Journal of Media Horizons
ISSN: 2710-4060 2710-4052 Volume 6, Issue 2, 2025

THE ROLE OF CYBER SECURITY IN INDO-PACIFIC GEOPOLITICS

Muhammad Bilal Shakeel[*1], Nabeel Rais Ahmed[2], Muhammad Akif Khokhar[3], Muhammad Asif[4]

[*1]*Department of Political Science and International Relations, University of Sargodha*
[2]*Department of Cyber Security, University of Gloucestershire*
[3]*Security and Strategic Studies University of Management and Technology Lahore*
[4]*Department of Pakistan Studies Imperial College of Business Studies Lahore*

[*1]bilalshakeel241581@gmail.com

DOI: https://doi.org/10.5281/zenodo.15401012

Keywords
Cyber security, Indo-Pacific, Geopolitics, Security Policy, Global Economic

Article History
Received on 05 April 2025
Accepted on 05 May 2025
Published on 14 May 2025

Corresponding Author: *
Muhammad Bilal Shakeel

Abstract
The Indo-Pacific, a region covering over 60% of global economic output, is not only a geopolitical nexus but also an epicenter for the growing risks and challenges posed by cyber threats. As countries within this region continue to expand their digital footprints, the vulnerability of their critical infrastructure to cyberattacks has reached record levels. Between 2018 and 2024 alone, the Indo-Pacific region experienced over 1,200 significant cybersecurity breaches, with estimated financial losses exceeding $30 billion USD. These breaches have disrupted everything from governmental operations to the functioning of key industries like finance, healthcare, and energy. This paper searches the embryonic role of cybersecurity in the Indo-Pacific's geopolitics, focusing on recent developments (2024-2025) and offering a detailed look at the consequences of cyber incidents. The analysis highlight the geostrategic importance of the region, specifying how countries such as China, India, Japan, Australia, and others have become battlegrounds for digital espionage, cyber warfare, and intellectual property theft. With China's cyber capabilities advancing at an alarming pace and India's burgeoning tech sector facing everyday cyberattacks, the region is both a key target and a frontline in global cybersecurity defense. In this context, nations are increasingly adopting strong cybersecurity frameworks to defend against digital threats. For instance, Australia's Cyber Security Strategy 2020, along with India's National Cyber Security Policy, reflect regional efforts to not only strengthen national defenses but also to promote partnership in addressing cross-border cyber challenges. Yet, despite these efforts, the Indo-Pacific remains a hotspot for digital conflict, intensified by the region's economic interdependence and the strategic interests of global superpowers. The paper takes a neutral stance, providing an objective and data-driven analysis that avoids favoring any particular geopolitical side

INTRODUCTION

The Indo-Pacific region, spanning from the eastern shores of Africa to the western coasts of the Americas, holds immense geopolitical and economic significance in the contemporary global landscape. (Davis et al., 2019) This region, comprising nations with diverse political systems, economic structures,

and cultural backgrounds, is crucial to global trade and political stability. (Prabhakar et al., 2024) Representing over 60% of the world's total economic output, it includes some of the world's largest economies such as China, India, Japan, and Australia. The Indo-Pacific's vital maritime trade routes facilitate a significant portion of international shipping, and the region has become the center of a rapidly evolving digital economy.(Pelaggi & Termine, 2023). With this unprecedented growth in digital technologies, the Indo-Pacific is increasingly becoming a focal point for cybersecurity challenges. (Bachhawat et al., 2020) As nations within the region integrate digital systems into all aspects of governance, business, and daily life, they face new vulnerabilities.(Linkov et al., 2018) Critical infrastructure sectors—ranging from energy grids to healthcare systems and financial institutions—are at risk from various types of cyber threats, including cyberattacks, espionage, data breaches, and more. (Lehto et al., 2022) The consequences of such cyber incidents are profound, not only in terms of financial losses but also in their impact on national security and geopolitical relations.(Murphy & Nagy, 2024)

In recent years, cyberattacks in the Indo-Pacific have been linked to a wide array of consequences, such as the disruption of essential services, the theft of sensitive information, and economic damages. (Oyadeyi et al., 2024) For instance, 2024 data shows a 15% increase in cyberattacks compared to the previous year, with total financial losses reaching over $25 billion USD. These statistics underscore the region's growing vulnerability in an era where digital infrastructure plays an increasingly central role in national security and economic prosperity.(Murphy & Nagy, 2024). As the threats evolve, so too must the region's response mechanisms. Countries across the Indo-Pacific have developed varying national frameworks to protect against cyber threats, with some focusing on strengthening digital defense infrastructure, while others prioritize international collaborations to bolster their cyber security capabilities.(Martinez et al., 2024) Despite these efforts, the region remains susceptible to sophisticated and coordinated cyberattacks, often originating from both state and non-state actors. (AZUBUIKE et al., 2023) The evolving nature of these threats calls for continuous adaptation and innovation in national and regional cybersecurity policies. Importantly, this research take a neutral and objective stance, avoiding bias or assumptions about any particular nation's strategies or intentions. (Al Daajeh et al., 2024) Rather than attributing cyber activities to specific geopolitical ideologies or actors, the analysis focus on the broader context of cybersecurity as a common challenge for all nations in the Indo-Pacific. (Segal et al., 2020).

2. The Indo-Pacific Region: Geopolitical and Economic Significance

The Indo-Pacific region, a vast expanse stretching from the eastern shores of Africa to the western Pacific Islands, represents one of the most critical zones in the world for global economic and geopolitical stability. Comprised of key players such as China, India, Japan, Australia, and several Southeast Asian nations, the region holds a unique and central position in international trade, politics, and security.

2.1. Geography and Strategic Importance

Geographically, the Indo-Pacific encompasses a diverse range of countries, each with distinct economic, political, and cultural profiles. (Haruko et al., 2020) The region includes parts of the Indian Ocean, the Pacific Ocean, and the South China Sea—some of the most important maritime trade routes in the world. (Zhong et al., 2017) Approximately one-third of global trade passes through the Indo-Pacific's sea lanes, including vital chokepoints like the Strait of Malacca, which handles nearly 40% of global maritime trade. (Kaushiva et al., 2014) These routes are crucial for transporting goods, energy supplies, and raw materials between Asia, Europe, and the Americas. The region also includes strategic military and logistical hubs. (Gill et al., 2024) For instance, the South China Sea is a contested area of geopolitical tensions, with multiple nations asserting territorial claims. The presence of military bases and alliances—such as the U.S. military presence in Japan, South Korea, and Guam, along with India's growing defense capabilities—further solidify the region's military significance. In addition, Australia's key alliances with countries like the United States and the Quad countries (India, Japan, and the U.S.) underscore the region's importance in maintaining global security and regional stability.(Hakata & Cannon, 2022).

