

DOI: https://doi.org/10.48009/4_iis_2026_149

The influence of national cybersecurity capabilities on e-government development: A PLS-SEM analysis

Raul Diaz-Parra, *Universidad Esan*, jdiazp@esan.edu.pe

Abstract

The increasing dependence on digital government services has intensified the need for robust national cybersecurity capabilities to ensure secure, resilient, and sustainable digital public infrastructures. Despite the growing relevance of cybersecurity in digital governance, limited empirical research has examined how multidimensional cybersecurity capabilities collectively influence e-government development across countries. This study investigates the relationship between the Global Cybersecurity Index (GCI) and the E-Government Development Index (EGDI) using a cross-country dataset composed of 119 countries. Grounded in the Resource-Based View (RBV) and Dynamic Capabilities Theory, the study conceptualizes cybersecurity capability as a strategic national resource that enables governments to sustain digital transformation and improve public digital service delivery. The proposed model was analyzed using Partial Least Squares Structural Equation Modeling (PLS-SEM). The GCI was modeled as a formative construct composed of legal, technical, organizational, cooperation, and capacity development indicators, while EGDI was modeled as a reflective construct represented by online services, telecommunications infrastructure, and human capital indicators. The findings reveal a strong and statistically significant positive relationship between cybersecurity capability and e-government development ($\beta = 0.661$, $p < 0.001$), explaining 43.7% of the variance in EGDI ($R^2 = 0.437$). The results indicate that stronger cybersecurity capabilities are associated to digital government maturity and institutional digital resilience. The study contributes to the digital government and information systems literature by empirically validating cybersecurity capability as a strategic enabler of e-government development in international contexts. Additionally, the findings provide practical implications for policymakers seeking to strengthen cybersecurity governance and sustainable digital transformation strategies.

Keywords: Cybersecurity capabilities, E-government development, Digital government, PLS-SEM, Dynamic capabilities theory

Introduction

The rapid expansion of digital transformation has significantly increased the dependence of governments, businesses, and citizens on digital infrastructures and online services. However, this transformation has also expanded the attack surface for cyber threats, creating critical challenges related to security, institutional resilience, and trust in digital ecosystems. Cybersecurity threats are increasingly recognized as a major risk to the digital economy, digital trade, and the continuity of digital government services (Huang & Madnick, 2021). As nations accelerate the adoption of digital technologies, governments are pressured to strengthen their cybersecurity capabilities through legal frameworks, technical mechanisms, organizational structures, capacity-building initiatives, and international cooperation. Nevertheless, measuring national cybersecurity capability remains a complex challenge due to the multidimensional nature of cybersecurity and the lack of standardized and comparable metrics across countries (Kupeli & Sogut, 2024). Existing studies highlight that limited data availability, methodological inconsistencies, and fragmented cybersecurity indicators

create substantial uncertainty in evaluating and comparing national-level cybersecurity readiness (Kupeli & Sogut, 2024).

Digital government has become a fundamental component of national digital transformation by enabling governments to deliver more accessible, efficient, and citizen-centric public services through the adoption of advanced digital technologies (Hujran et al., 2023). Digital government improves administrative efficiency, information flow, and decision-making processes within public institutions (Hujran et al., 2023). Additionally, digital government initiatives promote transparency, citizen engagement, and accountability, which are considered essential dimensions of modern governance (Chan et al., 2021). In this context, citizen-centric approaches emphasize the importance of designing digital services around citizens' needs and expectations to improve public service quality and citizens' experiences with government institutions (Dechamps et al., 2025).

Cybersecurity has become a critical component of electronic government initiatives because the increasing digitalization of public services exposes governments to cyber threats, data breaches, and operational disruptions. Effective cybersecurity measures strengthen the protection of governmental systems, improve the reliability of online services, and enhance citizens' trust in digital public services. According to Abbas et al. (2022), stronger cybersecurity capabilities support institutional governance, secure public databases, and improve the sustainability and quality of e-government services in developing countries. Furthermore, digital government strategies increasingly integrate cybersecurity, artificial intelligence, and secure ICT infrastructure to ensure resilient, citizen-centered service delivery. The case of GovTech Singapore demonstrates how cybersecurity, secure digital infrastructures, and proactive cyber defense mechanisms contribute to effective digital transformation and public trust in government services (Perdana & Mokhtar, 2025). Therefore, cybersecurity is not only a technical requirement but also a strategic enabler of digital government performance, citizen trust, and sustainable public value creation.

Literature Review

The rapid expansion of digital government initiatives has transformed how public institutions interact with citizens, businesses, and other government entities. E-government systems aim to improve public service delivery, transparency, operational efficiency, and citizen participation through the use of digital technologies. However, the increasing dependence on digital infrastructures, interconnected systems, and online public services has simultaneously increased governments' exposure to cyber threats, cybercrime, data breaches, ransomware attacks, and disruptions affecting critical public services. As a result, cybersecurity capabilities have become a strategic requirement for the sustainable development of e-government ecosystems.

