DIGITALIZATION AND NATIONAL SECURITY IN SRI LANKA: EMERGING CYBERSECURITY CHALLENGES

Major M.H.M Imran[1]

INTRODUCTION

Digital transformation has fundamentally reshaped governance systems, economic interactions, and national security environments across the world. Governments increasingly rely on digital infrastructures for administrative services, financial transactions, public communication, and development planning. While digitalization improves efficiency, connectivity, and economic productivity, it also introduces complex security vulnerabilities that challenge traditional conceptions of national security.

Historically, national security was primarily understood in terms of territorial integrity, military defense, and protection from external armed threats. However, in the twenty-first century, technological advancements have significantly expanded the scope of security concerns. Cyberspace has emerged as a new domain of strategic competition where state and non-state actors can disrupt political institutions, economic systems, and social stability without conventional military confrontation.

Sri Lanka has actively embraced digital transformation as part of its broader development strategy. Recent initiatives such as e-governance platforms, digital payment systems, smart city initiatives, and the Digital Sri Lanka 2030 strategy illustrate the country's ambition to modernize governance and strengthen the digital economy. While these developments offer considerable opportunities for economic growth and administrative efficiency, they simultaneously expand the country's cyber-attack surface and expose institutions and citizens to emerging digital threats.

This article examines the relationship between digitalization and national security in Sri Lanka. It argues that while digital transformation presents significant developmental benefits, it also introduces cybersecurity vulnerabilities related to governance fragmentation, digital misinformation, and weaknesses in technological infrastructure. Addressing these challenges requires the development of an integrated national cybersecurity strategy supported by stronger institutional coordination and regulatory frameworks.

[1] General Sir John Kotelawala Defence University.

Faculty of Defence and Strategic Studies, General Sir John Kotelawala Defence University, Sri Lanka

Digitalization and the Changing Nature of National Security

The concept of national security has evolved significantly in recent decades. Traditional security frameworks primarily focused on military capabilities and geopolitical threats. However, scholars increasingly recognize that security threats now extend into economic, informational, and technological domains.

Joseph Nye (2010) argues that cyber power has become a critical component of modern statecraft, enabling actors to influence political and economic systems through digital networks. Similarly, Manuel Castells (2010) highlights how the emergence of the "network society" has transformed global power structures, making information flows and digital infrastructures central to political authority and social stability.

In this context, cybersecurity has become an essential component of national security policy. Cyber-attacks can disrupt critical infrastructure such as financial systems, energy grids, communication networks, and government databases. Unlike traditional military threats, cyber threats often originate from decentralized networks and anonymous actors, making attribution and deterrence significantly more complex.

For developing countries such as Sri Lanka, the rapid expansion of digital infrastructure often outpaces the development of cybersecurity governance mechanisms. As digital services expand across public administration and economic sectors, the risks associated with cyber vulnerabilities become increasingly significant.

Sri Lanka's experience reflects this broader global trend. The country's growing reliance on digital technologies has created new opportunities for innovation and economic modernization, but it has also introduced new forms of strategic vulnerability.

Digital Transformation in Sri Lanka

Sri Lanka has made considerable progress in digital governance over the past decade. Government agencies have increasingly adopted digital platforms to deliver public services, manage administrative processes, and improve citizen engagement.

Major initiatives include the development of e-governance services, online tax platforms, digital identity systems, and electronic payment infrastructures. The government's Digital Sri Lanka 2030 strategy further outlines plans to expand digital infrastructure, promote digital entrepreneurship, and strengthen technological innovation across multiple sectors.

These initiatives reflect the broader recognition that digital transformation is essential for economic competitiveness and governance efficiency. Digital technologies enable faster information exchange, improved transparency in administrative processes, and enhanced accessibility of public services for citizens.

However, rapid digitalization also introduces significant security challenges. As government systems become increasingly interconnected, vulnerabilities in one sector can potentially affect multiple critical systems simultaneously. Cybersecurity therefore becomes a foundational requirement for ensuring the resilience and sustainability of digital governance.