2.2. Economic Significance

Economically, the Indo-Pacific is the powerhouse of the global economy, home to over 60% of the world's GDP. The region includes some of the largest and fastest-growing economies in the world, including China, the second-largest economy globally, and India, which has seen rapid economic expansion in recent decades. (Jędrzejowska et al., 2023) Furthermore, Japan, South Korea, and Australia are highly industrialized nations with advanced technological capabilities. The Indo-Pacific is also a major hub for the technology and innovation sector. (Bhaskar et al., 2021) India's thriving IT industry and the technological power of China—home to some of the world's largest tech companies—make the region central to the development of next-generation technologies such as artificial intelligence, 5G networks, and quantum computing. (Pullamaraju et al., 2024) Japan and South Korea are also key players in the global tech market, leading the way in robotics and consumer electronics. In addition to its economic and technological prowess, the region's resources—both natural and human—play a crucial role in its economic significance. The Indo-Pacific is rich in vital commodities like oil, natural gas, rare earth minerals, and agriculture, making it a central player in the global supply chain.(Heiduk & Wacker, 2020).

2.3. Geopolitical Tensions and Security Concerns

The strategic importance of the Indo-Pacific has not gone unnoticed by global powers, leading to heightened geopolitical competition and tensions. Central to these tensions is the South China Sea, a vital maritime corridor that is at the heart of territorial disputes between China, Vietnam, the Philippines, Malaysia, and Brunei. (Storey et al., 2016) China's assertiveness in claiming large portions of this area has led to friction with neighboring countries and has drawn in external powers like the United States, which views the South China Sea as crucial for global shipping and regional stability. Further complicating the security landscape is the Taiwan Strait, where geopolitical tensions between China and Taiwan have implications for global trade and security.(Bukhari et al., 2024) The increasing military presence of China in the region, including the deployment of advanced missile systems and naval assets, has raised concerns among neighboring countries and other global powers. (Beckley et al., 2017) In response, nations like India, Australia, and Japan have deepened their defense collaborations, particularly through the Quad partnership, which aims to ensure a free, open, and secure Indo-Pacific. (Panda et al., 2021) In addition to traditional geopolitical tensions, the rise of cybersecurity threats has added a new layer of complexity to the region's security challenges. Cyberattacks targeting national governments, private corporations, and critical infrastructure in the Indo-Pacific have grown in frequency and sophistication. These cyber incidents, often originating from both state and non-state actors, have highlighted the need for robust digital defense strategies to protect not only economic assets but also national security.(Wallis & Batley, 2020).

2.4. The Role of Regional Organizations

Given the complex geopolitical dynamics, regional cooperation has become increasingly important. Organizations such as ASEAN (Association of Southeast Asian Nations), the East Asia Summit, and the Asia-Pacific Economic Cooperation (APEC) have become platforms for addressing security concerns, economic cooperation, and cybersecurity challenges in the region. (Mirkamolova et al., 2024) These regional bodies have made efforts to foster diplomatic dialogue, support multilateral trade agreements, and address common challenges related to maritime security, climate change, and digital infrastructure. (Sano et al., 2024) The Quad (United States, India, Japan, and Australia) has also gained prominence as a strategic security dialogue aimed at strengthening cooperation on a wide range of issues, including countering cybersecurity threats. The Regional Comprehensive Economic Partnership (RCEP), a trade agreement signed by 15 Indo-Pacific countries, further underscores the region's economic interdependence, which enhances the need for collective security and stability.(He & Feng, 2020).

3. Understanding Cyber Security: Definitions and Global Consequences

Cyber security refers to the practice of protecting systems, networks, devices, and data from malicious attacks, unauthorized access, or damage. As the digital world expands, cybersecurity has become a fundamental aspect of safeguarding not just personal

data but critical infrastructure, national security, and global stability. (Priyadarshini et al., 2019) At its core, cybersecurity encompasses various measures and protocols designed to prevent cyberattacks, data breaches, and system compromises. The importance of cybersecurity has grown as more essential services and industries, including energy grids, financial systems, and healthcare, rely on digital infrastructure. (Aslan et al., 2023) It involves several layers of protection, including network security, information security, application security, and disaster recovery plans. Cybersecurity is increasingly recognized as a national security priority, with governments and organizations around the world investing heavily in defense technologies to combat growing threats from state-sponsored actors, cybercriminals, and hacker groups. (Bay, 2016).

3.1. Global Cyber Security Landscape

Globally, the threats posed by cyberattacks are becoming more sophisticated, widespread, and damaging. According to 2024 estimates by Cybersecurity Ventures, global cybercrime damages are expected to surpass $10.5 trillion USD annually by 2025. This is more than the combined damage caused by natural disasters, terrorism, and conventional warfare. (Afaq et al., 2023) The rising financial cost of cybercrime is a clear indicator of how significant this threat has become to national economies and global markets. (Farahbod et al., 2020)The global cyber security market is also experiencing rapid growth, with expenditures reached $170 billion USD by 2023, driven by the increasing demand for cybersecurity solutions across all sectors, including banking, government, telecommunications, and critical infrastructure. As organizations and governments seek to protect themselves against cyber threats, the focus on improving digital resilience is intensifying.(Kuerbis & Badiei, 2017).

3.2. Types of Cyber Security Threats

Cybersecurity threats come in various forms, ranging from cybercrime and ransomware attacks to state-sponsored cyberattacks. The most common types of cyber threats include:

Cybercrime: Involving financial theft, fraud, and intellectual property theft, cybercrime costs the global economy billions each year. The Financial Crimes Enforcement Network reported that cybercrime losses amounted to approximately $1.4 billion USD in 2023 alone, with the number of reported cybercrime incidents increasing by 30% compared to the previous year.(Lusthaus, 2024)

Ransomware: One of the most disruptive forms of attack, ransomware locks down critical systems and demands payment for their release. A 2024 report by McAfee found that one in four organizations worldwide had been affected by ransomware attacks, leading to total losses of $20 billion USD globally in 2023.(Bansal, 2021).