Prior studies have highlighted the importance of cybersecurity in digital government environments. Abbas et al. (2022) argued that cybersecurity measures contribute to stronger institutional governance, improved digitalization processes, and more sustainable public service delivery by protecting government systems and information assets. Similarly, Gandonou et al. (2025) emphasized that resilient e-government ecosystems require comprehensive cybersecurity frameworks that integrate technical controls, governance structures, standards, and organizational coordination mechanisms to mitigate cyber risks in public digital infrastructures. These studies suggest that cybersecurity is no longer merely an operational concern, but a strategic enabler of digital government maturity.

At the national level, cybersecurity capability is commonly measured using the Global Cybersecurity Index (GCI), developed by the International Telecommunication Union. The GCI conceptualizes cybersecurity

capability through five indicators: legal measures, technical measures, organizational measures, capacity development, and cooperation (Sharma & Vishvakarma, 2026). These dimensions collectively evaluate the extent to which governments establish cybersecurity legislation, incident response mechanisms, governance structures, awareness initiatives, workforce development programs, and international collaboration practices (International Telecommunication Union, 2024). Huang and Madnick (2021) used the GCI to examine how cybersecurity capability influences digital trade systems and found that cybersecurity capability contributes indirectly to more open digital ecosystems through e-government maturity.

Therefore, this study addresses this research gap by examining the relationship between the multidimensional cybersecurity capabilities represented by the Global Cybersecurity Index (GCI) and the multidimensional e-government development components represented by the E-Government Development Index (EGDI). Specifically, the study addresses the gap in understanding how multidimensional national cybersecurity capabilities collectively contribute to the development of digital government ecosystems. The research examines how legal, technical, organizational, capacity development, and cooperation capabilities influence e-government development, as reflected through online public services, telecommunication infrastructure, and human capital readiness.

Although prior studies recognize cybersecurity as a critical enabler of secure digital government, limited empirical research has examined how multidimensional national cybersecurity capabilities are associated with e-government development. Existing studies generally treat cybersecurity capability and e-government maturity as aggregate measures, offering limited insight into how legal, technical, organizational, capacity development, and cooperation capabilities collectively relate to the key dimensions of e-government, including online services, telecommunications infrastructure, and human capital. Furthermore, unlike Huang and Madnick (2021), who examined cybersecurity capability in the context of digital trade through the mediating role of e-government maturity, the present study directly investigates the relationship between national cybersecurity capabilities and e-government development. By modeling both the Global Cybersecurity Index (GCI) and the E-Government Development Index (EGDI) as multidimensional latent constructs within a PLS-SEM framework and analyzing a broad cross-country sample, this study provides a more comprehensive understanding of how national cybersecurity capabilities are associated with digital government development.

Theoretical Framework

Resource-Based View

The Resource-Based View (RBV) theory was proposed by Barney (1991), who argues that the internal resources of an organization are the primary source of sustained competitive advantage. To achieve competitive advantage, an organization must possess valuable, rare, imperfectly imitable, and non-substitutable (VRIN) resources and capabilities. These resources and capabilities may include both tangible and intangible assets, such as managerial skills, organizational processes and routines, information, and knowledge. Furthermore, states that organizations must also demonstrate the ability to adapt and reconfigure their resources in order to achieve competitive advantage and superior performance.

RBV provides a useful framework for organizations to identify, evaluate, and exploit their unique resources and capabilities to achieve sustained competitive advantage. Through the VRIN criteria, organizations can develop strategies that secure their long-term competitive position (Barney, 1991). Recent studies emphasize that cybersecurity actions are not merely defensive mechanisms, but strategic assets that enhance reliability, innovation capability, and long-term organizational performance (Chang et al., 2026). Furthermore, government support and institutional frameworks can amplify the effectiveness of

cybersecurity initiatives by aligning organizational strategies with broader digital governance objectives. From this perspective, cybersecurity capabilities can be conceptualized as critical strategic resources that enable governments and organizations to sustain digital operations, protect information assets, and support the successful development of digital platforms and e-government initiatives (Chang et al., 2026).

Dynamic Capabilities

Dynamic Capabilities Theory, proposed by David J. Teece, Gary Pisano, and Amy Shuen, argues that organizations must continuously integrate, build, and reconfigure internal and external competencies to respond effectively to rapidly changing environments. The theory emphasizes that competitive advantage depends not only on possessing valuable resources, but also on the capability to adapt, innovate, and transform organizational processes in dynamic contexts characterized by technological change and uncertainty (Teece et al., 1997). Furthermore, dynamic capabilities reflect an organization's ability to achieve new forms of competitive advantage by adapting its processes, positions, and strategic paths to environmental changes (Teece et al., 1997).

