessment and security certification procedures often slow down adoption cycles. While these mechanisms improve reliability and reduce exposure, they hinder iterative experimentation. Past studies explain that formalising processes and controls enhances reliability but restricts exploratory activities, thereby reducing innovative change (Benner & Tushman, 2003; Cinar et al, 2022). Gradually, such environments cultivate risk aversion, causing organisations and public agencies to prioritise compliance over innovation. This imbalance delays the spread of digital services, constrains cross-sector collaboration, reduces flexibility and hampers adaptive learning. Consequently, exposure to external threats is lessened, but experimentation slows and digital transformation falls behind (Nelson & Madnick, 2017; Heierhoff & Hoffmann, 2022). However, recent empirical research shows a similar pattern: increased cybersecurity risks and precautions are associated with lower innovation intensity, underscoring the stability–agility trade-off at the core of this dynamic (Wang, Ho & Shan, 2024).

3.3 High Digital Adoption/High Cybersecurity Capacity

The third quadrant represents the closest alignment between digital adoption and cybersecurity capacity. States in this category integrate cybersecurity capacity as a core element of digital transformation rather than as a subsequent correction. Policy coordination, education systems and regulatory oversight develop alongside technological infrastructure, producing a dynamic equilibrium: the continuous co-adaptation of technical, institutional and human subsystems (Geels, 2002; OECD, 2023). In this quadrant, governance structures

proactively address risks instead of reacting to them, integrating cybersecurity principles into every stage of digital service design. Consequently, national strategies treat resilience as a capacity that evolves with technological ecosystems.

This category illustrates coherence across multiple levels of governance. Strategic intent, operational processes and technical capabilities are synchronised, reducing the gap between innovation and cybersecurity capacity (Henderson & Venkatraman, 1993; Chan & Reich, 2007). As digital services expand, cybersecurity frameworks mature in tandem, ensuring that both trajectories remain balanced over time (ENISA, 2020; National Institute of Standards and Technology [NIST], 2024).

However, this balance is dynamic rather than static. As digitalisation accelerates, maintaining alignment requires continuous adaptation and institutional agility, a capacity reflected in both national policy frameworks and international governance models (Teece, 2007; OECD, 2023; NIST, 2024). Therefore, the real marker of maturity in this quadrant is not the initial achievement of balance, but the ability to sustain and recalibrate it amid technological and organisational change. High adoption and high capacity do not eliminate the cyber gap but transform it into an ongoing challenge of governance, vigilance and renewal.

3.4 Low Digital Adoption/low Cybersecurity Capacity

This category describes states that remain at early stages of both digitalisation and cybersecurity development. Limited fiscal resources, institutional fragility and dependence on external technology providers constrain progress across both domains (Hurel, 2022). The cyber gap here is latent until digitalisation begins to accelerate.

In the short term, these countries appear less exposed because their digital footprint is small. However, this limited exposure can hide deep structural vulnerabilities, as underlying weaknesses in institutional design, education systems and digital infrastructure remain concealed beneath low connectivity rates. As digital adoption expands, often through e-government projects or imported platforms for finance, education or public administration, their cybersecurity capacity rarely scales at the same rate. Legal frameworks, enforcement mechanisms and skilled human resources tend to lag, leaving new systems dependent on external expertise and inconsistent regulatory protections (Collett, 2021; Hurel, 2022).

States with a dual constraint of low technological adoption and minimal cybersecurity readiness possess limited institutional capacity, which may postpone the emergence of the cyber gap but ultimately exposes a deferred vulnerability. Preventing this requires anticipatory governance that invests early in legal and institutional foundations, enabling cybersecurity capacity to evolve alongside future digital growth (OECD, 2023).

These four quadrants map the structural diversity of national manifestations of the cyber gap, capturing how states differ in sequencing, governance priorities and institutional adaptability. The typology demonstrates that imbalance is a relational condition arising from sequencing reforms, the design of institutions and the logic of governance that either links or decouples adoption from cybersecurity capacity. By translating the abstract notion of the cyber gap into these distinct national trajectories, the typology offers a comparative lens through which policymakers and scholars can diagnose how well the two trajectories co-evolve. The following section expands on this typology by exploring methods to measure and compare the cyber gap among states through the use of composite indicators and dynamic alignment metrics.