As highlighted in the original analysis of Sri Lanka's digital security landscape, the expansion of digital infrastructure has increased the country's exposure to cyber threats affecting government institutions, financial systems, and information networks.

Institutional Fragmentation in Cybersecurity Governance

One of the most significant challenges facing Sri Lanka's cybersecurity framework is institutional fragmentation. Multiple government institutions are responsible for managing different aspects of cybersecurity policy and implementation.

Key organizations include the Sri Lanka Computer Emergency Readiness Team (SLCERT), the Information and Communication Technology Agency (ICTA), and the Data Protection Authority established under the Personal Data Protection Act. Each of these institutions performs important roles in cybersecurity monitoring, digital governance development, and data protection.

However, coordination between these institutions remains limited. The absence of a fully integrated national cybersecurity command structure can create gaps in policy implementation, information sharing, and crisis response mechanisms.

Comparative international experience demonstrates the importance of centralized cybersecurity coordination. Countries such as Estonia, widely recognized for their advanced digital governance systems, have developed integrated cybersecurity frameworks that combine national security institutions, digital infrastructure management, and emergency response systems within a unified governance structure.

Sri Lanka's current system remains largely reactive rather than proactive. Cyber incidents are often addressed after they occur rather than through systematic risk assessment and preventive security mechanisms. Strengthening institutional coordination and developing a centralized cybersecurity governance structure would significantly enhance national cyber resilience.

Digital Misinformation and Information Security

Another major security challenge associated with digitalization is the rapid spread of misinformation through online platforms. Social media networks enable information to spread quickly across large audiences, often without adequate verification or fact-checking mechanisms.

In politically sensitive or socially fragile contexts, misinformation can contribute to social polarization, communal tensions, and public distrust in institutions. Scholars such as Ronald Deibert (2013) argue that information warfare and digital propaganda have become important tools in contemporary political conflict.

Sri Lanka's experience demonstrates the potential security implications of digital misinformation. During periods of political instability or national crisis, online platforms have sometimes amplified rumors, false narratives, and communal rhetoric.

The aftermath of the 2019 Easter Sunday attacks illustrated how digital communication networks can accelerate the spread of misinformation and fear within society. Online platforms became channels for the rapid circulation of unverified claims and inflammatory narratives, which intensified social tensions during an already sensitive national moment.

In post-conflict societies, where historical grievances and identity politics remain significant, digital misinformation can act as a powerful force multiplier for social instability. Unlike conventional propaganda, digital misinformation spreads through decentralized networks that are difficult for governments to regulate without raising concerns about freedom of expression.

Addressing this challenge therefore requires a balanced approach that promotes digital literacy, encourages responsible platform governance, and strengthens mechanisms for identifying and countering disinformation campaigns.

Vulnerabilities in Digital Infrastructure

In addition to governance and information challenges, Sri Lanka's technological infrastructure also faces cybersecurity vulnerabilities. Several cyber incidents involving government institutions have highlighted weaknesses in digital security systems.

Cybersecurity experts have pointed to issues such as outdated software systems, irregular security audits, limited cybersecurity expertise, and insufficient monitoring capabilities within certain government institutions. These vulnerabilities increase the risk of cyber intrusions and data breaches.

As Sri Lanka expands its digital financial infrastructure and online government services, the potential consequences of cyber-attacks could become increasingly severe. Cyber threats targeting banking systems, digital payment networks, or national data repositories could have significant economic and political implications.

The 2016 Bangladesh Bank cyber heist, in which hackers attempted to steal nearly one billion dollars through the SWIFT banking system, illustrates the scale of potential cyber risks in the region. The incident demonstrated how sophisticated cyber operations can exploit vulnerabilities in financial infrastructure, even within highly regulated institutions.For Sri Lanka, strengthening cybersecurity infrastructure is therefore not only a technological issue but also a strategic national security priority.

Strengthening Cybersecurity Governance

Given these emerging challenges, strengthening cybersecurity governance must become a central component of Sri Lanka's national security strategy. Several policy measures could significantly enhance the country's cyber resilience.