In the context of digital government, cybersecurity capabilities can be conceptualized as dynamic capabilities because governments must continuously adapt their technological infrastructures, regulatory frameworks, technical competencies, and security mechanisms to evolving cyber threats and digital transformation challenges. Strong cybersecurity capabilities improve resilience, operational continuity, and the protection of digital public services, thereby supporting the sustainable development of e-government systems. Since digital government initiatives rely heavily on secure and trustworthy digital infrastructures, countries with advanced cybersecurity capabilities are more likely to achieve higher levels of e-government development and more effective digital service delivery (Huang & Madnick, 2021).

Global Cybersecurity Index

The Global Cybersecurity Index (GCI), developed by the International Telecommunication Union, is an international index designed to measure countries' commitment to cybersecurity through a multidimensional and evidence-based approach. Its main objective is to assess national cybersecurity capabilities and identify improvement opportunities to strengthen digital resilience and trust in electronic services (International Telecommunication Union, 2024). The GCI considers cybersecurity a critical component of sustainable digital development, particularly in a context characterized by increasing cyber threats, digital transformation, and the rapid adoption of emerging technologies (International Telecommunication Union, 2024).

The GCI framework is structured around five main dimensions: legal measures, technical measures, organizational measures, capacity development, and cooperation. The legal dimension evaluates regulations related to cybercrime, privacy, and data protection; the technical dimension assesses operational capabilities such as CERTs and CIRTs; while the organizational dimension measures national cybersecurity strategies and governance mechanisms. Additionally, the capacity development dimension examines cybersecurity education, awareness, and training initiatives, whereas the cooperation dimension evaluates national and international partnerships for information sharing and cybersecurity collaboration (International Telecommunication Union, 2024).

According to the ITU, these five dimensions provide a comprehensive assessment of a country's cybersecurity maturity and its ability to build a secure, resilient, and trustworthy digital environment. In the 2024 edition, the GCI evaluated 194 countries through 83 questions grouped into 20 indicators, incorporating a tier-based model to classify countries according to their level of cybersecurity maturity. This approach enables cross-country comparison and supports the development of public policies aimed at strengthening national cybersecurity capabilities (International Telecommunication Union, 2024).

In addition to the Global Cybersecurity Index (GCI), other international frameworks have been developed to assess national cybersecurity and digital government maturity. For example, the National Cyber Security Index (NCSI) evaluates countries' preparedness to prevent and manage cyber threats through governance, operational capabilities, and capacity-building measures (Kupeli & Sogut, 2024). Likewise, the Organisation for Economic Co-operation and Development (OECD) Digital Government framework emphasizes institutional capabilities, digital governance, user-centered public services, and public sector innovation (Gale, 2025). These complementary initiatives highlight that national cybersecurity and digital government are multidimensional concepts requiring coordinated legal, technical, organizational, and governance capabilities. Nevertheless, the GCI was selected for this study because it provides a globally recognized and comprehensive measure of national cybersecurity capabilities that aligns with the proposed theoretical framework.

E-government Development Index

The E-Government Development Index (EGDI) is a composite indicator developed by the United Nations to measure the level of digital government development across its Member States. The EGDI evaluates how governments use information and communication technologies (ICTs) to deliver public services, improve administrative efficiency, and promote citizen participation. According to the United Nations, the EGDI is composed of three equally weighted dimensions: the Online Service Index (OSI), the Telecommunications Infrastructure Index (TII), and the Human Capital Index (HCI). These indicators collectively assess the readiness and capability of governments to provide accessible, inclusive, and effective digital public services (United Nations, 2024).

The Online Service Index (OSI) measures the scope and quality of digital services provided through national government portals and online platforms. It evaluates aspects such as institutional frameworks, service delivery, technological features, digital participation, and information accessibility. The Telecommunications Infrastructure Index (TII) examines the availability and quality of ICT infrastructure, including internet access, broadband subscriptions, mobile connectivity, and affordability of digital services. Meanwhile, the Human Capital Index (HCI) evaluates the population's educational and digital literacy capacities, which are essential for effective participation in digital government ecosystems (United Nations, 2024).

The EGDI has become one of the most widely recognized global benchmarks for assessing digital government performance and monitoring digital transformation trends. Since its introduction in 2001, the index has evolved continuously to reflect technological advancements and emerging governance challenges. The United Nations emphasizes that the EGDI is not intended to measure absolute digital maturity, but rather to provide a comparative assessment that enables countries to identify strengths, weaknesses, and opportunities for improvement in their digital government strategies. The index also supports policymakers in aligning digital transformation initiatives with the Sustainable Development Goals (SDGs) and national development priorities (United Nations, 2024).