4. Conceptual Operationalisation of CGA

To make contrasts analytically usable, this paper introduces CGA as a conceptual diagnostic. Treating the two constructs of digital adoption and cybersecurity capacity as parallel but interdependent trajectories allows for a relational expression of the cyber gap rather than viewing it as an absolute measure. In practice, increased adoption may stimulate protective investments, while improved capacity can accelerate further adoption. However, for diagnostic clarity, this assessment treats them as analytically separate but empirically interdependent.

CGA distinguishes between two complementary dimensions:

- **Level gap (GL):** This represents the relative position of digital adoption and cybersecurity capacity at a given time.
- **Pace gap (GD):** This represents the difference in the year-on-year growth rates of digital adoption and cybersecurity capacity.

These two parameters form a two-dimensional vector (GL, GD) capturing both state and momentum. A positive GL indicates that adoption is ahead of capacity, while a positive GD shows that adoption is accelerating faster than capacity, as previously explained. This vector approach avoids reducing multidimensional complexity into a single composite score (Saisana, Saltelli & Tarantola, 2005) and instead offers a diagnostic view of relative trajectories.

Conceptually, CGA functions as a lens rather than a scorecard. Its diagnostic value lies in revealing where imbalance occurs and how it evolves while remaining modular across different indicator sets and country contexts (Creese et al, 2021). In policy terms, it bridges the typology and the pathways that follow: CGA bands map directly onto regulatory levers, secure-by-design policies, workforce development, operational readiness and international cooperation. By emphasising the parallel development of adoption and capacity, the CGA reinforces the principle of anticipatory governance, encouraging states to scale protective capacity before vulnerabilities mature into systemic risk (Collett et al, 2021).

Table 2: Conceptual components of CGA

Component	Description
Digital adoption (A)	Trajectory of digital infrastructures and services (e.g. broadband, e-government, digital payments)
Cybersecurity capacity (P)	Trajectory of cybersecurity capacity (e.g. laws, computer emergency response teams, standards, workforce, governance)
Level gap (GL)	Relative position of digital adoption versus cybersecurity capacity at a given time
Pace gap (GD)	Difference in year-on-year growth of digital adoption and cybersecurity capacity
Vector form	CGA = (GL, GD) captures both state and momentum.
Decision bands	Surge risk, security drag and convergence (based on persistence over multiple years)
Purpose	Diagnostic tool to link typology to institutional drivers and policy levers

5. Mathematical Representation of CGA

This formalisation follows established practices in composite-indicator design and enables a reproducible way to quantify the relative trajectories of digital adoption and cybersecurity capacity across states.

Let:

- $\mathrm{A}_{i,t}^{A}$ = digital adoption score for country *i* at time *t,*
- $\mathrm{P}_{i,t}^{A}$ = cybersecurity capacity score for country *i* at time *t.*

Because these indicators are heterogeneous in scale and distribution, they are standardised using a per-year z-score transformation (OECD & JRC, 2008):

$$\mathrm{z}_{i,t}^{A} = \frac{\mathrm{A}_{i,t} - \mu_t^{A}}{\sigma_t^{A}}, \mathrm{z}_{i,t}^{P} = \frac{\mathrm{P}_{i,t} - \mu_t^{P}}{\sigma_t^{P}},$$

where μ_t and σ_t represent the cross-sectional mean and standard deviation across all countries in year t. The level gap captures the static divergence between digital adoption and cybersecurity capacity:

$$\mathrm{G}_{i,t}^{L} = z_{i,t}^{A} - z_{i,t}^{P}.$$

A positive $G_{i,t}^{L}$ indicates that digital adoption exceeds cybersecurity capacity (structural exposure), while a negative value reflects a security-first orientation where cybersecurity capacity leads digital adoption.

The pace gap captures the dynamic divergence in year-on-year change:

$$\mathrm{G}_{i,t}^{D} = \left(\mathrm{z}_{i,t}^{A} - \mathrm{z}_{i,t-1}^{A}\right) - \left(\mathrm{z}_{i,t}^{P} - \mathrm{z}_{i,t-1}^{P}\right),$$

where a positive $G_{i,t}^{D}$ signals that digital adoption is accelerating faster than cybersecurity capacity. Both components together yield a relational representation of the cyber gap over time. To minimise volatility from single-year fluctuations, $G_{i,t}^{D}$ can be smoothed using a multi-year moving average (Chatfield, 2000). Moreover, country-level indicators may be subject to definitional inconsistencies or data gaps. Smoothing techniques and robustness checks can help mitigate such issues and ensure interpretive stability (Box et al, 2015).

