

Strategic Management in Security Institutions: Origins, Content, and Impacts of Digital Transformation and Sustainability Strategies: Applied to Study

Lt. Gen (Staff). Amer Saddam Almaliki, Dr. Azzam Khalid Aljashami

Ministry of interior ,Higher Institute for Security and Administrative Development

DOI: 10.37648/ijps.v22i01.005

¹Received: 21/03/2026; Accepted: 10/04/2026; Published: 20/07/2026

Abstract

This study examines strategic management in security institutions in light of the growing importance of digital transformation and sustainability. It explores the origins, content, and strategic impacts of these two approaches and proposes that their integration—supported by strategic leadership, data governance, and cybersecurity—can enhance institutional effectiveness, resilience, decision quality, and service continuity. The study adopts a descriptive-analytical approach. A hypothetical applied model is developed using a sample of 120 leaders, officers, technical personnel, and administrative employees in a hypothetical Iraqi security institution. The simulated results indicate positive effects of digital transformation and sustainability on strategic effectiveness, with an additional positive effect arising from their interaction.

Keywords: *Strategic management; security institutions; digital transformation; sustainability; cybersecurity; organizational resilience.*

1. Research Methodology

1.1 Research Problem

Security institutions operate in highly complex environments characterized by uncertainty, cyber threats, rapidly growing volumes of data, pressure for immediate response, and the need to maintain sustainable human, technological, financial, and operational capabilities. The central research question is: What is the impact of integrating digital transformation and sustainability strategies on the strategic effectiveness of security institutions?

1.2 Research Importance and Objectives

The importance of the study lies in integrating three domains that are often examined separately: strategic management, digital transformation, and sustainability within the context of security institutions. The study aims to establish the conceptual foundations of these domains, identify the major components of digital and sustainability strategies, develop an explanatory model of their relationships, and test that model through a hypothetical empirical scenario.

1.3 Research Hypotheses

¹ *How to cite the article:* Almaliki A.S., Aljashami A.K (July 2026); Strategic Management in Security Institutions: Origins, Content, and Impacts of Digital Transformation and Sustainability Strategies: Applied to Study; *International Journal of Professional Studies*; Jul-Dec 2026, Vol 22, 43-50; DOI: <http://doi.org/10.37648/ijps.v22i01.005>

H1: Digital transformation strategy has a significant positive effect on strategic effectiveness. H2: Sustainability strategy has a significant positive effect on strategic effectiveness. H3: The integration of digital transformation and sustainability has a significant positive effect on strategic effectiveness. H4: Strategic leadership and cybersecurity governance strengthen the effectiveness of digital transformation.

1.4 Method, Population, Sample, and Instrument

The study adopts a descriptive-analytical method. For the application, the population consists of 350 members of an Iraqi security institution, from which a stratified sample of 120 respondents. A 30-item questionnaire using a five-point Likert scale is proposed: digital transformation (10 items), sustainability (8 items), leadership and governance (5 items), and strategic effectiveness (7 items). Reliability is assessed through Cronbach's alpha.

1.5 Boundaries and Statistical Methods

The subject boundaries cover strategic management, digital transformation, and sustainability. The spatial boundary is a Iraqi security institution, while the human boundary includes leaders, officers, technical staff, and administrative personnel. The assumed time boundary is 2026. Statistical techniques include means, standard deviations, Cronbach's alpha, Pearson correlation, and multiple regression. Digital transformation is treated as an organizational and strategic transformation rather than merely technological adoption (Vial, 2019; Verhoef et al., 2021).

Theoretical Framework – Page 1 of 5

2. Strategic Management in Security Institutions: Origins and Specific Characteristics

Strategic management evolved from long-range planning toward an integrated approach to managing resources, capabilities, environmental uncertainty, and strategic choices. Dynamic capabilities theory argues that performance in changing environments depends on the ability to sense opportunities and threats, seize them, and reconfigure resources accordingly (Teece et al., 1997; Teece, 2007). This perspective is especially relevant to security institutions because of uncertainty, information sensitivity, and the need for rapid response.

