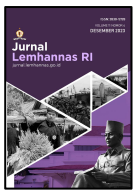

Jurnal Lemhannas RI (JLRI)
E-ISSN : 2830-5728
Vol. 13 No. 4, December 2025: 534-550
DOI: 10.55960/jlri.v13i4.1215
https://jurnal.lemhannas.go.id/index.php/jkl

Quantum Computing as a Global Game Changer in Technological Transformation towards National Resilience

Edi Permadi[1], Margaretha Hanita[2], Stanislaus Riyanta[3], Ahmad Ibrahim Badry[4]
[1,2,3,4]Departemen Kajian Strategis dan Ketahanan, Graduate School of Sustainable Development, Universitas Indonesia, Indonesia

Corresponding Author: edi.permadi@ui.ac.id

Article Info:

Keywords:
Digital Security, National Resilience, Quantum Computing, Quantum Cryptography

Article History:
Received: 13-10-2025
Revised : 22-10-2025
Accepted: 30-12-2025

Article DOI :
10.55960/jlri.v13i4.1215

Abstract

Purpose: This study investigates the implications of quantum computing for Indonesia's national resilience by placing digital security, data sovereignty, and governance preparedness as the focus of analysis. It examines how quantum technology may affect the stability and adaptive capacity of Indonesia's national resilience system, particularly in the dimensions of cybersecurity, defence, and strategic governance.

Study Design/Methodology/Approach: This study uses a descriptive qualitative approach based on an analysis of international and domestic literature published between 2018 and 2025, using Indonesia's national resilience framework, including *Asta Gatra* and ATHG, combined with Complex Adaptive Systems theory to examine the interactions of actors, institutions, and technologies in facing strategic disruption in the quantum computing era.

Findings: The findings reveal that the US, China, Japan and the EU have created advanced and coordinated quantum research ecosystems. quantum computing presents risks to public-key cryptography, digital infrastructure, signals intelligence, data sovereignty, and several dimensions of *Asta Gatra* because of limited human resources, insufficient research facilities, fragmented regulation, and the absence of an integrated post-quantum cryptography roadmap. This risk advocates for immediate actions such as the creation of a post-quantum cryptography roadmap, cryptographic asset mapping across public institutions, and national coordination in digital security. Long-term responses should include strengthening technological sovereignty, developing advanced quantum education, and building national research capacity in post-quantum security.

Originality/Value: This study presents a new insight by incorporating quantum computing into Indonesia's national resilience analysis through the *Asta Gatra*, ATHG, and Complex Adaptive Systems frameworks and gives policy recommendations for Indonesia to increase its technological sovereignty and adaptive capacity at an early stage in the quantum revolution.

How to cite : Permadi, E., Hanita, M., Riyanta, S, A.I. Badry. (2025). Quantum Computing as a Global Game Changer in Technological Transformation towards National Resilience. *Jurnal Lemhannas RI, 13* (4), 534-550. https://doi.org/10.55960/jlri.v13i4.1215

E-ISSN: 2830-5728

INTRODUCTION

Rapid technological progress has accelerated the development of quantum computing, which applies qubits through the principles of superposition and entanglement to perform complex computations at speeds surpassing those of classical binary-based systems (McKinsey & Company, 2025; Steane, 2000). Its coexistence with conventional processors for input and output operations has broadened the digital system connection with artificial intelligence (AI) and cloud computing (Rietsche et al., 2022).

Giant global player, like Google and IBM demonstrated quantum advantage over the most advanced supercomputers, and world leader countries such as the United States, China, Japan and the European Union intensified investment by establishing research laboratories, cultivating specialised talent and reinforcing quantum technology value chains (Arute et al., 2019; Rietsche et al., 2022). The technology has since evolved through scientific modelling, economic optimisation and cyber security, from molecular simulation of innovative materials (Gerbert & Ruess, 2018) to portfolio or logistics optimisation (Langione et al., 2019; Menard et al., 2020). as well as for the discovery of next-generation encryption. Despite this advancement, current machines sit in the Noisy Intermediate Scale Quantum phase, where qubit stability is limited and susceptibility to interference is high (Almudever et al., 2017).

The rise of quantum computing is transforming Indonesia's understanding of national resilience, particularly the threat (*ancaman*), challenge (*tantangan*), obstacle (*hambatan*), disturbance (*gangguan*) or ATHG in technology and cyber defence (Suryohadiprojo, 1997). Rising reliance on digital since Covid-19 has left government, economic and defence systems newly susceptible to quantum-enabled attacks that could compromise data sovereignty by mass decryption. Shor's algorithm, for example, can break RSA and ECC, the Indonesian government's asymmetric cryptographic algorithms utilised in our government systems, and it becomes necessary to strengthen the national policies on post-quantum digital security (Bova et al., 2021).

The Quantum Technology and Applications Consortium (QUTAC) states that readiness for quantum risk management requires state-of-the-art facilities, institutional collaboration and workforce capacity to conduct research-baseline expectations that are now being fulfilled by the world's largest economies through targeted government action" (Bayerstadler et al., 2021). In the United States, federal agencies are mandated to adopt quantum-resistant encryption with reference to standards issued by National Institute of Standards and Technology (NIST) years of 2024 and The White House (2022) . The European Union and China have made post-quantum cryptography a cybersecurity priority (European Union Agency for Cybersecurity, 2021; State Council of China, 2021). However, compared to these countries, Indonesia still falls short in these criteria. Therefore, Indonesia must develop a national strategy to reduce dependence on foreign cryptography and maintain digital security in the post-quantum era.

Previous studies on quantum computing have largely focused on technical development, cryptographic vulnerability, quantum algorithms, industrial applications, and global technological competition. In Indonesia, related studies have mainly discussed cybersecurity, digital transformation, and national resilience in general, without

DOI: 10.55960/jlri.v13i4.1215

E-ISSN: 2830-5728

specifically examining quantum computing as a strategic disruption to national resilience. This shows a research gap in analysing quantum computing through the Asta Gatra, ATHG, pentahelix, and Complex Adaptive Systems frameworks.

To address this gap, this study offers novelty by integrating quantum computing, post-quantum cryptographic risk, Indonesia's national resilience framework, and Complex Adaptive Systems theory. This integration enables quantum computing to be analysed not only as a technological issue, but also as a non-traditional security challenge affecting data sovereignty, governance, human resources, technological independence, and national adaptive capacity.