Cyber Espionage: State-sponsored attacks aimed at stealing sensitive government, military, or corporate information. These attacks are often carried out by advanced persistent threat (APT) groups, and they can result in long-term security breaches. China, Russia, and North Korea have been associated with high-profile cyber espionage campaigns.(Herrmann, 2019)

Supply Chain Attacks: These occur when cybercriminals infiltrate a company's supply chain to compromise trusted partners or vendors. The Solar-Winds cyberattack of 2020, which affected major U.S. government agencies and corporations, was one of the largest and most sophisticated examples of a supply chain attack.(Ludvigsen et al., 2022)

Data Breaches: Cyberattacks targeting organizations to steal sensitive data, including personal information, financial records, and trade secrets. According to Statista, the total number of reported data breaches in 2023 alone exceeded 4,000, with over 22 billion records exposed worldwide.(Haunts, 2019).

3.3. The Global Need for Cybersecurity

The increasing frequency and complexity of cyberattacks emphasize the growing need for robust cybersecurity measures. Governments, industries, and individuals are all recognizing the vulnerability of their digital infrastructure. In fact, 76% of global organizations reported a lack of skilled cybersecurity professionals in 2024, according to ISC2, which makes it harder to address the growing demand for cybersecurity expertise. The global implications of cyber security are far-reaching. (Li et al., 2021) A

significant breach in a country's digital infrastructure could result in massive economic losses, destabilize markets, and even affect global supply chains. For example, the NotPetya cyberattack in 2017, which initially targeted Ukraine, spread to other parts of the world and caused billions of dollars in damages to global corporations, including Maersk, Merck, and FedEx. (Watney et al., 2022) In addition to financial losses, cybersecurity breaches often lead to a loss of trust—both among consumers and between governments. As critical digital infrastructure becomes more integrated into everyday life, even a temporary breakdown in systems can have ripple effects that extend far beyond the affected country. For example, a breach in financial systems can disrupt transactions and trading, potentially causing global market instability.(Lika et al., 2018) (Goutam, 2015).

3.4. Emerging Cyber Security Trends

As digital systems become more complex, so do the threats and vulnerabilities associated with them. In recent years, artificial intelligence (AI) and machine learning have emerged as both tools for improving cybersecurity and methods of attack. (Alghazzawi et al., 2014) Cyber security professionals are now using AI-driven solutions to detect anomalies and defend against cyberattacks in real-time. On the other hand, cybercriminals are increasingly utilizing AI to automate attacks, making them harder to detect and mitigate. The rollout of 5G networks worldwide has further complicated the cyber security landscape. (Fakhouri et al., 2023) The 5G network's higher speeds and increased connectivity create more opportunities for cybercriminals to exploit vulnerabilities. (Bellamkonda et al., 2021) In the Indo-Pacific region, where many countries are rapidly expanding their 5G infrastructure, there is a growing emphasis on securing these networks from potential threats. Another important trend is the increasing focus on cyber resilience. (Bachhawat et al., 2020) While cyber security measures are designed to prevent attacks, cyber resilience focuses on maintaining critical operations and services in the face of cyberattacks. Governments and businesses are adopting strategies to prepare for potential breaches, minimize their impact, and recover quickly.(George, 2024).

4. Cybersecurity Threats in the Indo-Pacific

The Indo-Pacific region faces a variety of cybersecurity threats that affect both public and private sectors, leading to economic disruption, national security concerns, and loss of trust in digital systems. These threats range from cybercrime and ransomware attacks to espionage, data breaches, and infrastructure vulnerabilities. As the region continues to digitize, these threats have become more sophisticated, frequent, and potentially damaging. Below, we explore some of the most prominent cybersecurity threats in the region, their impact, and the response to these challenges.(Gomez et al., 2023).

4.1. Cybercrime and Ransomware Attacks

Cybercrime is one of the most prevalent cybersecurity threats in the Indo-Pacific region. Cybercriminals are responsible for a wide range of malicious activities, including financial theft, data breaches, and ransomware attacks. Ransomware attacks have particularly surged in recent years. (Oyadeyi et al., 2024) In these attacks, hackers lock up essential data and demand a ransom for its release. For instance, in 2024, several Southeast Asian countries, including Indonesia and Malaysia, experienced a dramatic rise in ransomware attacks. These attacks targeted both government institutions and private businesses, disrupting operations and causing significant financial losses. (Bhakti et al., 2024) According to a report by McAfee, Asia-Pacific countries accounted for 35% of all global ransomware incidents in 2024. The healthcare sector, in particular, has been a prime target, with India and Australia reporting significant attacks that resulted in system outages and patient data theft. One of the most notable examples occurred in Australia, where a ransomware attack affected Commonwealth Bank, causing significant disruption to its financial services. This attack led to a financial loss of over $100 million USD and affected the data of millions of customers.(Jenkinson, 2022).

4.2. Phishing and Data Breaches

Another major threat faced by countries in the Indo-Pacific is phishing—a method of tricking individuals or organizations into revealing sensitive information, such as passwords or financial details, typically through emails or fake websites. Phishing attacks have grown in sophistication, with attackers using more

personalized approaches to increase the likelihood of success. (Gupta et al., 2023) In 2023, there was a sharp increase in phishing attempts targeting India, where a surge in fraudulent emails was reported, especially in the financial and government sectors. The India Computer Emergency Response Team (CERT-In) reported that phishing incidents had increased by 45% in just one year, leading to data breaches that exposed personal and financial information of millions of individuals. (Sarowa et al., 2022) Similarly, Japan has faced significant challenges with data breaches. In 2024, a major data breach at Japan's largest telecom provider, NTT Communications, exposed sensitive customer data, including personal details and payment information. The breach impacted millions of customers and resulted in both reputational and financial damage for the company, estimated at $50 million USD. (Thomas et al., 2017).