Furthermore, the EGDI plays a critical role in understanding the relationship between digital government and sustainable development. Higher EGDI levels are commonly associated with improved public service delivery, stronger institutional effectiveness, greater transparency, and enhanced citizen engagement. The 2024 United Nations E-Government Survey highlights that digital government has become a fundamental enabler for achieving inclusive and resilient societies, although substantial disparities remain between developed and developing regions. Consequently, the EGDI serves not only as a measurement framework but also as a strategic policy instrument for guiding digital transformation and reducing the global digital divide (United Nations, 2024).

Although the Resource-Based View and Dynamic Capabilities Theory were originally developed to explain competitive advantage at the organizational level, recent studies have extended these perspectives to broader institutional and national contexts. In this study, national cybersecurity capabilities are conceptualized as strategic institutional resources embedded in legal frameworks, technical infrastructure, organizational arrangements, capacity development, and international cooperation. While these capabilities may not satisfy the VRIN criteria in the same manner as firm-specific resources, they represent difficult-to-develop institutional capabilities that require long-term investments, policy coordination, specialized expertise, and governance maturity. From this perspective, Dynamic Capabilities Theory further explains how governments continuously adapt and reconfigure these capabilities to respond to evolving cyber threats and support sustainable digital transformation.

Research Model

Cybersecurity capabilities have become a critical enabler of e-government development because digital public services increasingly depend on secure, resilient, and trustworthy technological infrastructures. The literature emphasizes that the expansion of digital government exposes institutions to cyber threats, data breaches, and service disruptions that can undermine public confidence and institutional performance. Abbas et al. (2022) argue that as governments accelerate digitalization, cybersecurity measures become essential to protect organizational systems, public databases, and online services, thereby improving institutional governance and service sustainability. The study further highlights that stronger cybersecurity frameworks enhance data management systems, secure internet services, and online public service delivery, which directly supports the effectiveness of e-government initiatives.

The relationship between cybersecurity and e-government is also associated with service quality, transparency, and citizen trust. According to Al-Zahrani (2020), cybersecurity factors such as perceived security, privacy, and trust significantly influence the effectiveness and usage of e-government services. In particular, the findings reveal that cybersecurity indicators improve perceived safety and reduce perceived risks in online government platforms, which strengthens citizens' willingness to use digital public services. Furthermore, the research emphasizes that concerns related to cybercrime, privacy violations, and information security remain major barriers to the successful implementation of e-government systems in developing countries.

Several studies also suggest that cybersecurity capabilities contribute to broader institutional modernization and digital transformation. Abbas et al. (2022) found that cybersecurity measures significantly enhance e-government performance by strengthening institutional practices, reducing corruption risks, and supporting sustainable public service delivery across Asian economies. The authors conclude that effective cybersecurity capabilities promote secure ICT adoption, improve accessibility and reliability of digital services, and increase the resilience of government systems against cyber threats. Similarly, Al-Zahrani (2020) demonstrated that cybersecurity-related factors positively influence e-government effectiveness and citizen satisfaction through improved system quality, information quality, and service reliability. Together, these findings indicate that cybersecurity capabilities are not only technical protections but also strategic institutional resources that facilitate the successful development and sustainability of e-government ecosystems.

H1: National cybersecurity capabilities positively influence e-government development.

Methodology

Data Collection and Analysis

The proposed model includes two latent constructs. The Global Cybersecurity Index (GCI) was conceptualized as a formative construct composed of five indicators: legal, technical, organizational, cooperation, and capacity development. Similarly, the E-Government Development Index (EGDI) was modeled as a reflective construct, composed of the Human Capital Index, Online Service Index and Telecommunications Infrastructure Index.

The dataset used in this study comprises cross-national indicators from multiple countries worldwide. The Global Cybersecurity Index (GCI) measures national cybersecurity capabilities, while the E-Government Development Index (EGDI) evaluates the level of digital government maturity. The use of multi-country data enables a comparative analysis of how cybersecurity capabilities influence e-government development across different institutional and technological contexts. The analysis is based on the 2024 editions of the Global Cybersecurity Index (ITU, 2024) and the United Nations E-Government Development Index (United Nations, 2024). Although historical GCI data are publicly available, this study intentionally employs the most recent cross-sectional dataset to examine the association between national cybersecurity capabilities and e-government development.