Consistent with these objectives, the study analyses the dynamics of quantum computing development that affect threats, challenges, roadblocks and disruptions to Indonesia's digital security and data sovereignty through national resilience system in a new quantum technology realm. The study assesses advanced economies' implementation of best practices of laws and policies towards establishing standards-setting for quantum-resistant cybersecurity regimes including regulation and post-quantum cryptographic research infrastructure and people development strategy to meet standard requirement. Finally, this study ascertains strategic policy which would be required to upgrade national preparedness in facing risks related to the emerging field of quantum technologies.

LITERATURE REVIEW

Theoretical Studies

The national resilience categorized resilience across eight interrelated dimensions (*Asta Gatra*), that are geography, demography, natural resources, ideology, politics, economy, social, culture, defence, security (Alfi et al., 2023). The concept of national resilience is based on *Pancasila* (The Five Principles of Ideology Countries of Indonesia), the 1945 Constitution of the Republic of Indonesia, and the Archipelagic Outlook (*Wawasan Nusantara*). The framework is aimed to map threat threat (*ancaman*), challenge (*tantangan*), obstacle (*hambatan*), disturbance (*gangguan*), in more well-known term, ATHG, based on the eight dimensions of resilience (Suryohadiprojo, 1997). A threat is when there is a deviation from a target. A challenge is a new target that needs to be achieved. An obstacle is something that weakens the achievement of a target. A disturbance is something that prevents the achievement of a target (Hanita, 2020). The ATHG concept also categorized threats into military or non-military, and internal or external to help state optimise capabilities and to maintain national resillience (Hikmawan, 2020). The national resilience concept stated that resilience require collective effort from 5 groups of society or stakeholders (pentahelix), that are government, academics, media, business, communities (Sari et al., 2024).

The concept of resilience is complexity is interrelated (Scharte, 2025). The Complex Adaptive System (CAS) theory suggests that complexity is essential for resilience because complex systems are made up of agents that can learn and adapt. However, as systems become more complex, they face a greater likelihood of sudden and

E-ISSN: 2830-5728

serious disruptions, which increases the need for resilience. Malik (2024) found that CAS can improve quantum computing approaches and quantum computing, in turn, can advance CAS-based analysis. CAS are defined by complexity, adaptability, self-organization, and emergent behaviour that appear across many fields, hence able to cover the 8 national resilience dimensions. Whole-systems quantum computing operates by manipulating the global quantum state through entanglement and superposition to solve difficult problems. Therefore, the integration of CAS principles into quantum computing can support the development of more advanced quantum algorithms, ultimately enabling more effective solutions to ATHG.

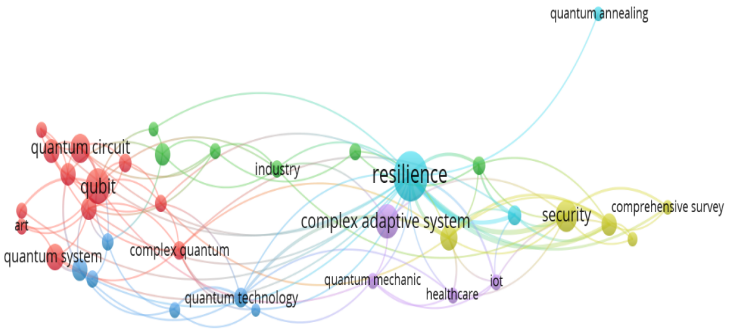

Figure 1. Network visualization of literature on quantum computing, national resilience concept and complex adaptive system theory

Figure 1 presents a network visualization on thematic relationships between literature on quantum computing, national resilience, and Complex Adaptive Systems (CAS) theory. At the centre of the network, the term "resilience" appears as the largest and most interconnected node, indicating that resilience is the primary conceptual bridge between the literature on quantum technologies and CAS. Resilience also has linkages to "complex adaptive system," "security," "quantum technology," and "industry" indicate that resilience has been discussed broadly. On the left side of the network, a dense cluster of red and blue nodes like "qubit," "quantum circuit," "quantum system," and "quantum technology" show the technically oriented literature on quantum computing. The proximity of these nodes indicates that literature on quantum computing focuses on technical aspects. These clusters connect to resilience cluster through concepts like "complex quantum" and "quantum mechanics". The right side of the network visualizes literature on CAS. Nodes like "security," "IOT" and "healthcare" form a cluster where resilience and CAS principles are used to assess the implications of emerging technologies. Overall, the network visualization show that quantum computing, CAS theory, and national resilience are increasingly interconnected. Quantum technologies form the technical base, CAS provides the theoretical framework for understanding system behaviour, and resilience linking technological advancement to societal needs. This pattern give room for research applying CAS-informed quantum methods to real-world resilience challenges, as part of transdisciplinary approach.

Empirical Studies

The empirical studies describe the approaches of the European Union, India, the United Kingdom, and the United States in legislative frameworks and standards

DOI: 10.55960/jlri.v13i4.1215

E-ISSN: 2830-5728

development to quantum technologies. Australia's policy on quantum technology is based on national security, responsible innovation, and economic development (Department of Industry Science and Resources, 2024; Lloyd-Jones & Manwaring, 2024; Resources, 2023). The National Quantum Strategy, "Shield 10" launched in May 2023, outlines the government's commitment in fostering Australia's quantum ecosystem. The strategy also set new standards to manage risks associated with quantum computing, especially on current cryptographic systems. Quantum technologies and cryptography are also designated as Critical based on the Foreign Acquisitions and Takeovers Act 1975. Act 2020 then set to amended Act 1975, to require foreign investments especially on quantum technologies or related infrastructure to undergo scrutiny by the Foreign Investment Review Board (FIRB). The Security of Critical Infrastructure (SOCI) Act reinforce the policy's impact by imposing obligations on operators of essential systems, including incident reporting to the Australian Signals Directorate, implementing risk management programs, and complying with requirements for Systems of National Significance. Although the current legislative reform does not contain quantum-specific measures, quantum technology challenge would still fall under the SOCI Act's risk and response frameworks. Moreover, Australia's telecommunications and intelligence legislation, for example the Telecommunications Act and Telecommunications (Interception and Access) Act, creates tension between national security access requirements and the technical properties of quantum communication systems. For example, quantum networks designed to be interception-proof may be incompatible with legal obligations for lawful access.