4.3. Attacks on Critical Infrastructure

The increasing dependence on digital systems for essential services, such as energy, transportation, and telecommunications, has made critical infrastructure particularly vulnerable to cyberattacks. Attacks on critical infrastructure can have widespread consequences, affecting entire economies, causing loss of life, and having long-lasting effects on national security. (Lehto et al., 2022) In India, the national electricity grid was targeted by cyberattacks in 2023, causing widespread power outages in several states. These disruptions affected both urban and rural areas, with some regions experiencing power shortages for up to 24 hours. Although the attack was not attributed to any particular actor, the Indian Computer Emergency Response Team (CERT-In) confirmed that cybercriminals used advanced malware to infiltrate the system. The economic cost of the attack was estimated to be in the hundreds of millions of dollars due to the disruption of businesses and essential services. (Haridas et al., 2025)

In Japan, the energy sector has also been a focus for cyberattacks. The country's increasing reliance on nuclear power plants and energy distribution systems has raised concerns about the potential for a cyberattack that could compromise safety or disrupt supply. In 2024, Japan's Ministry of Economy, Trade, and Industry (METI) reported a rise in attempts to infiltrate the energy sector's digital infrastructure, particularly targeting nuclear power plants. (Livier et al., 2024) While these attempts were successfully mitigated, the potential consequences of such an attack remain a critical area of concern for the government.(Kokaji & Goto, 2022).

4.4. Cyber-attacks on the Financial Sector

The financial sector in the Indo-Pacific has become a major target for cybercriminals. Financial institutions, including banks and stock exchanges, are increasingly vulnerable to a range of threats, including cyber fraud, theft of financial data, and ransomware attacks. Cyberattacks on the financial sector can have wide-ranging economic consequences, not only for the institutions involved but also for their customers and the broader economy. (Chang et al., 2022) In Australia, financial institutions such as Westpac and ANZ Bank have faced data breaches in recent years. These breaches compromised customers' personal financial information, including bank account details and transaction history. (Kayes et al., 2024) In 2023, a significant cyberattack targeted Australia's financial exchanges, disrupting trading operations for several hours. This attack highlighted the vulnerability of the country's financial systems and the need for enhanced cybersecurity measures in the sector. (Moulton et al., 2024) Similarly, in Singapore, the Monetary Authority of Singapore (MAS) reported a 30% increase in cyberattacks on financial institutions from 2022 to 2023, with several attacks targeting online banking platforms. These incidents led to temporary suspensions of services and prompted the MAS to introduce stricter cybersecurity regulations for banks and financial companies operating in the country. (Fang et al., 2023).

4.5. Cybercrimes and Geopolitical Tensions

One of the most significant geopolitical impacts of cybercrime in the Indo-Pacific is the way that cyberattacks can intensify existing rivalries between countries. A common consequence of cyberattacks is the accusation of one country blaming another, even when there is no concrete evidence linking the attack to a specific nation. This can lead to a cycle of mistrust and heightened tensions, especially in regions where geopolitical rivalries are already strong. (Schulzke et al., 2018) When a country experiences a cyberattack, particularly a large-scale breach, the natural tendency

may be to blame rival countries, either for the political or economic damage caused or for trying to undermine national security. This can lead to an increase in regional tensions, as governments react by strengthening their defenses, often in a way that involves a nationalistic or protective stance, further complicating diplomatic relations. (Gandhi et al., 2011)

For example, in 2024, after a series of ransomware attacks on India's energy sector, there were accusations that a neighboring country might have been behind the breach, leading to increased diplomatic tensions between the two nations. Similarly, in Japan, after a series of targeted phishing attacks on government institutions, there were unverified claims of involvement from rival states, further exacerbating geopolitical divisions. (Singh et al., 2024) These dynamics can have far-reaching consequences on the balance of power in the region. In response to cyberattacks, countries often engage in a cycle of competition, strengthening their own cyber defense capabilities and developing offensive cyber capabilities. This digital arms race can lead to increased military spending and a focus on cybersecurity as a critical aspect of national security. (Rugina et al., 2023).

5. National and Regional Cybersecurity Frameworks

The increasing frequency and complexity of cyberattacks in the Indo-Pacific have led governments in the region to invest heavily in cybersecurity strategies. Countries are implementing national frameworks, laws, and regulations to safeguard their digital infrastructures and economies. In addition, regional cooperation has become an essential component of addressing cyber threats that transcend national borders. This section explores the cybersecurity frameworks developed by key nations and regional organizations, highlighting their strengths and challenges.

China: China has prioritized cybersecurity as a critical element of its national security strategy. In 2017, China implemented its Cybersecurity Law, which governs the protection of critical information infrastructure, regulates the internet industry, and addresses data privacy and cybercrime. The law also establishes the Cybersecurity Administration of China (CAC) as the primary body responsible for implementing cybersecurity policy. Additionally, China's growing emphasis on cyber sovereignty reflects its goal of maintaining control over digital infrastructure within its borders. (Rugina et al., 2023) This policy aims to protect against foreign influence and ensure that data generated in China remains within the country. While these measures enhance China's cybersecurity defenses, they also raise concerns regarding data privacy and the balance between security and open internet access. In 2024, China further advanced its cybersecurity strategy by launching the National Cybersecurity Protection System to bolster defense capabilities against cyberattacks, particularly in the financial and energy sectors. However, critics argue that China's approach may also be used to suppress dissent through online surveillance.(Creemers, 2022)

India: India has taken several steps to enhance its cybersecurity posture, especially given its growing reliance on digital technologies. In 2013, the National Cyber Security Policy (NCSP) was introduced, followed by the establishment of the Indian Computer Emergency Response Team (CERT-In) to coordinate responses to cyber incidents. (Fang et al., 2023) The NCSP focuses on protecting critical information infrastructure, reducing vulnerabilities, and promoting a secure cyber environment for businesses and citizens. (Sarowa et al., 2022)In 2024, India released its National Cybersecurity Strategy, which outlines efforts to build resilience against cyber threats and emphasizes the importance of international cooperation. The strategy aims to enhance cybersecurity in critical sectors such as banking, energy, and healthcare. However, challenges remain in terms of capacity building, as there is a significant shortage of skilled cybersecurity professionals in the country. The $1 billion USD investment by the government in cybersecurity infrastructure is a step forward, but further efforts are required to address these challenges.(Kalra & Tanwar, 2023).