Both the Global Cybersecurity Index (GCI) and E-Government Development (EGDI) were conceptualized as latent constructs measured through multiple indicators derived from international cross-country indices. Although the GCI and EGDI are published composite indices, this study conceptualized national cybersecurity capability and e-government development as latent constructs represented by their respective multidimensional indicators within the PLS-SEM framework. Therefore, a structural equation modeling (SEM) technique was used, as it can assess relationships among latent variables (Pavlou, 2003). Among SEM options, this study relied on the partial least squares (PLS) variance-based technique due to its exploratory nature (Hair et al., 2010). As noted by Chin (2010, p. 660), PLS-SEM enables researchers “to constrain the new constructs and measures to its immediate nomological neighborhood of constructs and avoid possible CB-SEM estimation bias that can be affected by minor modeling or item selection errors.” Furthermore, the proposed model includes two latent constructs (GCI and EGDI), which are more suitable for PLS-SEM (Lowry & Gaskin, 2014). The SmartPLS 4.0 tool was used for analysis (Ringle et al., 2015). Because this study relies on cross-sectional secondary data, the results should be interpreted as evidence of statistical association rather than causal relationships.

Sample

To provide an overview of the study sample and the characteristics of the variables, descriptive statistical analyses were conducted using cross-country data obtained from international indices. The following tables 1, 2 and 3 present the distribution of countries included in the study, descriptive statistics of the constructs, and the operationalization of the measurement model. Frequency and percentage analyses were used to describe the composition of the sample.

Table 1: Distribution of Countries by Income Level

Income Level	Frequency	Percentage
High-income countries	45	37.80%
Upper-middle-income countries	38	31.90%
Lower-middle-income countries	25	21.00%
Low-income countries	11	9.30%

Total	119	100%
--------------	------------	-------------

Table 2: Distribution of Countries by Region

Region	Frequency	Percentage
Europe	32	26.90%
Asia	28	23.50%
Americas	24	20.20%
Africa	27	22.70%
Oceania	8	6.70%
Total	119	100%

Table 3: Classification of Countries by Cybersecurity Capability

Cybersecurity Capability Level	Frequency	Percentage
High GCI	41	34.50%
Medium GCI	49	41.20%
Low GCI	29	24.30%
Total	119	100%

For PLS, considering a maximum of one independent variable per dependent variable in the research model, prior literature recommends that it would be necessary to have a minimum of 33 observations to detect an R^2 value of at least 0.25 to achieve a statistical power of 0.8 at a significance level of 0.05 (Hair et al., 2010). Therefore, our sample size of 119 met the requirement. However, 119 is still not sufficient for the application of CB-SEM, which further supports the decision of using PLS in this study. The limitations associated with the sample size will be discussed in the Limitations and Future research subsection

Results

Multicollinearity

First, to evaluate multicollinearity among the constructs, this study employed the variance inflation factor (VIF). To assess multicollinearity among the formative indicators of the Global Cybersecurity Index (GCI), variance inflation factor (VIF) values were examined. As shown in Table 4, the VIF values for the formative indicators ranged from 2.419 to 5.737. Although the Technical Measures indicator exhibited a VIF slightly above the commonly recommended threshold of 5, the remaining indicators were below this value, suggesting that multicollinearity was not severe. (Hair et al., 2011). The E-Participation Index (EPI) was initially considered as part of the EGDI construct. However, the indicator was excluded from the final model due to multicollinearity concerns and to maintain consistency with the original structure of the United Nations E-Government Development Index (EGDI), which is formally composed of the Online Service Index, Human Capital Index, and Telecommunications Infrastructure Index. Removing EPI improved VIF values and enhanced the stability of the measurement model.

Table 4: Variance inflation factor values

Formative Indicator	VIF
Legal Measures (LEG)	2.419
Organizational Measures (ORG)	3.279
Cooperation Measures (COO)	3.907
Capacity Development (DEV)	4.982
Technical Measures (TEC)	5.737

Validation of Variables

This process included assessments of construct reliability and convergent validity. Given that E-government development index variable is reflective, reliability was assessed using internal consistency measures. Specifically, Cronbach's Alpha and Composite Reliability were calculated for each variable. As shown in Table 5, EGDI indicator exceeded the recommended minimum threshold of 0.70 (Nunnally, 1978), confirming adequate reliability. Convergent validity was assessed through two criteria. First, as displayed in the Table 5, all item loadings on their respective indicator exceeded the threshold of 0.70, recommended by Barclay et al. (1995). Second, Table 6 shows that the average variance extracted (AVE) for each variable exceeded the minimum acceptable value of 0.50, as suggested by Hu et al. (2004).

