



Future Digital Resilience in Safeguarding Critical Infrastructure and Securing Digital Economy

Jean-Noël Bonnieu

Vice President, International Relations, Thales Group, France

Abstract

Accelerating digital transformation, geopolitical fragmentation, and advances in artificial intelligence and quantum computing have elevated cybersecurity from a technical issue to a strategic imperative for protecting national infrastructure. This paper examines how middle powers can strengthen resilience amid growing dependence on interconnected digital ecosystems and increasingly sophisticated cyber threats. It argues that sustainable capability is shaped by two structural realities: the substantial investment required to develop advanced digital infrastructure and the practical limitations that prevent any country from independently mastering every critical technology. Consequently, infrastructure-agnostic solutions supported by trusted international partnerships become essential for ensuring operational continuity and security. Drawing on Thales' experience in post-quantum cryptography, sovereign cloud computing, digital identity, and trustworthy artificial intelligence, the paper highlights practical approaches to strengthening sovereign capabilities through technology transfer, local industrial participation, and knowledge development. Indonesia is presented as an example of how long-term collaboration can reinforce cybersecurity, protect critical infrastructure, and support sustainable digital transformation. The paper concludes that credible resilience depends on combining international cooperation with sustained investment in domestic expertise and innovation.

Corresponding Author:
Jean-Noël Bonnieu

Email:
jean-noel.bonnieu@thalesgroup.com

This article, authored by Jean-Noël Bonnieu, is published under the terms of the [Creative Commons Attribution-ShareAlike 4.0 International Licence](#), which permits unrestricted use, distribution, and reproduction in any medium, provided that proper credit is given to the original author(s), the title of the work, the journal citation, and the corresponding DOI. The selection and peer-review of this article were conducted under the responsibility of the JGF Conference Committee.



Published by Lemhannas Press.

Keywords: Critical Infrastructure, Cybersecurity, Digital Resilience, Sovereign Technology, Trusted Partnership.

Introduction

Digitalisation has significantly improved security, connectivity, and operational efficiency while simultaneously creating new vulnerabilities across critical infrastructure. The accelerating integration of digital technologies into public services, financial systems, transportation, cloud computing, and communication networks has expanded the cyber threat landscape, particularly amid growing geopolitical fragmentation and rapid advances in artificial intelligence and quantum computing. These developments have elevated digital resilience from a technical concern to a strategic priority for ensuring the continuity, adaptability, and security of critical national infrastructure.

The presentation examined how middle-sized countries can strengthen cyber resilience despite increasing dependence on globally interconnected digital infrastructure and rapidly evolving technologies. It argued that effective resilience requires recognising two structural realities: the substantial investment needed to develop advanced digital infrastructure and the practical limitations preventing any single country from mastering every critical technology independently. These conditions reinforce the importance of trusted technological partnerships and infrastructure-agnostic solutions capable of maintaining secure and reliable operations across diverse digital environments.

Drawing on Thales' experience in cybersecurity, defence technologies, cloud computing, digital identity, and artificial intelligence, the presentation explored practical approaches to strengthening sovereign technological capability. Attention was given to Indonesia as Southeast Asia's largest digital economy, where technology transfer, local industrial participation, knowledge development, and long-term partnerships were presented as fundamental elements for reinforcing digital resilience, protecting critical infrastructure, and supporting sustainable digital transformation.

Result and Discussion

Digitalisation has transformed the operation of modern societies by improving security, efficiency, and connectivity across digital identity, financial services, air traffic management, cloud computing, and interconnected networks. At the same time, increasing digital dependence has expanded vulnerabilities across these systems. As digital technologies become more deeply integrated into critical functions, cyber risks continue to grow alongside the complexity of digital ecosystems and the increasing use of interconnected infrastructure.