These two components of the gap define the assessment vector:

$$\mathrm{G}_{i,t} = \left(\mathrm{G}_{i,t}^{L}, \mathrm{G}_{i,t}^{D}\right),$$

representing both the static alignment (level) and dynamic momentum (pace) of each country's digital trajectory.

However, the vector form remains the primary analytical lens, as it preserves state and direction, preventing the loss of interpretive richness that comes with aggregation.

- $G^L > 0 \rightarrow$ digital adoption exceeds cybersecurity capacity (*structural exposure*)
- $G^D > 0 \rightarrow$ digital adoption accelerates faster than cybersecurity capacity (*dynamic risk*)
- $G^L \approx 0$ and $G^D \approx 0 \rightarrow$ relative alignment (*convergence*)

By explicitly outlining this relational structure, CGA offers a transparent and replicable foundation for identifying areas of divergence and convergence between digital adoption and cybersecurity capacity, as well as determining where strategic intervention is most needed.

6. Strategic Implications of CGA

CGA demonstrates that misalignment between digital adoption and cybersecurity capacity is not merely conceptual but has systemic consequences. High level gap values reveal digitalisation advancing beyond protective capacity, translating directly into strategic vulnerability. Research on hybrid conflict shows that adversaries exploit weak protective capacity rather than technological inferiority (Hoffman, 2007; Rid, 2012). States with such imbalances are more susceptible to espionage, disruption and disinformation. As Cavelty and Egloff (2019) note, even advanced economies with sophisticated infrastructure remain strategically fragile when governance and enforcement lag.

When the pace gap persists, digital trajectories accelerate faster than protective capacity can adapt, compounding risk across security, infrastructure, trust and international relations. This pattern is particularly acute in cyber-physical domains such as energy grids, transport networks and e-health systems. Moreover, resilience theory warns that vulnerabilities in one subsystem can cascade across others (Perrow, 1999; Linkov et al, 2018). Evidence from ransomware attacks on critical infrastructure confirms how delayed cybersecurity capacity multiplies disruption (Benmalek, 2024). When acceleration continues unchecked, insecure systems become embedded, creating compounding risks and costly retrofits. Therefore, CGA links sustained pace gap trajectories with structural fragility in critical sectors that cannot easily be secured after deployment.

Public trust is central to digital governance. Empirical research shows that data breaches and misuse of information erode confidence, undermining adoption (Ou et al, 2022; Stewart, 2023). Within CGA, high level gap and persistent pace gap values indicate environments where protective institutions lag behind growth. Citizens face insecure e-government services, unprotected digital identities and poorly regulated fintech platforms. Thus, persistent misalignment generates a paradox: the drive for modernisation risks delegitimising the transformation when security fails to converge.

Finally, CGA reveals how divergence and convergence shape states' relative positions in the international system. Convergent states, where level gap and pace gap remain near zero, gain reputational advantages as trusted hubs for digital trade and governance (Madise & Martens, 2006). CGA highlights how structural misalignment crystallises globally, redistributing power along lines of security capacity.

This imbalance transforms cybersecurity from a technical function into a structural condition of digital governance. Bridging the cyber gap requires expanding capacity and sustaining synchronisation to ensure that institutional development keeps up with technological advancements. Hence, CGA is an analytical tool and a diagnostic lens that indicates how nations manage the balance between digital ambition and resilience.

7. Conclusion

This paper introduced the cyber gap as a structural misfit between the trajectories of digital adoption and cybersecurity capacity. Through CGA, the paper reconceptualised national readiness not as a fixed score but as a relational dynamic between two interdependent systems: digital adoption and cybersecurity capacity. The distinction between level gaps and pace gaps reveals how institutional inertia, workforce shortages, governance fragmentation and uneven international cooperation perpetuate imbalance over time. Practically, the paper provides policymakers with a diagnostic lens to locate vulnerabilities, anticipate systemic risks and sequence reforms that align digital expansion with protective capacity. While this study develops the cyber gap assessment

as a conceptual and analytical framework, its full potential will emerge through empirical application. Testing the CGA with multi-year datasets that combine indicators of digital adoption and cybersecurity capacity would enable validation of the typology and calibration of both level and pace gaps across countries. Future research can extend this work by operationalising the framework in comparative analyses to explore regional patterns, temporal dynamics, and the policy effectiveness of interventions aimed at narrowing the cyber gap. Bridging the cyber gap is a matter of governance design, ensuring that each advance in connectivity is matched by an equivalent advance in cybersecurity capacity.