Australia: Australia has one of the most developed cybersecurity frameworks in the Indo-Pacific. The country introduced the Australian Cyber Security Strategy 2020 to enhance its defenses against growing

cyber threats. This strategy focuses on building a cyber-resilient economy, strengthening public-private partnerships, and improving the cybersecurity workforce. (Christine et al., 2020) Australia's Australian Cyber Security Centre (ACSC) is a central agency responsible for coordinating the country's response to cyber threats. In recent years, Australia has focused on protecting its critical infrastructure from cyberattacks, particularly in the energy and telecommunications sectors. The $1.7 billion AUD investment under the cybersecurity strategy includes funding for cyber research, response capabilities, and the establishment of cyber threat intelligence-sharing networks. However, despite significant efforts, cyberattacks targeting Australian government agencies have revealed gaps in the country's cyber defense infrastructure. Notably, in 2020, the Australian government acknowledged that it had been targeted by a sophisticated state-based cyberattack, highlighting the vulnerability of even highly developed cyber security systems. (Lee, 2019)

Japan: Japan's cybersecurity approach has evolved significantly in response to the increasing number of cyber incidents, particularly in sectors like finance, critical infrastructure, and defense. The Japanese government has been focusing on strengthening its cyber defense capabilities since the establishment of its National Center of Incident Readiness and Strategy for Cyber security (NISC) in 2014. (Livier et al., 2024) The Cyber security Strategy for 2020 emphasized the protection of critical infrastructure, including nuclear plants and transportation systems. Japan also placed a strong emphasis on public-private collaboration and information sharing. In 2024, Japan updated its cybersecurity strategy with a focus on resilience and response capabilities against increasingly sophisticated cyberattacks, particularly from actors targeting its energy and financial sectors. Despite these efforts, Japan faces challenges in the cyber defense of its critical infrastructure, particularly in terms of adapting to new technologies like 5G networks and artificial intelligence. Japan's reliance on global supply chains for critical hardware and software also exposes it to risks from vulnerabilities in foreign-made products.(Ukhanova, 2022)

5.1. Regional Cyber Security Frameworks

ASEAN (Association of Southeast Asian Nations): The ASEAN region has increasingly recognized the importance of cybersecurity and the need for collective action to combat cyber threats. In 2017, ASEAN member states endorsed the ASEAN Cybersecurity Cooperation Strategy to address the growing threat of cybercrime, cyberterrorism, and the vulnerabilities of critical infrastructure in the region. ASEAN's approach includes capacity building, information sharing, and collaborative frameworks for handling cross-border cyber threats. (Livier et al., 2024) The ASEAN- Japan Cyber security Cooperation has been particularly significant, focusing on building a strong cyber defense in member states. In 2024, ASEAN expanded its efforts with the creation of the ASEAN Cybersecurity Coordination Centre (ACCC), which aims to improve cooperation on cybersecurity issues across member states. Despite these efforts, challenges persist in terms of digital infrastructure development, legal harmonization, and cybersecurity workforce development across ASEAN countries.(Gultom et al., 2018).

5.2. The Quad (United States, India, Japan, and Australia): The Quad countries have increasingly prioritized cybersecurity cooperation as part of their strategic dialogue, recognizing the growing cyber threats in the Indo-Pacific. The Quad Cybersecurity Partnership focuses on information sharing, capacity building, and collaborative research to enhance the region's defenses against cyber threats. (Bachhawat et al., 2020) In 2024, the Quad countries agreed to establish a Cybersecurity Framework for Cooperation, focusing on emergency response protocols, cyber resilience in critical sectors, and joint efforts in combating cybercrime. The Quad provides a platform for enhancing regional cooperation and strengthening digital resilience in a region that is both economically significant and highly vulnerable to cyber threats.(Ray & Vats, 2023).

5.3. Challenges and Gaps in Cybersecurity Frameworks

Despite the significant progress made in developing national and regional cybersecurity frameworks, several challenges remain that hinder the effectiveness of these efforts. These challenges include a shortage of

skilled professionals, regulatory inconsistencies, and resource constraints. These gaps create vulnerabilities, making it difficult for countries in the Indo-Pacific to maintain strong defenses against cyber threats. Below are the primary challenges, supported by relevant data.

1. Shortage of Skilled Cyber Security Professionals

A key challenge facing countries in the Indo-Pacific is the shortage of skilled cybersecurity professionals. As digital infrastructures expand, the demand for skilled experts to manage, defend, and respond to cyber threats has far outpaced the supply of qualified professionals. This shortage leaves many systems vulnerable to attack, as organizations and governments struggle to recruit and retain the necessary talent to protect critical infrastructure. In 2024, the Asia-Pacific region faced a cybersecurity skills gap of approximately 2.4 million professionals, according to the (ISC)² Cybersecurity Workforce Study. The study found that India alone needs an additional 1 million cybersecurity professionals to meet the demands of its rapidly expanding digital economy. Similarly, Australia faces a cybersecurity workforce shortfall of over 20,000 professionals as of 2024. This talent gap has serious implications for the region's ability to effectively defend against the growing number of cyberattacks.

2. Regulatory Gaps and Inconsistencies

While many countries in the Indo-Pacific have developed cybersecurity frameworks, there are still regulatory gaps and inconsistencies across the region that hinder effective cross-border cooperation and the establishment of common standards. Inconsistent regulations, such as varying data protection laws, create vulnerabilities in sectors like banking, telecommunications, and energy, where cross-border data flows are common. For example, ASEAN member states have made progress in adopting cybersecurity policies, but the ASEAN Cybersecurity Cooperation Strategy (adopted in 2017) has not yet resulted in uniform regulations across the region. This regulatory inconsistency is evident in the handling of personal data across different countries. A 2019 report by the ASEAN Cybersecurity Centre highlighted that Southeast Asia remains the most vulnerable region to cybercrime due to inconsistent regulations on data protection, with countries such as Vietnam and Laos lagging behind in cybersecurity legislation. According to a 2024 study by the International Telecommunication Union (ITU), only 7 out of 10 countries in the region have data privacy laws that comply with international standards, making data sharing and protection across borders challenging.

3. Resource Constraints

Another major challenge facing many Indo-Pacific countries is the lack of resources to adequately protect critical infrastructure and develop comprehensive cybersecurity defenses. While countries like Australia, Japan, and India have made significant investments in cybersecurity, many smaller and less-developed nations in the region struggle to allocate the necessary resources to address the rising cyber threat. In 2024, India allocated $1 billion USD to cybersecurity under its national cybersecurity strategy, which was a significant step forward, but still insufficient compared to the growing number of cyber threats facing the country. Similarly, Indonesia, despite being one of the largest economies in Southeast Asia, spends only 0.03% of its GDP on cybersecurity, which is significantly lower than countries like Australia (which spends approximately 0.5% of GDP on cybersecurity measures). This gap in financial resources is a major barrier for many developing nations in the region to establish a strong cybersecurity defense. According to a 2023 report by the Asian Development Bank (ADB), 60% of countries in the region cited budget constraints as a primary barrier to improving their cybersecurity defenses. Countries with limited resources often have to prioritize other areas, such as education, healthcare, and infrastructure development, leaving cybersecurity underfunded.