The presentation identified two major factors driving this acceleration in cyber vulnerability. The first is the intensification of geopolitical tensions, where the digital and cyber domains

have become arenas of strategic competition, extending beyond conventional cyberattacks to broader disruptions across technological and electromagnetic environments. The second is rapid technological advancement, particularly the emergence of AI-powered cyberattacks and the future impact of quantum computing on existing cybersecurity systems. Together, these developments raise a common challenge for middle-sized countries, including Indonesia and France, to ensure the continuity, resilience, and adaptability of essential infrastructure against increasingly sophisticated threats.

Responding to this challenge requires recognising two structural realities. Developing advanced digital infrastructure demands investments that only a limited number of global hyperscalers are currently able to provide, while no middle-sized country can independently master every advanced digital and cybersecurity technology. These conditions reinforce the importance of trusted technological partnerships capable of providing leading technological capability. Consequently, resilience depends on developing infrastructure-agnostic solutions that continue to operate securely across different digital architectures despite increasing infrastructure fragmentation.

The presentation illustrated this approach through three technological initiatives developed by Thales. The first is post-quantum cryptography, supported by sovereign hardware security modules developed and mastered end-to-end to strengthen cybersecurity before quantum computing becomes operational. The second is sovereign cloud computing, which combines hyperscale cloud infrastructure with national oversight and cybersecurity certification to deliver trusted cloud services while maintaining sovereign control over critical digital assets. The third is trustworthy artificial intelligence, where algorithms, training data, and operational outputs are mastered end-to-end to support defence mission systems through sovereign AI solutions designed for secure and reliable decision support.

These principles have been implemented through Thales' long-standing partnership with Indonesia across defence systems, air traffic management, satellite programmes, digital identity, and cybersecurity. Beyond delivering technology, the partnership places particular emphasis on local industrial participation, domestic operation and maintenance, technology transfer, and the development of local know-how through collaboration with Indonesian partners and national institutions. This approach helps ensure that the resilience of Indonesia's digital systems is supported by expertise developed and sustained within the country itself.

Building credible resilience therefore rests on three complementary foundations: recognising digital security as a strategic requirement throughout the digital ecosystem, strengthening technological knowledge and local know-how within Indonesia, and selecting trusted partners that reinforce long-term resilience rather than long-term dependency. These priorities align with Indonesia's national cybersecurity strategy

and support the development of secure, resilient, and sovereign digital capabilities in an increasingly fragmented technological environment.

Conclusion

Building credible digital resilience requires a comprehensive approach that enables essential services and critical infrastructure to remain secure and operational amid geopolitical uncertainty and rapid technological change. The presentation emphasised that resilience depends on three mutually reinforcing priorities: recognising digital security as a strategic requirement across the entire digital ecosystem, strengthening technological knowledge and local know-how, and establishing trusted partnerships that support long-term resilience rather than long-term dependency.

These priorities reflect Indonesia's efforts to strengthen its national cybersecurity strategy while adapting to emerging challenges associated with artificial intelligence, quantum computing, and increasingly interconnected digital infrastructure. Through trusted technological partnerships, infrastructure-agnostic solutions, and sustained investment in local capability, digital resilience becomes not only a cybersecurity objective but also a foundation for safeguarding critical infrastructure, supporting digital economic transformation, and reinforcing Indonesia's long-term technological resilience.

Publication Note

This article presents an academic adaptation of the presentation delivered at the 10th Jakarta Geopolitical Forum (JGF X) 2026. Editorial revisions were limited to structure, language, and readability, while the speaker's original arguments, meaning, and policy recommendations remain unchanged.

References

1. Lembaga Ketahanan Nasional Republik Indonesia (Lemhannas RI). **Jakarta Geopolitical Forum X/2026: Strengthening Multilateralism: Survival Amid Global Turbulence and a Fragmented World** [video on the Internet]. Jakarta: Lemhannas RI; 2026 Jul 9 [cited 2026 Jul 17]. Available from: <https://www.youtube.com/watch?v=IbYayky-FmQ>