Ethics Declaration: Ethical clearance was not required for this research, as it did not involve human participants, personal data, or experimental procedures. This research is based solely on conceptual analysis and secondary data from publicly available sources.

AI Declaration: No generative artificial intelligence (AI) tools were used in the conception, design, analysis, or writing of this paper. All content was created by the author. Standard software applications were used only for text editing and reference management.

References

Ansari, S. and Garud, R. (2009) 'Inter-generational transitions in socio-technical systems: The case of mobile communications', *Research Policy*, Vol. 38, No. 3, pp 382–392. https://doi.org/10.1016/j.respol.2008.11.009

Araujo, M.S.D., Machado, B.A.S. and Passos, F.U. (2024) 'Resilience in the context of cyber security: A review of the fundamental concepts and relevance', *Applied Sciences*, Vol. 14, No. 5, 2116. https://doi.org/10.3390/app14052116

Balarabe, A. (2025) 'Digital borders and beyond: Establishing normative grounds for cybersecurity and sovereignty in international law', *Computer Law & Security Review*, Vol. 53, 106321. https://doi.org/10.1016/j.clsr.2025.106321

Benmalek, M. (2024) 'Ransomware on cyber-physical systems: Taxonomies, case studies, security gaps, and open challenges', *Internet of Things and Cyber-Physical Systems*, Vol. 4, pp 186–202. https://doi.org/10.1016/j.iotcps.2023.12.001

Benner, M.J. and Tushman, M.L. (2003) 'Exploitation, exploration, and process management: The productivity dilemma revisited', *Academy of Management Review*, Vol. 28, No. 2, pp 238–256. https://doi.org/10.5465/amr.2003.9416096

Box, G.E.P., Jenkins, G.M., Reinsel, G.C. and Ljung, G.M. (2015) *Time Series Analysis: Forecasting and Control*. 5th edn. Hoboken, Wiley, New Jersey.

Brezavšček, A. and Baggia, A. (2025) 'Recent trends in information and cyber security maturity assessment: A systematic literature review', *Systems*, Vol. 13, No. 1, p 52. https://doi.org/10.3390/systems13010052

Büyüközkan, G. and Güler, M. (2025) 'Cybersecurity maturity model: Systematic literature review and a proposed model', *Technological Forecasting and Social Change*, Vol. 213, 123996. https://doi.org/10.1016/j.techfore.2025.123996

Catal, C., Ozcan, A., Donmez, E. and Kasif, A. (2023) 'Analysis of cyber security knowledge gaps based on cyber security body of knowledge', *Education and Information Technologies*, Vol. 28 No. 2, pp 1809–1831. https://doi.org/10.1007/s10639-022-11261-8

Cavelty, M.D. and Egloff, F.J. (2019) 'The politics of cybersecurity: Beyond the technical', *Global Policy*, Vol. 10, No. 3, pp 456–471.

Chan, Y.E. and Reich, B.H. (2007) 'IT alignment: What have we learned?', *Journal of Information Technology*, Vol. 22, No. 4, pp 297–315. https://doi.org/10.1057/palgrave.jit.2000109

Chatfield, C. (2000) *Time-Series Forecasting*. Boca Raton, Chapman & Hall/CRC, Florida.

Cinar, E., Demircioglu, M.A. and Yildiz, M. (2022) 'Public sector innovation in context: A comparative study of innovation types', *Public Management Review*, Vol. 26, No. 1, pp 265–292. https://doi.org/10.1080/14719037.2022.2080860

Collett, R. (2021) 'Understanding cybersecurity capacity building and its relationship to norms and confidence building measures', *Journal of Cyber Policy*, Vol. 6, No. 3, pp 298–317. https://doi.org/10.1080/23738871.2021.1948582

Craigen, D., Diakun-Thibault, N. and Purse, R. (2014) 'Defining cybersecurity', *Technology Innovation Management Review*, Vol. 4, No. 10, pp 13–21. Available at: https://timreview.ca/article/835

Creese, S., Goldsmith, M., Nurse, J.R.C. and Phillips, E. (2021) 'A cybersecurity capacity maturity model: Cross-national insights and lessons learned', *Journal of Cyber Policy*, Vol. 6, No. 3, pp 394–416. https://doi.org/10.1080/23738871.2021.1995811

Doty, D.H. and Glick, W.H. (1994) 'Typologies as a unique form of theory building: Toward improved understanding and modeling', *Academy of Management Review*, Vol. 19, No. 2, pp 230–251.