The European Union has set goals for advancing quantum technologies while acknowledging the risks to current cryptographic systems (European Comission, 2024; European Commision, 2023; Lloyd-Jones & Manwaring, 2024; Technologies, 2023). On 11 April 2024, the European Commission released a recommendation for member states to coordinate post-quantum cryptography (PQC) adoption. Although the EU does not yet have quantum-cybersecurity legislation, several policies already moving towards preparedness. For example, the proposed Cyber Solidarity Act of April 2023 is aimed to strengthen EU's cyber preparedness, detection, and response capabilities. This Act includes the establishment of a European Cybersecurity Shield. In April 2024, the Commission recommended that member states to begin migrating public-sector and critical infrastructure systems to PQC as soon as possible and collaborate in the selection of PQC algorithms as EU-wide standards. The Regulation (EU) 2021/821, controls export for dual-use items, covering quantum computers, qubit devices, quantum circuits, and other related components or technologies. European standards bodies have developed adoption frameworks of quantum technologies. The CEN-CENELEC Focus Group published a quantum technology standardization roadmap in March 2023. ETSI has released multiple technical reports and specifications complementing the NIST standardization.

India advancing its quantum technology ecosystem through national initiatives, funding, and research partnerships (Electronic and IT Division Council (LITDC), 2024; Lloyd-Jones & Manwaring, 2024; PMINDIA, 2023; The Economic Times, 2023). In January 2024, the Ministry of Electronics and Information Technology released a

E-ISSN: 2830-5728

Quantum Technologies Roadmap that prioritize research and development in cybersecurity. India has already demonstrated operational quantum capabilities, for example India has launched quantum-secure communication link in March 2023. The government has invested over INR 6000 crore (USD 730 million) under the National Quantum Missions that supports nearly one hundred quantum projects covering computing, communications, sensing, metrology, materials, and device innovation. The proposed Digital India Act (DIA) is set to pose stronger cybersecurity obligations. Export is also regulated under the Foreign Trade Policy (FTP) 2023 and the SCOMET list. Investment in quantum sectors is governed by the Foreign Exchange Management Act (FEMA). Investment in several sectors relevant to quantum technologies still require government approval. India is also developing its own quantum standards. The Bureau of Indian Standards (BIS) oversees technical standards for quantum computing and align India's quantum standards with international standards.

The United Kingdom has made long-term investments through National Quantum Technologies Programme (2014–2024) and the National Quantum Strategy (2023–2033), totalling over GBP 4.5 billion in public and private funding (Lloyd-Jones & Manwaring, 2024). The National Cyber Security Centre (NCSC) has issued guidance on quantum key distribution (QKD) and quantum-safe cryptography (QSC) (National Cybersecurity Connect, 2020). However, the NCSC advises that QKD is unsuitable for government or military use and discourages the deployment of non-standardized quantum-safe cryptography. The Investigatory Powers Act 2016 (IPA) and Regulation of Investigatory Powers Act 2000 (RIPA) govern the interception and acquisition of encrypted communications, and The National Security Investment Act 2021 (NSIA) allows the government to review and intervene foreign investments in including quantum technologies (GOV.UK, 2024). Additionally, quantum-related items are regulated as dual-use goods under the Export Control Order 2008, which oversees export controls for technologies with both civilian and military applications. In November 2023, the UK established the Quantum Standards Network Pilot to as participation in international quantum standards efforts. The UK works closely with IEEE Standards Association, ISO, and IEC, and is awaiting formal post-quantum cryptography standards from NIST and ETSI before continuing to large-scale adoption.

The United States has developed one of the most comprehensive frameworks for quantum technologies, covering even to the economic potential of quantum commercialisation (Lloyd-Jones & Manwaring, 2024; National Institute of Standards and Technology, 2025; National Quantum Coordination Office, 2022). The National Quantum Initiative Act (2018) established the National Quantum Initiative, that direct NIST, the National Science Foundation, and the Department of Energy in quantum research and development. Funding for quantum innovation and defence applications also provided through National Defence Authorization Acts (NDAA) and the CHIPS and Science Act 2022. The Quantum Computing Cybersecurity Preparedness Act (2022) mandates federal agencies to identify vulnerable in cryptographic systems and develop migration plans to adopt NIST-approved post-quantum cryptography (PQC). The U.S. also set legal basis for communications interception through Communications Assistance for Law Enforcement Act (CALEA), the Foreign Intelligence Surveillance Act (FISA),

DOI: 10.55960/jlri.v13i4.1215

E-ISSN: 2830-5728

and the PATRIOT Act. These legal acts require telecommunications providers to assist law enforcement under court order. Under the Export Control Reform Act 2018, key quantum technologies can be restricted to prevent uncontrolled proliferation. The U.S. primarily relies on the National Institute of Standards and Technology (NIST) that leads global efforts in post-quantum cryptography. NIST, alongside the National Security Agency, has issued guidelines for quantum-resistant algorithms. On 14 August 2024, NIST published the first three finalized PQC standards.

Differing to developed country, research on quantum computing in Indonesia are still dominated in studies on technical aspects with research gap on the implication to national resilience (Hidary, 2021; Preskill, 2023; Steane, 2000). In developing countries like Indonesia, quantum computing research is not common and still focus on classical computing level issues (Alfi et al., 2023; Putranti et al., 2020; Vincha & Satrio, 2024). Answering the research gap, this study offers novelty by integrating quantum technology and national resilience using transdisciplinary approach of technology policy and non-traditional security. The study also maps the implications of quantum computing for national data and digital infrastructure sovereignty.

METHODS

This study uses qualitative descriptive approach (Krippendorff, 2018; Saunders et al., 2015) that integrates empirical literature with the theoretical foundations of Indonesia's national resilience concept and the grand theory of Complex Adaptive Systems (CAS). Secondary empirical data are sourced from academic publications, government policy and strategy documents, and institutional reports concerning the digital, economic, and defence sectors. The reviewed sources were limited to academic publications, policy documents, and institutional reports published between 2018 and 2025 and were selected based on their relevance to quantum computing, signals intelligence, cybersecurity governance, post-quantum cryptography, and national resilience. These sources are used to identify patterns of policy responses to quantum technology, which are then mapped onto Indonesia's resilience framework to formulate strategic recommendations in the post-quantum era.