Digitalization introduced a new dimension to strategy. Information technology is no longer merely a support function but part of strategy formulation and implementation. Bharadwaj et al. (2013) conceptualized digital business strategy as a fusion of business and IT strategy, while Matt et al. (2015) described digital transformation strategy as a central framework for coordinating transformation priorities and initiatives across the organization.

In security institutions, digital strategy should be directly linked to institutional missions such as situational awareness, command and control, risk analysis, incident management, critical-infrastructure protection, resource management, and public services. Transformation therefore requires redesign of processes, structures, skills, and culture rather than the simple acquisition of new systems.

Research on dynamic capabilities for digital transformation emphasizes that digital capability building is a continuing process of strategic renewal involving flexibility, organizational restructuring, collaboration, and cultural change (Warner & Wäger, 2019). Related studies identify practical routines including digital sensing, digital strategy development, decomposition of transformation into projects, and creation of a unified digital backbone (Ellström et al., 2022).

Theoretical Framework – Page 2 of 5**3. Origins and Content of Digital Transformation Strategy**

Digitization, digitalization, and digital transformation represent different levels of change. Digitization converts information from analogue to digital form; digitalization uses technology to improve processes; and digital transformation involves broader changes in value creation, structures, capabilities, and organizational processes (Verhoef et al., 2021). Vial (2019) describes digital transformation as a process through which organizations respond to disruptions caused by digital technologies by altering value-creation paths while managing structural changes and organizational barriers.

Core components of a digital transformation strategy in a security institution include reliable digital infrastructure, integrated databases, analytics and artificial intelligence, process automation, command-and-control platforms, digital identity and access management, information security, digital skills, and data governance. Hanelt et al. (2021) emphasize that digital transformation involves deep strategic and organizational changes whose outcomes depend on context, structures, and capabilities.

Gong and Ribiere (2021) argue that digital transformation goes beyond technology adoption and constitutes fundamental organizational change enabled by digital technologies to create significant value and improvement. This comprehensive view is especially important in security institutions operating critical systems, where integration among technology, people, procedures, and governance is essential.

In the public sector, Mergel et al. (2019) show that digital transformation involves redesigning services, processes, and organizational culture rather than simply converting paper procedures into electronic form. Research on UK policing also suggests that large-scale digital transformation may remain fragmented or uneven when local practices and institutional arrangements are not aligned with the broader strategic direction (Laufs et al., 2024).

Theoretical Framework – Page 3 of 5**4. Cybersecurity and Governance as Conditions for Transformation**

As security institutions become more digital, the value of their data and their exposure to cyber risk increase. Digital transformation therefore cannot be separated from information security and risk management. Evidence indicates that effective information-security management during transformation depends on leadership capabilities and attitudes, organizational culture and structure, IT governance, strategic alignment, and human-resource practices (Kraus et al., 2024).

Digital governance requires clear data ownership, classification, access rules, responsibilities, performance indicators, continuity and recovery plans, supplier review, and emerging-risk management. These requirements are particularly important in security institutions because failures of confidentiality, integrity, or availability can directly undermine operational capability and public trust.

From a strategic perspective, transformation quality depends on the institution's ability to absorb external knowledge, convert it into internal capabilities, and coordinate technical, administrative, and operational actors. Recent literature supports integrating digital transformation, cybersecurity, and sustainability within the strategic framework rather than treating them as separate initiatives (Kasmo et al., 2025).

Digital-government research further indicates that moving from assessment to action requires decision methods that jointly consider human, organizational, governance, technical, financial, and legal factors (Halim & Bounabat, 2026). Accordingly, security-sector transformation should begin with assessments of digital maturity, risk, and readiness, followed by prioritization, success metrics, and security controls.

Theoretical Framework – Page 4 of 5**5. Sustainability Strategy in Security Institutions**

Sustainability in strategic management refers to maintaining an organization's ability to achieve its objectives over the long term without exhausting resources or weakening future capability. Bansal and DesJardine (2014) emphasize the temporal dimension of sustainability: balancing present and future needs. In security institutions, sustainability includes the continuity of human, technological, financial, environmental, and institutional readiness.