Table 5: Construct reliability and validity

Latent Variable	Cronbach's Alpha	Composite Reliability	AVE
E-government (EGDI)	0.918	0.935	0.859

Table 6: Outer Loadings

Variable	Loading	p-value
Human Capital (HUC)	0.958	< 0.001
Online Service (OLS)	0.930	< 0.001
Telecommunication Infrastructure (TLI)	0.891	< 0.001

Regarding discriminant validity, the heterotrait-monotrait ratio (HTMT) was not assessed because the model includes only one reflective construct (EGDI), while the Global Cybersecurity Index (GCI) was specified as a formative construct. Since HTMT is used to assess discriminant validity between two or more reflective constructs, its evaluation is not applicable in the present study. The construct, Global Cybersecurity Index (GCI), was conceptualized as a formative variable. Since GCI was conceptualized as a formative construct, internal consistency reliability measures such as Cronbach's alpha and composite reliability were not assessed. Instead, formative measurement evaluation focused on the significance and relevance of outer weights (Table 7) as well as multicollinearity assessment using VIF values. GCI construct revealed that several outer weights were not statistically significant. However, all formative indicators exhibited high outer loadings, exceeding the recommended threshold of 0.70, indicating strong absolute contributions to the construct. Following PLS-SEM guidelines, the indicators were retained due to their theoretical relevance and conceptual importance in representing national cybersecurity capability.

Table 7: Outer Weights

Variable	Weights	p-value
Cooperation Measures (COO)	-0.071	> 0.05
Capacity Development Measures (DEV)	0.405	> 0.05
Legal Measures (LEG)	0.219	> 0.05
Organizational Measures (ORG)	0.360	> 0.05
Technical Measures (TEC)	0.177	> 0.05

Structural Model

The structural model results indicate that national cybersecurity capabilities are positively associated with e-government development ($\beta = 0.661$, $t = 12.606$, $p < 0.001$, 95% BCa CI [0.519, 0.741]). The results support the proposed hypothesis and indicate that countries with stronger cybersecurity capabilities tend to exhibit higher levels of e-government development. The model explained 43.7% of the variance in EGDI ($R^2 = 0.437$). The effect size ($f^2 = 0.776$) indicates that national cybersecurity capabilities have a large explanatory effect on e-government development.

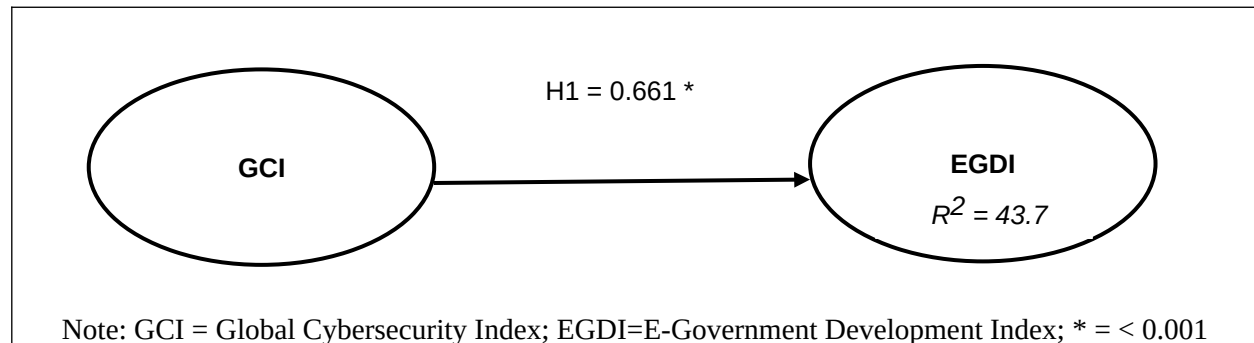


Figure 1: Structural Equation Model Assessment

Discussion

The findings indicate that national cybersecurity capabilities significantly and positively influence e-government development. The structural model revealed a strong, statistically significant relationship between the Global Cybersecurity Index (GCI) and E-Government Development (EGDI) ($\beta = 0.661$, $p < 0.001$), accounting for 43.7% of the variance in EGDI ($R^2 = 0.437$). These results suggest that countries with stronger cybersecurity capabilities tend to achieve higher levels of digital government maturity. The findings reinforce the idea that cybersecurity is not merely a technical or operational requirement, but rather a strategic enabler of digital transformation and sustainable public digital services.

From a theoretical perspective, the results support the assumptions of the Resource-Based View (RBV) and Dynamic Capabilities Theory. RBV argues that strategic resources and capabilities contribute to superior organizational and institutional performance. In this context, cybersecurity capabilities can be interpreted as strategic national resources that strengthen digital resilience, institutional trustworthiness, and the continuity of online public services. Similarly, Dynamic Capabilities Theory suggests that governments must continuously adapt and reconfigure technological and organizational capabilities in response to evolving digital threats and environmental changes. The findings suggest that cybersecurity capabilities may support governments in sustaining digital transformation processes and maintain reliable digital

ecosystems. Therefore, this study contributes to the information systems and digital government literature by empirically validating cybersecurity capability as a critical determinant of e-government development across countries.