The analysis was conducted through document analysis and thematic content analysis. First, the selected sources were reviewed to identify the development of quantum computing and its implications for cybersecurity, data sovereignty, and national defence. Second, the findings were organised into four analytical themes: quantum computing and signals intelligence (SIGINT), global cybersecurity responses, quantum computing and national resilience, and policy directions for Indonesia. Third, these themes were interpreted through the concepts of threats, challenges, obstacles, and disturbances (ATHG) to assess how quantum technology may affect Indonesia's digital security and strategic resilience.

The study utilizes national resilience concept through the *Asta Gatra* framework, which categorises resilience into eight interrelated dimensions, and is normatively grounded in Pancasila, the 1945 Constitution of the Republic of Indonesia, and *Wawasan Nusantara*. The framework further recognises that resilience requires collective effort

E-ISSN: 2830-5728

from the pentahelix stakeholders. CAS theory is used to position complexity, adaptability, and institutional interaction as essential elements of resilience. In this study, the Asta Gatra framework is used to map the multidimensional impact of quantum computing on Indonesia's political, economic, socio-cultural, defence, and security dimensions. Meanwhile, CAS theory is used to explain national resilience as an adaptive system involving the interaction of government institutions, research organisations, universities, industry, security agencies, and society. This approach enables the study to formulate short-term and long-term policy directions for strengthening Indonesia's preparedness in the post-quantum era.

RESULT AND DISCUSSION

Quantum Computing and Signals Intelligence (SIGINT)

Quantum computing can increase the signals intelligence (SIGINT) capabilities in the interception and decryption of electronic communications. Quantum computing offers stronger cryptanalytical power far beyond classical systems, particularly over public-key cryptography methods like RSA and ECC (Mustafovski et al., 2025). Security studies increasingly view quantum technologies as drivers of a new era of information superiority in conflict environments, particularly within functions like command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR), in which SIGINT is situated.

Nation that achieve quantum decryption capabilities at early stage will possess significant advantages in mapping communication networks, identifying command structures, and accessing encrypted data that are valuable for diplomacy and defence planning (European Union Agency for Cybersecurity, 2022). The threat is not limited to immediate breaches of classified channels but includes practices like "harvest now, decrypt later", in which encrypted communications collected today may be decrypted in the future when large-scale quantum computers become available.

For Indonesia, the SIGINT dimension of quantum computing is directly linked to defence and diplomacy. ENISA and NIST have warned that foreign intelligence with more advance quantum decryption capabilities may gain access to encrypted archives containing sensitive material related to national security, foreign policy, and economic negotiations. Indonesia government must begin transition to quantum-resistant cryptographic standards and enhance technical capacity across defence and cybersecurity institutions so that Indonesia does not fall into an asymmetric position in the emerging quantum-era SIGINT competition when the operational quantum computers era finally emerge (European Union Agency for Cybersecurity, 2022).

Quantum Computing in Global Cybersecurity

The development of quantum technology has become global race for major powers (Shivakumar et al., 2025). More advanced quantum capabilities can give nations greater influence over data security, governance, military modeling, and SIGINT (Gruska, 2013; Shivakumar et al., 2025). The United States is advancing quantum development through the National Quantum Initiative Act that implement cross-agency collaboration and

DOI: 10.55960/jlri.v13i4.1215

E-ISSN: 2830-5728

mandatory migration to quantum-resistant encryption (Office of Management and Budget, 2022; United States Congress, 2018). IBM and Cisco have announced plans to build network of large-scale and fault tolerant quantum computers (IBM, 2025). JPMorganChase has launched $1.5trillion investment in sectors, one of them is quantum computing (JPMorganChase, 2025). China use centralized, state-driven model supported by substantial public investment. One example is the launch of the Micius satellite as a part of the national strategy for quantum communications (Hmaidi & Groenewegen-Lau, 2024; Liao et al., 2017). The European Union implement Quantum Technologies Flagship, although the private investment and hardware manufacturing still lags behind the US and China (European Commission, 2025b; Nolan, 2025).

The quantum industry is projected to surpass USD 1 trillion by 2035 (McKinsey Digital, 2025; Rietsche et al., 2022). However, without a global governance framework, the widening capability gap could increase security inequities and instability, particularly given the potential uses of quantum computing in decryption and defence systems (Nolan, 2025; Shivakumar et al., 2025). One of the example is the Shor's algorithm that break RSA and ECC (Shor, 1994) and prompted US authorities, NIST, and ENISA to deploy cryptographic asset mapping, migration planning, and developed post-quantum cryptography standards (National Institute of Standards and Technology, 2023).

Quantum Computing and National Resilience

Digital resilience and information security are core elements of Indonesia's socio-political and defence pillars in the national resilience framework (Lemhannas RI, 2018; Santoso, 2020). Therefore, National resilience is defined in this study as the nation's capacity to anticipate and withstand threats, challenges, obstacles, and disruptions (ATHG) from global technological transformation into quantum computing (Gidney & Eker, 2021; Hanita, 2020; Shor, 1994). Within the resilience framework, the quantum computing threats are categorized as non-military ATHG that threaten data security, public trust, and the continuity of digital development (Sari et al., 2024). Viewed through the Asta Gatra framework, quantum computing affects several dimensions of Indonesia's national resilience. In the defence and security dimension, quantum-enabled decryption may weaken the protection of strategic communication, intelligence archives, and classified state data. In the political dimension, cyber vulnerability may reduce the state's capacity to protect public institutions and maintain trust in digital governance. In the economic dimension, the exposure of financial, banking, and industrial data may disrupt digital economic stability. In the socio-cultural and demographic dimensions, limited quantum literacy and the shortage of specialised human resources may weaken Indonesia's adaptive capacity. Therefore, quantum computing should not be treated merely as a technical cybersecurity issue, but as a multidimensional resilience challenge

One example of threats is the "harvest now, decrypt later" (HNDL) strategy that is asymmetric and transnational. This threat require as soon as possible cryptographic asset mapping and transition to post-quantum cryptography (European Union Agency for Cybersecurity, 2021; National Institute of Standards and Technology, 2023). Countries like the United States and European Union are already transitioning to PQC and establishing deadlines for securing critical infrastructure (National Institute of Standards

E-ISSN: 2830-5728

and Technology, 2024) unlike Indonesia that still lacks on policies requiring encryption inventories or PQC migration plans. Right now, HNDL directed at public institutions or the financial sector will trigger large-scale data breaches and destabilise the digital economy.