Security sustainability may include energy and facility efficiency, technology life-cycle management, reduced reliance on paper-based procedures, preservation of human capital and institutional knowledge, resilient supply chains, business continuity, disaster resilience, and social responsibility. Digital technologies can support these goals through better measurement, forecasting, resource allocation, and reduction of waste.

George et al. (2012) identify sustainability challenges as a major concern for management and organization research because they require institutional innovation and coordination among multiple interests. In the digital context, Guandalini (2022), through a systematic review of 153 studies, concludes that the relationship between digitalization and sustainability is promising but complex and fragmented, requiring integrated managerial frameworks linking strategy to implementation.

Seele and Lock (2017) highlight the game-changing potential of digitalization for sustainability through new opportunities for accountability, communication, and innovation. Reviews of digital environmental transformation further show that artificial intelligence, big data, the Internet of Things, and cloud computing can support pollution control, waste management, sustainable production, and urban sustainability (Feroz et al., 2021).

Theoretical Framework – Page 5 of 5**6. Integration of Digital Transformation and Sustainability and Its Strategic Impacts**

Digital transformation and sustainability should not be treated as two parallel agendas. Digital technologies can improve resource efficiency, responsiveness, transparency, and measurement, while sustainability gives digital transformation a long-term orientation and criteria for evaluating investments and their consequences. Guandalini (2022) describes digital sustainability as an emerging field linking digital decisions to sustainability objectives.

Recent reviews suggest that integrating sustainability and digital transformation as an organizational strategy can reduce fragmented decision making and build a unified logic of value, resilience, and long-term performance (Kumer et al., 2025). At the same time, digitalization may generate negative environmental effects through energy consumption and electronic waste; therefore, evaluation should include both direct and indirect benefits and costs.

In a security institution, integration can be pursued through five paths: digitizing operations to reduce time and waste; using analytics for risk-based resource allocation; developing resilient and sustainable cyber infrastructure; continuously developing digital skills; and adopting balanced performance indicators covering operational, security, financial, environmental, and social outcomes.

Research indicates that successful transformation depends on alignment among strategy, capabilities, organizational structure, and performance measures (Verhoef et al., 2021). Big-data analytics also generates greater value when analytical capabilities are aligned with organizational strategy (Akter et al., 2016). Thus, strategic effectiveness is proposed as an outcome of interaction among digital maturity, sustainability, leadership, and governance rather than the product of a single factor.

7. Applied Study: Sample and Measurement

For academic demonstration, a dataset was constructed for 120 respondents.

Category	N	%
Senior and middle leadership	24	20.0
Officers / supervisors	54	45.0
Technical and administrative staff	42	35.0
Total	120	100

Years of service	N	%
Less than 5 years	18	15.0
5–10 years	35	29.2
11–15 years	31	25.8
More than 15 years	36	30.0

Reliability of the Instrument

Variable	Items	Cronbach's α	Assessment
Digital transformation	10	0.91	High
Sustainability	8	0.88	High
Leadership and governance	5	0.86	High
Strategic effectiveness	7	0.9	High
Overall instrument	30	0.94	Very high

The alpha coefficients indicate strong internal consistency. A neutral benchmark of 3.00 was assumed on the five-point scale.

8. Descriptive Analysis

Dimension	Mean	SD	Relative importance %	Rank
Digital infrastructure and data integration	4.08	0.61	81.6	2
Automation and analytics	3.89	0.67	77.8	5
Cybersecurity and governance	4.15	0.58	83.0	1
Digital skills and culture	3.76	0.72	75.2	6
Resource and operational sustainability	3.94	0.63	78.8	4

Business continuity and resilience	4.01	0.6	80.2	3
Strategic effectiveness	3.92	0.65	78.4	—

Cybersecurity and governance received the highest mean (4.15), while digital skills and culture received the lowest (3.76), suggesting that human-capability gaps may persist even where technological infrastructure is available.