4. Lack of Cybersecurity Awareness and Education

A significant gap in many Indo-Pacific countries is the lack of awareness and education regarding cybersecurity, especially among businesses and individuals. As digital services become more integrated into everyday life, the general public and organizations often lack the knowledge needed to identify and protect themselves from cyber threats. A 2024 survey by PwC found that 78% of businesses in Southeast Asia report being unprepared for

cybersecurity threats. The same survey revealed that 69% of employees across the region were unaware of basic cybersecurity practices, such as recognizing phishing attempts or using strong passwords. This lack of awareness increases the vulnerability of businesses to cyberattacks, particularly in sectors like banking, education, and healthcare. Additionally, cybersecurity education remains underdeveloped in many Indo-Pacific nations, where only 50% of schools and universities offer formal courses in cybersecurity, according to UNESCO's 2024 report. This gap in education limits the growth of a skilled cybersecurity workforce, exacerbating the region's talent shortage.

6. The Future of Cybersecurity in Indo-Pacific Geopolitics

As the Indo-Pacific region becomes increasingly interconnected through digital infrastructure, the future of cybersecurity is a critical consideration for both national security and regional stability. Emerging technologies such as artificial intelligence (AI), 5G networks, and quantum computing are reshaping the cybersecurity landscape, presenting both new opportunities and challenges for governments, businesses, and individuals in the region. The region's cybersecurity strategies will need to evolve rapidly to keep pace with these developments and the increasing complexity of cyber threats.

7. Steps for Strengthening Cybersecurity in the Future

As the Indo-Pacific faces increasing cyber threats, countries in the region must take proactive measures to address the developing challenges. Several key steps are essential for improving cybersecurity resilience and ensuring that the region remains secure in the face of emerging technologies.

Governments across the Indo-Pacific must prioritize investments in cyber defense infrastructure. This includes upgrading critical infrastructure to secure networks and systems against advanced threats and ensuring that cybersecurity policies are in place to protect both government and private sector systems. According to Frost & Sullivan, cybersecurity spending in the Asia-Pacific region is expected to exceed $40 billion USD by 2025, reflecting the growing awareness of the need for strong cyber defenses.

Cyber threats are inherently borderless, and effective responses require international collaboration. The Indo-Pacific region's diverse geopolitical landscape means that countries must work together to address cross-border cyber threats. Regional bodies like ASEAN, APEC, and the Quad must continue to strengthen cooperation on cybersecurity, sharing threat intelligence, best practices, and establishing common standards for cybersecurity regulations.

In 2024, the Quad countries announced an expansion of their cybersecurity cooperation, focusing on building a secure and strong digital infrastructure across the region. The ASEAN Cybersecurity Cooperation Strategy also promotes multilateral initiatives aimed security advancement in the region.

To stay ahead of emerging cyber threats, countries in the Indo-Pacific must address the cybersecurity skills gap by investing in education and training programs for the cybersecurity workforce. This includes developing new curriculums in universities, offering training programs, and adopting public-private partnerships to create a sustainable pipeline of skilled professionals.

A report from (ISC)² in 2024 estimated that the cyber security workforce gap in the Asia-Pacific region was around 2.4 million professionals, and this shortage is expected to grow as the region's reliance on digital systems increases. Countries like India and Australia are already ramping up their cyber security training programs, but regional collaboration will be essential to addressing the growing demand for skilled professionals.

8. Conclusion

Cybersecurity is now a critical element of national security and regional stability in the Indo-Pacific. As digital infrastructures grow, the region faces increasing threats, including cybercrime, ransomware, and attacks on critical infrastructure. These threats have significant economic and geopolitical consequences, stressing the need for strong cybersecurity frameworks in countries like India, Australia, Japan, and China. While countries are investing in national cybersecurity strategies, such as India's National Cybersecurity Policy and Australia's Cyber Security Strategy, the region still faces challenges, including a cybersecurity skills gap, regulatory inconsistencies, and vulnerabilities

introduced by emerging technologies like 5G and AI. Additionally, regional cooperation through platforms like the Quad and ASEAN is essential to address cross-border cyber threats and develop collective defense. To secure the future, Indo-Pacific nations must prioritize cybersecurity investments, workforce development, and regional collaboration to diminish threats, develop resilience, and protect both national and economic security.

REFERENCES

1. Bansal, U. (2021). A review on ransomware attack. 2021 2nd International Conference on Secure Cyber Computing and Communications (ICSCCC),
2. Bay, M. (2016). What is cybersecurity. French Journal for Media Research, 6, 1-28.
3. Creemers, R. (2022). China's emerging data protection framework. Journal of Cybersecurity, 8(1), tyac011.
4. George, A. S. (2024). Emerging Trends in AI-Driven Cybersecurity: An In-Depth Analysis. Partners Universal Innovative Research Publication, 2(4), 15-28.
5. Gomez, M. A., Sukin, L., & Winger, G. (2023). Alliance Commitments and Cybersecurity in the Indo-Pacific.
6. Goutam, R. K. (2015). Importance of cyber security. International Journal of Computer Applications, 111(7).
7. Gultom, R. A. G., Supriyadi, A. A., & Kustana, T. (2018). Strengthening Asean Cyber Cooperation in Countering Cyber Terrorist Groups Activities on the Internet by Implementing the Six-Ware Cyber Security Framework. Journal: INTENATIONAL JOURNAL OF MANAGEMENT AND INFORMATION TECHNOLOGY, 13(1).
8. Hakata, K., & Cannon, B. J. (2022). The Indo-Pacific as an emerging geography of strategies. In Indo-Pacific Strategies (pp. 3-21). Routledge.
9. Haunts, S. (2019). What Are Data Breaches? In Applied Cryptography in. NET and Azure Key Vault: A Practical Guide to Encryption in. NET and. NET Core (pp. 1-10). Springer.
10. He, K., & Feng, H. (2020). The institutionalization of the Indo-Pacific: problems and prospects. International Affairs, 96(1), 149-168.
11. Heiduk, F., & Wacker, G. (2020). From Asia-Pacific to Indo-Pacific: significance, implementation and challenges.
12. Herrmann, D. (2019). Cyber espionage and cyber defence. Information Technology for Peace and Security: IT Applications and Infrastructures in Conflicts, Crises, War, and Peace, 83-106.
13. Jenkinson, A. (2022). Ransomware and cybercrime. CRC Press.
14. Kalra, K., & Tanwar, B. (2023). Cyber security policy in India: Examining the issues, challenges, and framework. In Cybersecurity issues, challenges, and solutions in the business world (pp. 120-137). IGI Global Scientific Publishing.
15. Kokaji, A., & Goto, A. (2022). An analysis of economic losses from cyberattacks: based on input–output model and production function. Journal of Economic Structures, 11(1), 34.
16. Kuerbis, B., & Badiei, F. (2017). Mapping the cybersecurity institutional landscape. Digital Policy, Regulation and Governance, 19(6), 466-492.
17. Lee, H.-W. (2019). Proposal of Enhancing National Cybersecurity Legal Framework: Focusing on Case Study of Australia Cybersecurity. Law Journal, 67, 311-340.
18. Lika, R. A., Murugiah, D., Brohi, S. N., & Ramasamy, D. (2018). NotPetya: cyber attack prevention through awareness via gamification. 2018 International Conference on Smart Computing and Electronic Enterprise (ICSCEE),
19. Ludvigsen, K. R., Nagaraja, S., & Daly, A. (2022). Preventing or mitigating adversarial supply chain attacks: A legal analysis. Proceedings of the 2022 ACM Workshop on Software Supply Chain Offensive Research and Ecosystem Defenses,
20. Lusthaus, J. (2024). Reconsidering Crime and Technology: What Is This Thing We Call