In terms of ATHG, quantum computing may be classified as a threat when it enables foreign actors to decrypt sensitive national data; as a challenge when Indonesia needs to develop post-quantum cryptographic standards and human resources; as an obstacle when limited research infrastructure and fragmented regulation weaken preparedness; and as a disturbance when sudden technological disruption affects the continuity of public services, financial systems, and defence communication. This classification strengthens the relevance of the national resilience framework in assessing quantum-related risks.

Indonesia initiatives towards quantum computing development also hindered by limited public investment, fragmented research policy, and weak institutional capacity when compared to major powers' initiatives like the U.S. National Quantum Initiative, the EU Quantum Flagship, and the QBN network (European Commission, 2025a). Indonesia has only one major investment, that is the USD 400 million Quantum AI Data Centre in Batam as part of the Indonesian Quantum Initiatives (BRIN, 2024; Ramli, 2024; S & Gewati, 2025). Beside the quantum data centre, Indonesia still lacks quantum laboratories and accessible quantum computing facilities (Almudever et al., 2017). Indonesia education system also does not have dedicated academic and mastery programmes, even on basic quantum principles, hindering human capital development (Hidary, 2021; Primayanti & Nasution, 2025; Steane, 2000). The root problem is weak legal framework that coordinated policies linking research, security, and commercialisation (Hidary, 2021). Therefore, strengthening national resilience requires a coordinated transition to post-quantum encryption and enhanced digital literacy across government, industry, and education.

Policy Directions for Indonesia

In the short term, Indonesia must prioritise the development of a national transitioning roadmap to post-quantum cryptography (PQC) within six to twelve months. The roadmap should begin with mapping digital assets of digital assets across critical sectors and determine the priority levels, taking the example of EU recommendation to assess quantum risk exposure early and systematically (European Union Agency for Cybersecurity, 2021). This process should also be accompanied by a full audit of cryptographic dependencies within government systems, similar to the U.S. requirement under OMB Memorandum M-23-02 (Office of Management and Budget, 2022). Indonesia should also accelerate the formulation of national cryptographic standards in alignment with Regulation of the National Cyber and Crypto Agency of the Republic of Indonesia Number 11 of 2024 concerning the Implementation of Indonesian Cryptographic Algorithms and Assessment of the Security Conformity of Cryptographic Modules, ensuring that migration to PQC are consistent, secure, and interoperable with international standards like standards from NIST (National Institute of Standards and Technology, 2024) and ETSI (Lloyd-Jones & Manwaring, 2024).

DOI: 10.55960/jlri.v13i4.1215

E-ISSN: 2830-5728

Human capital development should be short-term priority. Indonesia must integrate quantum computing, quantum cryptography, and PQC into university curricula, in line with the recommendations of the World Economic Forum (2024). Public awareness should be foster to reduce the socio-technical risks of quantum transition. Indonesia should follow the EU and UK examples by promoting multi-stakeholder engagement through public briefings, expert forums, and international conferences (European Commission, 2025b). Domestic research ecosystems should also be strengthened. Taking example of Australia's National Quantum Strategy and the U.S. National Quantum Initiative, Singapore's Smart Nation and Digital Government Office (SNDGO) and South Korea's Ministry of Science and ICT (OECD, 2025; Smart Nation Singapore, 2025), Indonesia should establish a national coordinating institution or a National Digital Agency that centralises agendas on cybersecurity with Penta-helix model (Bayerstadler et al., 2021). The pentahelix approach should involve the government as the regulator and coordinator, universities and research institutions as knowledge producers, industry as technology developers and adopters, communities as users and beneficiaries of secure digital systems, and the media as a channel for public awareness and risk communication. Through this collaborative structure, Indonesia can build a more adaptive and resilient response to quantum-related cybersecurity risks.

Integrating Complex Adaptive System (CAS) theory into policy formulation strengthens the short-term strategy with views that national resilience emerges from the interaction of adaptive agents operating across multiple domains. Under CAS, Indonesia's digital ecosystem should not be viewed only as a collection of technical infrastructures but as a dynamic, interdependent system where government, industry, universities, security agencies, and citizens all contribute to adaptive capacity. Therefore, policy must encourage decentralised learning, redundancy, diversity, and rapid feedback mechanisms, which have helped Australia and the UK cultivate agile, whole-of-society responses to quantum risks. By embedding CAS design principles into governance structures, Indonesia can enhance flexibility and responsiveness in dealing with unexpected disruptions associated with quantum technologies.

In the long term, Indonesia must pursue technological self-reliance in cryptography and digital security, as stated in the National Cybersecurity Strategy (*Strategi Keamanan Siber Nasional* or SKSN). Achieving this self-reliance requires establishment of advanced quantum information science programmes and national research centres dedicated to quantum computing and post-quantum security. Countries like the US (through NSF and DOE quantum institutes), the UK (through the Quantum Technology Hub network), and India (through the National Quantum Mission) demonstrate the advantage of long-term, state-supported quantum ecosystems that integrate research, industry, and defence. Indonesia should adopt a similar model by investing in quantum laboratories, high-performance computing facilities, and specialised doctoral programmes that are comparable to MIT's Quantum Engineering Programme and Oxford's Quantum Technology Hub (Bova et al., 2021; European Commission, 2025b; Gerbert & Ruess, 2018; Hidary, 2021; Steane, 2000).

CAS theory also provides direction for long-term strategy. Since quantum disruption affects all eight national resilience dimensions (*Asta Gatra*), quantum policy

E-ISSN: 2830-5728

cannot be siloed. Indonesia must foster a resilient socio-technical system with distributed adaptive capacity. The ecosystem-wide adaptability can be fostered through diversification of quantum research fields (computing, sensing, communications), redundancy in cryptographic infrastructure, continuous feedback loops across institutions, and flexible regulatory frameworks capable of evolving with technological change. This strategy aligns with the EU's coordinated PQC transition roadmap and Australia's resilience-based approach to critical technologies. Ultimately, Indonesia's long-term strategy must ensure that the country becomes an active producer, not a passive consumer of quantum technologies.