Dupont, B., Shearing, C., Bernier, M. and Leukfeldt, R. (2023) 'The tensions of cyber-resilience: From sensemaking to practice', *Computers & Security*, Vol. 132, 103372. https://doi.org/10.1016/j.cose.2023.103372

Elman, C. (2005) 'Explanatory typologies in qualitative studies of international politics', *International Organization*, Vol. 59, No. 2, pp 293–326. https://doi.org/10.1017/S0020818305050101

ENISA (European Union Agency for Cybersecurity) (2020) *National Cybersecurity Strategies: Practical Guide on Development and Execution*. Athens: ENISA. Available at: https://www.enisa.europa.eu/publications/national-cyber-security-strategies-toolset

Fan, P. (2024) 'Governance of high-risk technologies: The role of fragmented global regimes', *Global Political Economy*, Vol. 3, No. 2, pp 265–283. https://doi.org/10.1332/263514224X17211200207760

Forscey, D., Bateman, J., Beecroft, N. and Woods, B. (2022) *Systemic Cyber Risk: A Primer*, Carnegie Endowment for International Peace, Washington, DC.

Geels, F.W. (2002) 'Technological transitions as evolutionary reconfiguration processes: A multi-level perspective and a case study', *Research Policy*, Vol. 31, No.8–9, pp 1257–1274. https://doi.org/10.1016/S0048-7333(02)00062-8

Heierhoff, S. and Hoffmann, N. (2022) 'Cyber security vs. digital innovation: A trade-off for logistics companies?', in *Proceedings of the 55th Hawaii International Conference on System Sciences (HICSS)*, pp 6792–6801. Available at: https://hdl.handle.net/10125/80161

Henderson, J.C. and Venkatraman, N. (1993) 'Strategic alignment: Leveraging information technology for transforming organizations', *IBM Systems Journal*, Vol. 32, No. 1, pp 4–16. https://doi.org/10.1147/sj.321.0004

Hoffman, F.G. (2007) *Conflict in the 21st Century: The Rise of Hybrid Wars*, Potomac Institute for Policy Studies, Arlington, Virginia.

Hurel, L.M. (2022) 'Interrogating the cybersecurity development agenda: A critical reflection', *The International Spectator*, Vol. 57, No. 3, pp 66–84. https://doi.org/10.1080/03932729.2022.2095824

International Telecommunication Union (ITU) (2021) *Global Cybersecurity Index (GCI) 2020*. Geneva: ITU. Available at: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

Lee, G., Kim, S., Lee, I., Brown, S. and Carbajal, Y.A. (2025) 'Adapting cybersecurity maturity models for resource-constrained settings: A case study of Peru', *The Electronic Journal of Information Systems in Developing Countries*, Vol. 91, No. 1, e12350. https://doi.org/10.1002/isd2.12350

Linkov, I., Trump, B.D., Poinsatte-Jones, K. and Florin, M.-V. (2018) 'Governance strategies for a sustainable digital world', *Sustainability*, Vol. 10, No. 2, p 440.

Madise, Ü. and Martens, T. (2006) 'E-voting in Estonia 2005: The first practice of legally binding Internet voting in the world', *Electronic Voting in Europe*, pp 15–26.

Mettler, T., Miscione, G., Jacobs, C.D. and Guenduez, A.A. (2024) 'Same same but different: How policies frame societal-level digital transformation', *Government Information Quarterly*, Vol. 41, No. 2, 101932. https://doi.org/10.1016/j.giq.2024.101932

Mirzaei, A. (2024) 'Cybersecurity governance: Fragmentation, coordination, and institutional challenges', *Journal of Cybersecurity*, Vol. 10, No. 1, taae012. https://doi.org/10.1093/cybsec/taae012

National Institute of Standards and Technology (NIST) (2024) *The NIST Cybersecurity Framework (CSF) 2.0*. Gaithersburg, MD: NIST. https://doi.org/10.6028/NIST.CSWP.29

Nelson, N. and Madnick, S. (2017) 'Studying the tension between digital innovation and cybersecurity', in *Proceedings of the 3rd International Conference on Information Systems Security and Privacy (SIGSEC)*, Porto, Portugal, 19–21 February.