Cybercrime? Annual Review of Law and Social Science, 20(1), 369-385.
21. Murphy, T., & Nagy, S. (2024). Middle Power Cyber Security Cooperation in the Indo-Pacific: An Analysis Through the Lens of Neo-Middle Power Diplomacy. The Journal of Intelligence, Conflict, and Warfare, 7(1), 1-24.
22. Pelaggi, S., & Termine, L. (2023). Understanding the Indo-Pacific. Handbook of Indo-Pacific Studies, 29.
23. Ray, T., & Vats, A. (2023). Cyber mercenaries: a call to action for the Quad. In Cyber mercenaries: a call to action for the Quad: Ray, Trisha| uVats, Antara. New Delhi, India: ORF, Observer Research Foundation.
24. Thomas, K., Li, F., Zand, A., Barrett, J., Ranieri, J., Invernizzi, L., Markov, Y., Comanescu, O., Eranti, V., & Moscicki, A. (2017). Data breaches, phishing, or malware? Understanding the risks of stolen credentials. Proceedings of the 2017 ACM SIGSAC conference on computer and communications security,
25. Ukhanova, E. (2022). Cybersecurity and cyber defence strategies of Japan. SHS Web of Conferences,
26. Wallis, J., & Batley, J. (2020). How does the 'Pacific'fit into the 'Indo-Pacific'? The changing geopolitics of the Pacific Islands. Security Challenges, 16(1), 2-10.
27. Davis, A., & Balls, J. (2019). The Indian Ocean Region in the 21st Century: geopolitical, economic, and environmental ties.
28. Prabhakar, A. C. (2024). Colonial Echoes: Unraveling Economic Legacies and Geopolitical Shifts in the South Pacific Islands. African and Asian Studies, 1(aop), 1-29.
29. Bachhawat, A., Cave, D., Kang, J., Rajagopalan, R. P., & Ray, T. (2020). Critical technologies and the Indo-Pacific. Australian Strategic Policy Institute.[Electronic resource] URL: https://s3-ap-southeast-2. amazonaws. com/ad-aspi/2020-10/Critical% 20technologies_0. pdf.
30. Linkov, I., Trump, B. D., Poinsatte-Jones, K., & Florin, M. V. (2018). Governance strategies for a sustainable digital world. Sustainability, 10(2), 440.
31. Lehto, M. (2022). Cyber-attacks against critical infrastructure. In Cyber security: Critical infrastructure protection (pp. 3-42). Cham: Springer International Publishing.
32. Oyadeyi, O. O., Oyadeyi, O. A., & Bello, R. O. (2024). Cybercrime in the Asia-Pacific Region: A Case Study of Commonwealth APAC Countries. Commonwealth Cybercrime Journal, 2, 130-160.
33. Martinez, M. L. K. (2024). The European Union's emerging Indo-Pacific presence in terms of security cooperation (Master's thesis).
34. AZUBUIKE, C. F. (2023). Cyber security and international conflicts: An analysis of state-sponsored cyber attacks. Nnamdi Azikiwe Journal of Political Science, 8(3), 101-114.
35. AlDaajeh, S., & Alrabaee, S. (2024). Strategic cybersecurity. Computers & Security, 141, 103845.
36. Segal, A., Akimenko, V., Giles, K., Pinkston, D. A., Lewis, J. A., Bartlett, B., ... & Noor, E. (2020). The future of cybersecurity across the Asia-Pacific. asia policy, 15(2), 57-114.
37. Haruko, W. (2020). The" Indo-Pacific" concept: geographical adjustments and their implications.
38. Zhong, H., & White, M. (2017). South China Sea: Its importance for shipping, trade, energy and fisheries. Asia-Pacific Journal of Ocean Law and Policy, 2(1), 9-24.
39. Kaushiva, V. A. P., & Singh, C. A. (Eds.). (2014). Geopolitics of the Indo-Pacific. KW Publishers Pvt Ltd.
40. Gill, B., Lockyer, A., Lim, Y. H., & Tan, A. T. (2024). Geopolitics, Military Modernisation and the Future of the Indo-Pacific. Taylor & Francis.
41. Jędrzejowska, K. (2023). Political economy of the Indo-Pacific development. Handbook of Indo-Pacific Studies, 51.
42. Bhaskar, N. J. (2021). India's developing economic ties with the Indo-Pacific. Observer Research Foundation, 26.