CONCLUSION

This study shows that quantum computing offers strategic advantage and disadvantage for national resilience. Quantum capabilities become the basis of signals intelligence (SIGINT), providing unprecedented cryptanalytic power that threatens existing public-key systems through method like harvest now, decrypt later. Globally, major powers such as the United States, China, the European Union, the United Kingdom, and India have started preparation in facing the proliferation of quantum technologies through coordinated policy frameworks, mandatory encryption migration plans, multi-billion-dollar investments, and establishment of quantum research ecosystems. Compared to the developed countries, Indonesia remains at a very early stage of quantum technology development. Indonesia still faces structural limitations in investment, human capital, institutional capacity, and regulatory coherence. Therefore, this study proposes short- and long-term strategies by applying national resilience concept and Complex Adaptive Systems (CAS) theory. The study proposed strategy to enhance Indonesia's resilience in the quantum era based on the adaptive capacity across all *Asta Gatra* dimensions and mobilising pentahelix.

The study has several limitations. *First*, the analysis is primarily conceptual, policy based. The analysis lacks empirical modelling of Indonesia's cryptographic exposure, vulnerability levels, or quantitative risk projection. Future studies should explore these areas through simulations, mapping, and scenario analysis using CAS-based models. *Second*, this study does not evaluate Indonesia's organisational readiness or interagency coordination capacity in detail. Future work should include field studies, structured interviews, and institutional network analysis to assess governance bottlenecks. *Third*, future studies should also carry out empirical study on technologically emergent countries like Singapore, South Korea, and Japan. *Fourth*, the study does not explore the economic and industrial policy implications of emerging quantum markets, which future research could examine through value-chain analysis, domestic industry capability assessment, and techno-economic forecasting. Finally, future research should operationalise CAS theory by developing measurable indicators of adaptive capacity within Indonesia's digital ecosystem.

DOI: 10.55960/jlri.v13i4.1215

E-ISSN: 2830-5728

REFERENCE

Alfi, M., Yundari, N. P., & Tsaqif, A. (2023). Analisis Risiko Keamanan Siber dalam Transformasi Digital Pelayanan Publik di Indonesia. *Jurnal Kajian Stratejik Ketahanan Nasional*, *6*(2). https://doi.org/10.7454/jkskn.v6i2.10082

Almudever, C. G., Lao, L., Fu, X., Khammassi, N., Ashraf, I., Iorga, D., Varsamopoulos, S., Eichler, C., Wallraff, A., Geck, L., Kruth, A., Knoch, J., Bluhm, H., & Bertels, K. (2017). The engineering challenges in quantum computing. *Automation and Test in Europe*, 836–845. https://doi.org/10.23919/DATE.2017.7927104

Arute, F., Arya, K., Babbush, R., Bacon, D., Bardin, J. C., Barends, R., Biswas, R., Boixo, S., Brandao, F. G. S. L., Buell, D. A., Burkett, B., Chen, Y., Chen, Z., Chiaro, B., Collins, R., Courtney, W., Dunsworth, A., Farhi, E., Foxen, B., … Martinis, J. M. (2019). Quantum supremacy using a programmable superconducting processor. *Nature*, *574*(7779), 505–510. https://doi.org/10.1038/s41586-019-1666-5

Bayerstadler, A., Becquin, G., Binder, J., Botter, T., Ehm, H., Ehmer, T., Erdmann, M., Gaus, N., Harbach, P., Hess, M., Klepsch, J., Leib, M., Luber, S., Luckow, A., Mansky, M., Mauerer, W., Neukart, F., Niedermeier, C., Palackal, L., … Winter, F. (2021). Industry quantum computing applications. *EPJ Quantum Technology*, *8*(1). https://doi.org/10.1140/epjqt/s40507-021-00114-x

Bova, F., Goldfarb, A., & Melko, R. G. (2021). Commercial applications of quantum computing. *EPJ Quantum Technology*, *8*(1), 1–13. https://doi.org/10.1140/epjqt/s40507-021-00091-1

BRIN. (2024). *The Potential of Indonesia to Become a Pioneer in Quantum Technology*. BRIN. https://brin.go.id/en/news/120796/the-potential-of-indonesia-to-become-a-pioneer-in-quantum-technology

Department of Industry Science and Resources. (2024). *Theme 5: A Trusted, Ethical and Inclusive Quantum Ecosystem*. https://www.industry.gov.au/publications/national-quantum-strategy/themes-national-quantum-strategy/theme-5-trusted-ethical-and-inclusive-quantum-ecosystem

Electronic and IT Division Council (LITDC). (2024). *Strategic Roadmap*. https://www.services.bis.gov.in/tmp/ELECTRONICS AND IT DIVISION COUNCIL.pdf

European Comission. (2024). *Recommendation on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography*. https://digital-strategy.ec.europa.eu/en/library/recommendation-coordinated-implementation-roadmap-transition-post-quantum-cryptography

European Commision. (2023). *Regulation of the European Parliament and of The Council*. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52023PC0209

European Commission. (2025a). *Quantum Europe Strategy : Quantum Europe in a Changing World*. https://digital-strategy.ec.europa.eu/en/library/quantum-europe-strategy

European Commission. (2025b). *Quantum Technologies Flagship*. European Commission. https://digital-strategy.ec.europa.eu/en/policies/quantum-technologies-flagship

European Union Agency for Cybersecurity. (2021). *Post-Quantum Cryptography: Current State and Quantum Mitigation*. EINSA. https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation

European Union Agency for Cybersecurity. (2022). *Post Quantum Cryptography: Integration Study* (Issue October). European Union Agency for Cybersecurity. https://doi.org/10.2824/151162

Gerbert, P., & Ruess, F. (2018). *The Next Decade in Quantum Computing—and How to Play*. Boston Consulting Group. https://www.bcg.com/publications/2018/next-decade-quantum-computing-how-play

Gidney, C., & Eker, M. (2021). How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits. *ArXiv*, *1*(1), 1–31. https://doi.org/https://doi.org/10.22331/q-2021-04-15-433

GOV.UK. (2024). *National Security and Investment Act: Details of the 17 Types of Notifiable Acquisitions*. https://www.gov.uk/government/publications/national-security-and-investment-act-guidance-on-notifiable-acquisitions/national-security-and-investment-act-guidance-on-notifiable-acquisitions

Gruska, J. (1999). *Quantum computing*. McGraw-Hill.