Indicators Before and After Transformation

Indicator	Before	After	Change
Average incident-processing time	18.5 min	11.2 min	-39.5%
Digital transactions	42%	78%	+36 pp
Critical-system availability	96.8%	99.2%	+2.4 pp
Paper consumption/month	820 reams	390 reams	-52.4%
Service recovery time	5.4 h	2.7 h	-50.0%

These figures demonstrate how digital transformation and sustainability may be linked to measurable strategic and operational indicators.

9. Hypothesis Testing

9.1 Correlation Matrix

Variable	Digital transformation	Sustainability	Leadership & governance	Strategic effectiveness
Digital transformation	1.00	.61	.68	.72
Sustainability	.61	1.00	.55	.66
Leadership & governance	.68	.55	1.00	.70
Strategic effectiveness	.72	.66	.70	1.00

All correlations are positive and are assumed to be significant at $p < .01$.

9.2 Multiple Regression

Independent variable	Standardized β	t	p	Decision
Digital transformation	.39	5.84	<.001	Supported
Sustainability	.27	4.31	<.001	Supported
Leadership and governance	.30	4.76	<.001	Supported
Digital Sustainability $\times$	.14	2.62	.010	Supported

The model yields $R^2 = .67$ and $F = 58.4$ ($p < .001$), indicating that the predictors jointly explain approximately 67% of the variance in strategic effectiveness. The positive interaction coefficient suggests that the effect of digital transformation becomes stronger when sustainability practices are more developed.

10. Discussion of the Findings

The strong effect of digital transformation is consistent with literature that views transformation as a strategic process that reshapes value, operations, and capabilities (Vial, 2019; Verhoef et al., 2021). In security institutions, integrated data, analytics, and automation can shorten decision cycles, improve situational awareness, and reduce procedural duplication.

The sustainability effect indicates that security effectiveness depends not only on immediate readiness but also on continuity of resources, skills, systems, and supply chains. This is consistent with the temporal view of sustainability proposed by Bansal and DesJardine (2014) and with literature linking digitalization to resource efficiency and sustainability (Guandalini, 2022).

Leadership and governance emerge as critical because security-sector transformation requires clarity of authority, accountability, data ownership, and risk management. This finding is consistent with dynamic-capability theory, which places sensing, seizing, and reconfiguration at the center of strategic adaptation (Teece, 2007; Warner & Wäger, 2019).

The high evaluation of cybersecurity also illustrates that trust in digital systems is a prerequisite for institution-wide adoption. A transformation that expands connectivity and data dependence without appropriate security governance can increase rather than reduce strategic risk.

Finally, the interaction between digital transformation and sustainability implies that the best digital project is not necessarily the most technologically advanced one, but the one that improves performance while remaining maintainable, resilient, resource-efficient, and capable of preserving knowledge and skills over time.

11. Conclusions and Recommendations

11.1 Conclusions

1. Strategic management in security institutions is moving from periodic planning toward continuous management of dynamic capabilities in response to changing threats and opportunities.
2. Digital transformation is an organizational and strategic concept that extends beyond technology acquisition to redesigning processes, structures, culture, and decision systems.
3. Cybersecurity and data governance are foundational requirements for security-sector digital transformation.
4. Sustainability in security institutions includes the long-term continuity of operational readiness, human capital, technology, finance, environmental resources, and business continuity.
5. The hypothetical findings support positive effects of digital transformation, sustainability, leadership, and governance on strategic effectiveness and indicate additional value from integrating digital and sustainability strategies.

11.2 Recommendations

1. Develop an integrated digital transformation and sustainability strategy directly linked to institutional security objectives and measurable performance indicators.
2. Establish a strategic transformation office responsible for the digital project portfolio, benefits realization, risk, sustainability, and interdepartmental coordination.
3. Adopt a data-governance framework defining classification, ownership, access, quality, retention, and secure exchange.
4. Embed cybersecurity, resilience, and disaster recovery into the design stage of every digital initiative.
5. Implement continuous digital, analytical, and leadership skills development, supported by annual competency-gap assessments.
6. Use a balanced strategic dashboard covering response time, decision quality, system availability, cyber incidents, resource efficiency, service continuity, and stakeholder satisfaction.