The measurement model also provides important insights into the composition of national cybersecurity capability. Although several formative outer weights were not statistically significant, all formative indicators exhibited strong outer loadings, supporting the conceptual relevance of legal, technical, organizational, cooperation, and capacity development dimensions. Capacity development and organizational measures showed relatively stronger contributions to the GCI construct, highlighting the importance of institutional preparedness, cybersecurity governance, workforce development, and national coordination mechanisms.

From a practical perspective, the findings suggest investments in cybersecurity capabilities may support the advancement of digital government services. Governments should prioritize cybersecurity governance, technical infrastructure protection, workforce development, and institutional coordination to ensure resilient and trustworthy digital public services. More broadly, cybersecurity should be viewed not only as a defensive capability but also as a strategic component of national digital transformation and public sector innovation.

Limitations and Future Research

This study has several limitations. First, the analysis relies on secondary cross-country data obtained from international indices, which may not fully capture contextual differences in national cybersecurity practices or digital government implementation. Second, the cross-sectional design limits the ability to infer causal relationships or examine how cybersecurity capabilities and e-government development evolve over time. Third, although the model explains a substantial proportion of the variance in e-government development, additional institutional, economic, political, and social factors were beyond the scope of this study. Furthermore, the Global Cybersecurity Index is based on aggregated national indicators and may not fully reflect cybersecurity effectiveness at the organizational or agency level.

Another limitation is the use of a parsimonious structural model focused exclusively on the direct relationship between national cybersecurity capabilities and e-government development. Although this design was appropriate for establishing a foundational empirical relationship, it does not capture the mechanisms or contextual factors that may influence this association.

An additional limitation concerns the potential influence of omitted variables and endogeneity. Because both the Global Cybersecurity Index and the E-Government Development Index are composite national indicators, the observed relationship may also reflect broader institutional and economic conditions. Factors such as GDP per capita, governance quality, and regional characteristics may simultaneously influence both cybersecurity capabilities and e-government development. Although the present study focused on establishing the direct relationship between these constructs, future research should incorporate these variables as controls or employ longitudinal designs to better isolate the causal effect of cybersecurity capabilities on e-government development.

Future research should incorporate control variables such as national income level, GDP per capita, and governance quality to better isolate the relationship between cybersecurity capabilities and e-government development and reduce the potential influence of confounding factors. Future research should extend the proposed theoretical framework by incorporating mediating mechanisms that explain how cybersecurity capabilities translate into e-government development. Variables such as citizen trust in digital government, governance quality, digital literacy, technological readiness, and public service quality represent theoretically meaningful mechanisms through which cybersecurity capabilities may influence digital government outcomes. Likewise, moderating variables including national income level, regional context, and institutional maturity may help explain heterogeneity in the strength of the observed relationship. Longitudinal studies and comparative regional analyses would also provide a deeper understanding of how cybersecurity capabilities contribute to sustainable digital governance over time.

References

- Abbas, H. S. M., Qaisar, Z. H., Ali, G., Alturise, F., & Alkhalifah, T. (2022). Impact of cybersecurity measures on improving institutional governance and digitalization for sustainable healthcare. *PLoS ONE*, 17(11 November), 1–13. <https://doi.org/10.1371/journal.pone.0274550>
- Al-Zahrani, M. S. (2020). Integrating IS success model with cybersecurity factors for e-government implementation in the Kingdom of Saudi Arabia. *International Journal of Electrical and Computer Engineering*, 10(5), 4937–4955. <https://doi.org/10.11591/ijece.v10i5.pp4937-4955>
- Barclay, D., Thompson, R., dan Higgins, C. (1995). The Partial Least Squares (PLS) Approach to Causal Modeling: Personal Computer Adoption and Use an Illustration. *Technology Studies*, 2(2), 285–309. <https://doi.org/10.1017/CBO9781107415324.004>
- Barney, J. (1991). Firm Resources and Sustained Competitive Advantage. *Journal of Management*, 17(1), 99–120.
- Chan, F. K. Y., Thong, J. Y. L., Brown, S. A., & Venkatesh, V. (2021). Service Design and Citizen Satisfaction with E-Government Services: A Multidimensional Perspective. *Public Administration Review*, 81(5), 874–894. <https://doi.org/10.1111/puar.13308>
- Chang, Y.-Y., Lin, Y. M., Hu, Q., Chiang, F.-Y., Hung, T.-M., & Dai, S. (2026). Securing Strategic Advantage: The Role of Cybersecurity Actions and Government Support in Enhancing Digital Platform Capabilities. *Canadian Journal of Administrative Sciences / Revue Canadienne Des Sciences de l'Administration*, 43(2), e70033. <https://doi.org/https://doi.org/10.1002/cjas.70033>
- Chin, W. W. (2010). Handbook of Partial Least Squares. In *Handbook of Partial Least Squares* (Issue January 2010). <https://doi.org/10.1007/978-3-540-32827-8>
- Dechamps, S., Simonofski, A., & Burnay, C. (2025). Citizen-centricity in digital government: A theoretical and empirical typology. *Government Information Quarterly*, 42(1), 102005. <https://doi.org/10.1016/j.giq.2024.102005>
- Gale, W. G. (2025). Government at a Glance 2025. In *Fiscal Therapy*. <https://doi.org/10.1093/oso/9780190645410.003.0002>
- Gandonou, J. B., Dégila, J., Dagba, T. K., Wandji, T., Tognisse, I., & Adehan, A. (2025). Towards the Development