Hanita, M. (2020). *Ketahanan Nasional: Teori, Adaptasi, dan Strategi*. UI Publishing. https://scholar.ui.ac.id/en/publications/buku-ketahanan-nasional-teori-adaptasi-dan-strategi/

Hidary, J. D. (2021). *Quantum Computing: An Applied Approach Second Edition*. Springer Nature. https://link.springer.com/book/10.1007/978-3-030-83274-2

Hikmawan, R. (2020). Redefinisi Ketahanan Nasional Guna Mewujudkan Ketahanan Regional di Asia Tenggara. *Jurnal Ilmu Hubungan Internasional LINO*, *01*(01), 72–97. https://doi.org/https://doi.org/10.31605/lino.v1i1.828

Hmaidi, A., & Groenewegen-Lau, J. (2024). *China's Long View on Quantum Tech has The US and EU Playing Catch-Up*. Merics. https://merics.org/en/report/chinas-long-view-quantum-tech-has-us-and-eu-playing-catch

IBM. (2025). *IBM and Cisco Announce Plans to Build a Network of Large-Scale, Fault-Tolerant Quantum Computers*. https://newsroom.ibm.com/2025-11-20-ibm-and-cisco-announce-plans-to-build-a-network-of-large-scale,-fault-tolerant-quantum-computers

JPMorganChase. (2025). *JPMorganChase Launches $1.5 Trillion Security and Resiliency Initiative to Boost Critical Industries*. https://www.jpmorganchase.com/newsroom/press-releases/2025/jpmc-security-resiliency-initiative

Krippendorff, K. (2018). *Content Analysis: An Introduction to Its Methodology*. SAGE Publications. https://methods.sagepub.com/book/mono/content-analysis-4e/toc

Langione, M., Tillemann-Dick, C., Kumar, A., & Taneja, V. (2019). *Where Will Quantum Computers Create Value—and When?* Boston Consulting Group. https://www.bcg.com/publications/2019/quantum-computers-create-value-when

Lemhannas RI. (2018). *Buku Pedoman Sistem Pengukuran Ketahanan Nasional dan Simulasi Kebijakan Publik* (8th ed.). Lemhannas RI. https://lemhannas.go.id/

Liao, S., Cai, W., Liu, W., Zhang, L., Li, Y., Ren, J., Yin, J., Shen, Q., Cao, Y., Li, Z., Li, F., Chen, X., Sun, L., Jia, J., Wu, J., Jiang, X., Wang, J., Huang, Y., Wang, Q., … Pan, J. (2017). Satellite-to-ground quantum key distribution. *Nature*, *549*, 43–47. https://doi.org/10.1038/nature23655

Lloyd-Jones, S., & Manwaring, K. (2024). *Quantum Resilience in the Australian National Security Legislative Framework (Policy Brief)*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4936141

Malik, P. (2024). Integrating Complex Adaptive Systems Theory with Whole-Systems Quantum Computing Approaches. *2024 IEEE 15th Annual Information Technology,*

Electronics and Mobile Communication Conference (IEMCON), 31–38. https://doi.org/10.1109/IEMCON62851.2024.11093529

McKinsey & Company. (2025). *What is Quantum Computing?* McKinsey & Company. https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-quantum-computing

McKinsey Digital. (2025). *Quantum Technology Monitor*. Mcki. https://www.mckinsey.com/~/media/mckinsey/business functions/mckinsey digital/our insights/the year of quantum from concept to reality in 2025/quantum-monitor-2025.pdf

Menard, A., Ostojic, I., Patel, M., & Volz, D. (2020). *A Game Plan for Quantum Computing*. McKinsey & Company. https://www.mckinsey.com/capabilities/tech-and-ai/our-insights/a-game-plan-for-quantum-computing

Mustafovski, R., Petrovski, A., & Radovanovic, M. (2025). Integrating quantum technologies into mobile military systems and TOC frameworks. *Land Forces Academy Review, 30*(3), 466–478. https://doi.org/10.2478/raft-2025-0045

National Cybersecurity Connect. (2020). *Preparing for Quantum-Safe Cryptography*. https://www.ncsc.gov.uk/pdfs/whitepaper/preparing-for-quantum-safe-cryptography.pdf

National Institute of Standards and Technology. (2023). *Quantum-Readiness : Migration to Post-Quantum Cryptography*. https://www.nccoe.nist.gov/sites/default/files/2023-12/pqc-migration-nist-sp-1800-38b-preliminary-draft.pdf

National Institute of Standards and Technology. (2024). *NIST Releases First 3 Finalized Post-Quantum Encryption Standards*. NIST. https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards

National Institute of Standards and Technology. (2025). *Post-Quantum Cryptography*. https://csrc.nist.gov/pqc-standardization

National Quantum Coordination Office. (2022). *About the National Quantum Initiatives*. https://www.quantum.gov/about/

Nolan, P. (2025). *Europe's Quantum Leap Challenges US Dominance*. Center for European Policy Analysis. https://cepa.org/article/europes-quantum-leap-challenges-us-dominance/

OECD. (2025). *Digital Government Review of Korea: Harnessing Digital and Data to Transform Government*. https://doi.org/https://doi.org/10.1787/9defc197-en

Office of Management and Budget. (2022). *Memorandum for The Heads of Executive Department and Agencies*. Executive Office of the President. https://www.whitehouse.gov/presidential-actions/2025/02/memorandum-for-the-heads-of-executive-departments-and-agencies/

Peraturan Badan Siber Dan Sandi Negara Republik Indonesia Nomor 11 Tahun 2024 Tentang Penyelenggaraan Alogritma Kriptografi Indonesia Dan Penilaian Kesesuaian Keamanan Modul Kriptografi (2024). https://peraturan.bpk.go.id/Details/309832/peraturan-bssn-no-11-tahun-2024