Nye, J.S. Jr. (2022) 'Cyber power and the U.S. national security strategy', in Cox, M. and Stokes, D. (eds.) *The Routledge Handbook of U.S. Foreign Policy*. 2nd edn. Abingdon: Routledge, pp. 603–616

Organisation for Economic Co-operation and Development (OECD) (2023) *OECD Policy Framework on Digital Security: Towards Economic and Social Prosperity*, OECD Publishing, Paris. https://doi.org/10.1787/9789264276268-en

OECD and Joint Research Centre (JRC) (2008) *Handbook on Constructing Composite Indicators: Methodology and User Guide,* OECD Publishing, Paris. https://doi.org/10.1787/9789264043466-en

Őri, D. and Szabó, Z. (2024) 'A systematic literature review on business–IT misalignment research', *Information Systems and e-Business Management*, Vol. 22, pp 139–169. https://doi.org/10.1007/s10257-023-00664-w

Ou, C.X., Zhang, X., Angelopoulos, S., Davison, R.M. and Janse, N. (2022) 'Security breaches and organization response strategy: Exploring consumers' threat and coping appraisals', *International Journal of Information Management*, Vol. 65, 102498. https://doi.org/10.1016/j.ijinfomgt.2022.102498

Pérez-Nordtvedt, L., Payne, G.T., Short, J.C. and Kedia, B.L. (2008) 'An entrainment-based model of temporal organizational fit, misfit, and performance', *Organization Science*, Vol. 19, No. 5, pp 785–801.

Perrow, C. (1999) *Normal Accidents: Living with High-Risk Technologies*. 2nd edn. Princeton University Press, Princeton, New Jersey.

Rid, T. (2012) 'Cyber war will not take place', *Journal of Strategic Studies*, Vol. 35, No. 1, pp 5–32.

Saeed, S., Altamimi, S.A., Alkayyal, N.A., Alshehri, E. and Alabbad, D.A. (2023) 'Digital transformation and cybersecurity challenges for business resilience: Issues and recommendations', *Sensors*, Vol. 23, No. 15, 6666. https://doi.org/10.3390/s23156666

Saisana, M., Saltelli, A. and Tarantola, S. (2005) 'Uncertainty and sensitivity analysis techniques as tools for the quality assessment of composite indicators', *Journal of the Royal Statistical Society: Series A (Statistics in Society)*, Vol. 168, No. 2, pp 307–323. https://doi.org/10.1111/j.1467-985X.2005.00350.x

Stewart, H. (2023) 'Digital transformation security challenges', *Journal of Computer Information Systems*, Vol. 63, No. 4, pp 919–936. https://doi.org/10.1080/08874417.2022.2115953

Teece, D.J. (2007) 'Explicating dynamic capabilities: The nature and microfoundations of (sustainable) enterprise performance', *Strategic Management Journal*, Vol. 28, No. 13, pp 1319–1350. https://doi.org/10.1002/smj.640

Teichmann, F. and Sergi, B.S. (2025) 'The EU Cyber Resilience Act: Hybrid governance, compliance, and cybersecurity regulation in the digital ecosystem', *Computer Law & Security Review*, 59, 106209. https://doi.org/10.1016/j.clsr.2025.106209

Thierer, A. (2018) *The Pacing Problem and the Future of Technology Regulation,* Mercatus Center at George Mason University, Arlington, Virginia.

Von Solms, R. and Van Niekerk, J. (2013) 'From information security to cyber security', *Computers & Security*, Vol. 38, pp 97–102. https://doi.org/10.1016/j.cose.2013.04.004

Wang, J., Ho, C.Y. and Shan, Y.G. (2024) 'Does cybersecurity risk stifle corporate innovation activities?', *International Review of Financial Analysis*, Vol. 91, 103028. https://doi.org/10.1016/j.irfa.2023.103028

Xu, Y., Ji, J., Qiao, Y. and Huang, J. (2025) 'How and when does digital transformation promote technological innovation performance? A study of Chinese high-tech firms', *Technovation*, Vol. 146, 103294. https://doi.org/10.1016/j.technovation.2025.103294