43. Pullamaraju, P. (2024). Charting India's Path in the Global Technology Landscape A Comparative Policy Study (Doctoral dissertation, School of Public Policy in Partial Fulfilment of the Requirement for the Degree of Master of Public Policy (MPP) 2021-23 Pranitha Pullamaraju HP22PPOL0100026 Under the Supervision of Dr Kanica Rakhra Assistant Professor Kautilya School of Public Policy, Gandhi Institute of Technology and Management).
44. Storey, I. (2016). Rising Tensions in the South China Sea: Southeast Asian Responses. The South China Sea dispute: Navigating diplomatic and strategic tensions, 147.
45. Bukhari, S. R. H., Khan, A. U., Haq, I. U., & Ullah, T. (2024). The geopolitical implications of Taiwan-China relations on regional security. Spry Contemporary Educational Practices, 3(1).
46. Beckley, M. (2017). The emerging military balance in east asia: How china's neighbors can check chinese naval expansion. International Security, 42(2), 78-119.
47. Panda, J. P., & Gunasekara-Rockwell, E. (2021). Quad Plus and Indo-Pacific. London: Routledge.
48. Mirkamolova, G. J. Q. (2024). FOSTERING REGIONAL UNITY: THE ROLE OF SOUTHEAST ASIAN NATIONS IN INTERNATIONAL ORGANIZATIONS. XXI Asr: Fan va ta'lim masalalari (XXI век: Вопросы науки и образования), 3(3), 124-136.
49. Sano, K., & Rassias, M. (2024). Economic Diplomacy: Strategies for Enhancing Trade and Investment in a Globalized World.
50. Priyadarshini, I. (2019). Introduction on cybersecurity. Cyber security in parallel and distributed computing: Concepts, techniques, applications and case studies, 1-37.
51. Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. Electronics, 12(6), 1333.
52. Afaq, S. A., Husain, M. S., Bello, A., & Sadia, H. (2023). A critical analysis of cyber threats and their global impact. In Computational Intelligent Security in Wireless Communications (pp. 201-220). CRC Press.
53. Farahbod, K., Shayo, C., & Varzandeh, J. (2020). Cybersecurity indices and cybercrime annual loss and economic impacts. Journal of Business and Behavioral Sciences, 32(1), 63-71.
54. Blaskovic, A. K., Rusk, J. D., Parker Jr, V. C., & Payne, B. R. (2022, October). Cybercrime and intellectual property theft: An analysis of modern digital forensics. In Proceedings of the Future Technologies Conference (pp. 536-542). Cham: Springer International Publishing.
55. Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. Energy Reports, 7, 8176-8186.
56. Watney, M. (2022, June). Cybersecurity threats to and cyberattacks on critical infrastructure: a legal perspective. In Proceedings of the 21st European Conference on Cyber Warfare and Security. Available: https://papers. academic-conferences. org/index. php/eccws/issue/view/7/8.
57. Alghazzawi, D. M., Hasan, S. H., & Trigui, M. S. (2014). Information systems threats and vulnerabilities. International Journal of Computer Applications, 89(3).
58. Fakhouri, H. N., Alawadi, S., Awaysheh, F. M., Hani, I. B., Alkhalaileh, M., & Hamad, F. (2023). A comprehensive study on the role of machine learning in 5G security: Challenges, technologies, and solutions. Electronics, 12(22), 4604.
59. Bellamkonda, S. (2021). Strengthening Cybersecurity in 5G Networks: Threats, Challenges, and Strategic Solutions. Journal of Computational Analysis and Applications, 29(6).

60. Bachhawat, A., Cave, D., Kang, J., Rajagopalan, R. P., & Ray, T. (2020). Critical technologies and the Indo-Pacific. Australian Strategic Policy Institute.[Electronic resource] URL: https://s3-ap-southeast-2. amazonaws. com/ad-aspi/2020-10/Critical% 20technologies_0. pdf.
61. Oyadeyi, O. O., Oyadeyi, O. A., & Bello, R. O. (2024). Cybercrime in the Asia-Pacific Region: A Case Study of Commonwealth APAC Countries. Commonwealth Cybercrime Journal, 2, 130-160.
62. Bhakti, A., Sudirman, A., Sumadinata, R. W. S., & Bainus, A. (2024). State Defense Strategy in Facing Cyber Threats After Hacking Incidents on Government Institutions: A Case Study in Indonesia. Journal of Human Security, 20(1), 109-117.
63. Gupta, C. M. (Ed.). (2023). Financial crimes: A guide to financial exploitation in a digital age. Springer Nature.
64. Sarowa, S. K., Bhanot, B., & Kumar, V. (2022, December). Analysis of Cyber Attacks and Cyber Incident Patterns over APCERT Member Countries. In 2022 4th International Conference on Artificial Intelligence and Speech Technology (AIST) (pp. 1-6). IEEE.
65. Lehto, M. (2022). Cyber-attacks against critical infrastructure. In Cyber security: Critical infrastructure protection (pp. 3-42). Cham: Springer International Publishing.
66. Haridas, R., Sharma, S., Bhakar, R., & Gu, C. (2025). Cybersecurity Threats to Critical Energy Infrastructure in India: Challenges, Opportunities and Insights for Developing Nations. The Commonwealth Cyber Journal (CCJ), 3, 53-78.
67. Livier, J. (2024). The Cyber Policies Behind Critical Infrastructure: A Look at the Preparedness of the Top Nuclear Energy-Producing Nations.
68. Chang, L. Y., & Wei-Liu, H. (2022). Ensuring Cybersecurity for Digital Services Trade. JW Kang et al.
69. Kayes, A. S. M., Rahayu, W., Dillon, T., Shahraki, A. S., & Alavizadeh, H. (2024). Safeguarding Individuals and Organisations from Privacy Breaches: A Comprehensive Review of Problem Domains, Solution Strategies, and Prospective Research Directions. IEEE Internet of Things Journal.
70. Moulton, S. (2024). Cybersecurity and Trade: The Increasing Use of Cybersecurity Measures and their Impact on International Trade.
71. Fang, C. C. X. (2023). Finance and technology: why fintech is the future of finance–a case study of Singapore's financial sector.
72. Schulzke, M. (2018). The politics of attributing blame for cyberattacks and the costs of uncertainty. Perspectives on Politics, 16(4), 954-968.
73. Gandhi, R., Sharma, A., Mahoney, W., Sousan, W., Zhu, Q., & Laplante, P. (2011). Dimensions of cyber-attacks: Cultural, social, economic, and political. IEEE Technology and Society Magazine, 30(1), 28-38.
74. Singh, T. K. (2024). India's Cybersecurity Policy: Evolution and Trend Analyses. Taylor & Francis.
75. Rugina, J. M. (2023). Through the eyes of attackers: A comprehensive analysis of cybersecurity strategies in international relations. Afro Eurasian Studies, 12(1), 40-57.
76. Christine, D., & Thinyane, M. (2020). Cyber resilience in asia-pacific: a review of national cybersecurity strategies.