PMINDIA. (2023). *Cabinet Approves National Quantum Mission to Scale-Up Scientific & Industrial R&D for Quantum Technologies*. https://www.pmindia.gov.in/en/news_updates/cabinet-approves-national-quantum-mission-to-scale-up-scientific-industrial-rd-for-quantum-technologies/

Preskill, J. (2023). Quantum Computing 40 Years Later. *Feynman Lectures on Computation: Anniversary Edition*, 193–243. https://doi.org/10.1201/9781003358817-7

Primayanti, & Nasution, R. (2025, October 10). Indonesia Lags in Quantum Physics Education, Experts Warn. *Antara News*, 1. https://en.antaranews.com/news/385489/indonesia-lags-in-quantum-physics-education-experts-warn

Putranti, I. R., Amaliyah, A., & Windiani, R. (2020). Smartcity : Model Ketahanan Siber Untuk Usaha Kecil Dan Menengah. *Jurnal Ketahanan Nasional*, *26*(3), 359. https://doi.org/10.22146/jkn.57322

Ramli, A. M. (2024, November 20). RUU Keamanan dan Ketahanan Siber sebagai Prioritas Prolegnas 2025. *Kompas*, 1. https://nasional.kompas.com/read/2024/11/20/10484881/ruu-keamanan-dan-ketahanan-siber-sebagai-prioritas-prolegnas-2025?page=all

Resources, D. of I. S. and. (2023). *National Quantum Strategy*. https://www.industry.gov.au/publications/national-quantum-strategy

Rietsche, R., Dremel, C., Bosch, S., Steinacker, L., Meckel, M., & Leimeister, J. M. (2022). Quantum computing. *Electronic Markets*, *32*(4), 2525–2536. https://doi.org/10.1007/s12525-022-00570-y

S, I. J., & Gewati, M. (2025, July 14). Dengan Investasi Rp 6 Triliun, Indonesia Segera Bangun Pusat Komputasi Mutakhir AI dan Teknologi Kuantum di Asia. *Kompas*, 1. https://nasional.kompas.com/read/2025/07/14/10393081/dengan-investasi-rp-6-triliun-indonesia-segera-bangun-pusat-komputasi

Santoso, S. (2020). Memperkuat Pertahanan Siber Guna Meningkatkan Ketahanan Nasional. *Jurnal Lemhannas RI*, *6*(2), 43–48. https://jurnal.lemhannas.go.id/index.php/jkl/article/view/120

Sari, N. N., Fatya, A., Sinta, S., Erik, B. S., Rahmi, A., Aisyah, S., & Trisno, B. (2024). Urgensi Ketahanan Nasional dan Bela Negara Bagi Bangsa Indonesia Indonesia. *Politika Progresif: Jurnal Hukum, Politik Dan Humaniora*, *1*(3), 81–90. https://doi.org/https://doi.org/10.62383/progres.v1i3.467

Saunders, M., Lewis, P., & Thornhill, A. (2015). Research Methods for Business Students by Mark Saunders, Philip Lewis and Adrian Thornhill 8th edition. In *Research Methods For Business Students*. https://www.google.co.id/books/edition/Research_Methods_for_Business_Students/0DHFsgEACAAJ?hl=en

Scharte, B. (2025). The Need for General Adaptive Capacity: Discussing Resilience with Complex Adaptive Systems Theory. *Risk Analysis*, *45*(6), 1443–1452. https://doi.org/https://doi.org/10.1111/risa.17676

Shivakumar, S., Wessner, C., & Schumacher, A. (2025). *Quick Take: Quantum Technology Global Competition*. CSIS. https://www.csis.org/blogs/perspectives-innovation/quick-take-quantum-technology-global-competition

Shor, P. W. (1994). Algorithms for Quantum Computation : Discrete Logarithms and Factoring. *Proceedings 35th Annual Symposium on Foundations of Computer Science*, *1*(1), 124–134. https://doi.org/10.1109/SFCS.1994.365700

Smart Nation Singapore. (2025). *Our milestones: Trace the Key Milestones of Singapore's Smart Nation journey.* Smart Nation Singapore. https://www.smartnation.gov.sg/about/milestones/

E-ISSN: 2830-5728

State Council of China. (2021). The Outline of the 14th Five-Year Plan for Economic and Social Development and Long-Range Objectives Through the Year 2035 of the People's Republic of China. In *The Central People's Government of the People's Republic of China*. https://en.ndrc.gov.cn/policies/202203/P020220315511326748336.pdf

Steane, A. (2000). Quantum computing. *Reports on Progress in Physics*, *61*(2), 117–173. https://doi.org/10.1088/0034-4885/61/2/002

Suryohadiprojo, S. (1997). Ketahanan Nasional Indonesia. *Jurnal Ketahanan Nasional*, *2*(1), 13–32. https://doi.org/https://doi.org/10.22146/jkn.19163.

Technologies, C.-C. F. G. on Q. (2023). *Standardization Roadmap on Quantum Technologies*. https://www.cencenelec.eu/media/CEN-CENELEC/AreasOfWork/CEN-CENELEC_Topics/Quantum technologies/Documentation and Materials/fgqt_q04_standardizationroadmapquantumtechnologies_release1.pdf

The Economic Times. (2023). *India's First Quantum Computing-Based Telecom Network Link Now Operational: Ashwini Vaishnaw*. https://economictimes.indiatimes.com/industry/telecom/telecom-news/indias-first-quantum-computing-based-telecom-network-link-now-operational-ashwini-vaishnaw/articleshow/99026697.cms

The White House. (2022). *National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems*. The White House. https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/

United States Congress. (2018). *H.R.6227 - National Quantum Initiative Act*. Public Law 115-368. https://www.congress.gov/bill/115th-congress/house-bill/6227

Vincha, C., & Satrio, J. (2024). Kemunculan Ancaman Siber Teknologi 5G dan Implikasinya terhadap Ketahanan Siber di Jakarta. *Jurnal Ketahanan Nasional*, *30*(2), 222–241. https://doi.org/https://doi.org/10.22146/jkn.98563

World Economic Forum. (2024). *Quantum Security for the Financial Sector : Informing Global Regulatory Approaches* (Issue January). https://www3.weforum.org/docs/WEF_Quantum_Security_for_the_Financial_Sector_2024.pdf