First, Sri Lanka should further develop and operationalize a comprehensive national cybersecurity strategy that integrates the efforts of government agencies, military cyber units, private sector stakeholders, and academic institutions. Stronger institutional coordination would enable faster threat detection, more efficient information sharing, and more effective crisis response.

Second, legal and regulatory frameworks must be strengthened to address evolving cyber threats. The effective implementation of the Personal Data Protection Act and the full

operationalization of the Data Protection Authority will be essential for protecting sensitive information and ensuring accountability in digital governance.

Third, investment in cybersecurity capacity building is critical. Universities and research institutions should play a larger role in developing cybersecurity expertise through specialized training programs and academic research initiatives.

Finally, public awareness and digital literacy programs should be expanded to help citizens identify misinformation and protect their personal data in online environments. Cybersecurity is not only a technical issue but also a societal challenge that requires broad public participation.

CONCLUSION

Digitalization presents both strategic opportunities and significant security risks for Sri Lanka. The expansion of digital governance platforms, financial technologies, and communication networks offers important benefits for economic development, administrative efficiency, and global connectivity.

However, these developments also expose the country to new forms of cyber threats, including digital misinformation, cyber-attacks on critical infrastructure, and institutional vulnerabilities within cybersecurity governance systems.

Sri Lanka's experience demonstrates that national security in the digital age extends beyond conventional military defense. Protecting digital infrastructure, safeguarding information integrity, and strengthening cybersecurity governance are now essential components of national resilience.

By developing a comprehensive cybersecurity strategy, strengthening institutional coordination, and investing in technological and human capacity, Sri Lanka can maximize the benefits of digital transformation while mitigating the risks associated with emerging cyber threats.

REFERENCES

Cabinet Office of Sri Lanka (2025) National Cyber Security Strategy of Sri Lanka. Colombo: Government of Sri Lanka. Available at:

https://www.cabinetoffice.gov.lk/cab/index.php?option=com_content&view=article&id=16&Itemid=49&lang=en&dID=13299 (Accessed on 3rd of September 2025).

Castells, M. (2010) The Rise of the Network Society. 2nd edn. Oxford: Wiley-Blackwell.

Daily FT (2024) 'Government unveils National Digital Economy Strategy', Daily FT, 24 April. Available at: https://www.ft.lk/TOP-STORY/Govt-unveils-National-Digital-Economy-Strategy/26-760981 (Accessed on 6th of September 2025).

Deibert, R. (2013) Black Code: Surveillance, Privacy, and the Dark Side of the Internet. Toronto: Signal.

Digital Development (2024) National Digital Economy Strategy – 2030 (Sri Lanka). Available at: https://www.digitaldevelopment.org/library/national-digital-economy-strategy-2030/ (Accessed on 15th of September 2025).

Information and Communication Technology Agency (ICTA) (2025) Connected Government and Digital Transformation Initiatives. Available at: https://www.icta.lk/connected-government/ (Accessed on 15th of September 2025).

Mind of Cyber (2025) Cybersecurity in Sri Lanka: Structure, Strengths and Challenges. Available at: https://mindofcyber.com/cybersecurity-in-sri-lanka (Accessed on 16th September 2025).

Ministry of Technology (2023) Digital Sri Lanka 2030: National Digital Strategy. Colombo: Ministry of Technology. Available at:

https://www.icta.lk/icta-assets/uploads/2023/05/Annex-1-National-Digital-Strategy-2030.pdf (Accessed on 20th September 2025).

Nye, J. S. (2010) Cyber Power. Cambridge, MA: Harvard Kennedy School.

Perera, A. (2024) 'Cybersecurity Challenges in Sri Lankan Government Websites', Journal of Sri Lankan Technology, 10(2), pp. 45–60.

Sri Lanka Computer Emergency Readiness Team (SLCERT) (2025) National Cyber Security Strategy 2025–2029. Colombo: SLCERT. Available at:

https://www.cert.gov.lk/wp-content/uploads/policies/National_Cyber_Security_Strategy_of_Sri-Lanka.pdf (Accessed on 29th September 2025).