7. Conduct a future field study in an actual Iraqi security institution using a larger sample and structural equation modeling to validate the proposed model.

References

1. Bansal, P., & DesJardine, M. R. (2014). Business sustainability: It is about time. *Strategic Organization*, 12(1), 70–78.
2. Bharadwaj, A., El Sawy, O. A., Pavlou, P. A., & Venkatraman, N. (2013). Digital business strategy: Toward a next generation of insights. *MIS Quarterly*, 37(2), 471–482.
3. Ellström, D., Holtström, J., Berg, E., & Josefsson, C. (2022). Dynamic capabilities for digital transformation. *Journal of Strategy and Management*, 15(2), 272–286.
4. Feroz, A. K., Zo, H., & Chiravuri, A. (2021). Digital transformation and environmental sustainability: A review and research agenda. *Sustainability*, 13(3), 1530.
5. George, G., Howard-Grenville, J., Joshi, A., & Tihanyi, L. (2012). Understanding and tackling societal grand challenges through management research. *Academy of Management Journal*, 55(6), 1293–1304.
6. Gong, C., & Ribiere, V. (2021). Developing a unified definition of digital transformation. *Technovation*, 102, 102217.
7. Guandalini, I. (2022). Sustainability through digital transformation: A systematic literature review for research guidance. *Journal of Business Research*, 148, 456–471.
8. Halim, S., & Bounabat, B. (2026). From assessment to action: A decision-support methodology for digital government transformation. *Sustainability*, 18(9), 4362.
9. Hanelt, A., Bohnsack, R., Marz, D., & Antunes Marante, C. (2021). A systematic review of the literature on digital transformation. *Journal of Management Studies*, 58(5), 1159–1197.
10. Kasmu, A. B. P., Mor, S., Nugroho, L., Rohadi, M., & Purnama, A. (2025). Integrating corporate strategy with digital transformation, cybersecurity, and sustainability. *Jurnal Lemhannas RI*, 13(1).
11. Kumer, I. M., Richter, J., Alberto, M. F., & Guerra, R. M. A. (2025). Exploring the integration of sustainability and digital transformation as an organizational strategy. *Revista de Administração da UFSM*, 18(4).
12. Laufs, J., et al. (2024). Liminal digital transformation in public sector: The case of UK policing. *The Journal of Strategic Information Systems*, 33(3), 101851.
13. Matt, C., Hess, T., & Benlian, A. (2015). Digital transformation strategies. *Business & Information Systems Engineering*, 57, 339–343.
14. Mergel, I., Edelmann, N., & Haug, N. (2019). Defining digital transformation: Results from expert interviews. *Government Information Quarterly*, 36(4), 101385.
15. Seele, P., & Lock, I. (2017). The game-changing potential of digitalization for sustainability. *Sustainability Science*, 12, 183–185.
16. Teece, D. J. (2007). Explicating dynamic capabilities: The nature and microfoundations of enterprise performance. *Strategic Management Journal*, 28(13), 1319–1350.
17. Teece, D. J., Pisano, G., & Shuen, A. (1997). Dynamic capabilities and strategic management. *Strategic Management Journal*, 18(7), 509–533.
18. Verhoef, P. C., et al. (2021). Digital transformation: A multidisciplinary reflection and research agenda. *Journal of Business Research*, 122, 889–901.
19. Vial, G. (2019). Understanding digital transformation: A review and a research agenda. *The Journal of Strategic Information Systems*, 28(2), 118–144.
20. Warner, K. S. R., & Wäger, M. (2019). Building dynamic capabilities for digital transformation: An ongoing process of strategic renewal. *Long Range Planning*, 52(3), 326–349.
21. Akter, S., Wamba, S. F., Gunasekaran, A., Dubey, R., & Childe, S. J. (2016). How to improve firm performance using big data analytics capability and business strategy alignment? *International Journal of Production Economics*, 182, 113–131.