- of a Resilient and Compliant Cybersecurity Framework for E-Government: A Survey. *2025 IEEE 6th Annual World AI IoT Congress, AIIoT 2025*, 70–77. <https://doi.org/10.1109/AIIoT65859.2025.11105236>
- Hair, Joe F., Ringle, C. M., & Sarstedt, M. (2011). PLS-SEM: Indeed a silver bullet. *Journal of Marketing Theory and Practice*, 19(2), 139–152. <https://doi.org/10.2753/MTP1069-6679190202>
- Hair, Joseph F, Black, W. C., Babin, B. J., & Anderson, R. E. (2010). *Multivariate Data Analysis*. In *Englewood Cliffs*. Prentice Hall.
- Hu, X., Lin, Z., Whinston, A. B., & Zhang, H. (2004). Hope or hype: On the viability of escrow services as trusted third parties in online auction environments. *Information Systems Research*, 15(3), 236–249. <https://doi.org/10.1287/isre.1040.0027>
- Huang, K., & Madnick, S. (2021). Does high cybersecurity capability lead to openness in digital trade? The mediation effect of e-government maturity. *Proceedings of the Annual Hawaii International Conference on System Sciences, 2020-Janua*, 4352–4361. <https://doi.org/10.24251/hicss.2021.529>
- Hujran, O., Al-Debei, M. M., Al-Adwan, A. S., Alarabiat, A., & Altarawneh, N. (2023). Examining the antecedents and outcomes of smart government usage: An integrated model. *Government Information Quarterly*, 40(1), 101783. <https://doi.org/10.1016/j.giq.2022.101783>
- International Telecommunication Union. (2024). *International Telecommunication Union Global Cybersecurity Index 2024 5th Edition Global*. https://www.itu.int/dms_pub/itu-d/opb/hdb/d-hdb-gci.01-2024-pdf-e.pdf
- Kupeli, M., & Sogut, E. (2024). Assessment of the Cybersecurity Efficiency of G20 Countries Using Data Envelopment Analysis. *17th International Conference on Information Security and Cryptology, ISCTurkiye 2024 - Proceedings, Idi*, 2024–2027. <https://doi.org/10.1109/ISCTurkiye64784.2024.10779233>
- Lowry, P. B., & Gaskin, J. (2014). Partial Least Squares (PLS) Structural Equation Modeling (SEM) for Building and Testing Behavioral Causal Theory: When to Choose It and How to Use It. *IEEE Transactions on Professional Communication*, 57(2), 123–146.
- Moustaki, I. (1996). A latent trait and a latent class model for mixed observed variables. *British Journal of Mathematical and Statistical Psychology*, 49(2), 313–334. <https://doi.org/10.1111/j.2044-8317.1996.tb01091.x>
- Nunnally, J. C. (1978). Psychometric theory. *Psychometric Theory*, 640.
- Pavlou, P. A. (2003). Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model. *International Journal of Electronic Commerce*, 7(3), 101–134. <https://doi.org/10.1080/10864415.2003.11044275>
- Perdana, A., & Mokhtar, I. A. (2025). Digital transformation in government: Lessons from GovTech Singapore. *Journal of Information Technology Teaching Cases*, 0(0), 1–12. <https://doi.org/10.1177/20438869251362871>
- Ringle, Christian M; Wende, Sven; Becker, J.-M. (2015). *SmartPLS 3. Bönningstedt: SmartPLS*. <http://www.smartpls.com>
- Sharma, R. R. K., & Vishvakarma, N. K. (2026). *Measuring National Cybersecurity Preparedness : A Comparative Analysis Using the Global Cybersecurity Index*. 01(01), 17–27.
- Teece, D. J., Pisano, G., & Shuen, A. (1997). Dynamic capabilities and strategic management. *Strategic Management Journal*, 18(March), 77–116. <https://doi.org/10.4337/9781035334995.00014>

United Nations. (2024). *United Nations E-Government Survey 2024*.
<https://www.un-ilibrary.org/content/books/9789211067286>