BRICS and the Quest for a Global Cybersecurity Framework: Implications for Defence Strategies in the Indo-Pacific

Shivangi Shrivastava

Abstract

This study explores the contributions of BRICS (Brazil, Russia, India, China, South Africa) and the Quad (United States, India, Japan, Australia) in shaping the global cybersecurity framework, with a specific emphasis on the Indo-Pacific region. As the Indo-Pacific becomes increasingly vital for global trade and technological progress, it is also facing rising cybersecurity threats, such as state-sponsored cyberattacks, espionage, and attacks on critical infrastructure. Both BRICS and the Quad contribute to the development of global cybersecurity norms, but their approaches often differ. BRICS advocates for a multipolar, decentralised model that emphasises digital sovereignty, while the Quad supports a liberal, rules-based order. This research explores how these differing perspectives influence regional cybersecurity and defence strategies, with particular attention to India's unique role in bridging both groups. It also identifies potential areas for collaboration, such as joint capacity building and tackling cybercrime, alongside competitive issues, especially between China and the US. The study considers the implications of these dynamics for Indo-Pacific defence, emphasising the need for cooperation between BRICS and the Quad to strengthen regional cyber resilience and stability. Recommendations include the creation of a BRICS-Quad cybersecurity forum and the promotion of transparent cyber norms to foster trust and develop effective defence strategies.

Keywords: BRICS, QUAD, Indo-Pacific, Cybersecurity, Defense

Introduction

By 2040, the Indo-Pacific region, comprising around 40 economies, is expected to contribute more than 50 percent of the world's Gross Domestic Product (GDP). The combined economic output of nations such as China, Japan, India, South Korea, and Australia has already surpassed that of the entire European Union (EU). In recent years, this diverse and rapidly expanding region has drawn significant attention from countries such as Canada, the United Kingdom, the United States, and Australia, all of which have formulated their own strategies for engagement. A notable example of this is the AUKUS partnership, a trilateral security pact designed to bolster military cooperation and advance a range of sophisticated capabilities, particularly in areas such as cybersecurity, artificial intelligence (AI), quantum technologies, and other emerging fields. This collaborative initiative aims to enhance military coordination and ensure preparedness for future challenges.

Beyond economic, defence, and geopolitical considerations, the Indo-Pacific has also become a critical battleground for technological competition. Key areas of contention include semiconductor production in Taiwan, the intensifying rivalry between the United States and China, and growing concerns regarding cyber activities linked to the Chinese government. Moreover, policymakers must navigate the complex task of balancing cybersecurity with content regulation and moderation, all while countering the increasing cyber threats posed by both state-sponsored and independent actors.

In response, regional organisations such as the Association of Southeast Asian Nations (ASEAN) and the Quadrilateral Security Dialogue (Quad) have sought to address these challenges by prioritising the enhancement of cyber capabilities, safeguarding critical infrastructure, and fostering resilience across the region. However, cyberspace has largely mirrored the broader geopolitical conflicts unfolding in the Indo-Pacific. Earlier this year, a leak from a Chinese company revealed that China had been engaging in cyber espionage against several governments in the region, including targeting telecom companies in Pakistan, Mongolia, and Malaysia, as well as specific sectors of the Indian government.

India has responded by strengthening its cyber capabilities, establishing the National Cyber Agency in 2018, and conducting its own advanced persistent threat (APT) operations.

Meanwhile, Pakistan has been expanding its cyber capabilities, with groups such as APT36 allegedly targeting Indian organisations. In Southeast Asia, the APT32 group, linked to Vietnam, has carried out cyber-attacks against human rights activists in Vietnam and targeted organisations in the Philippines and Laos. The growing prevalence of these cyber operations highlights the close relationship between digital landscapes and geopolitical tensions in the region. (Hurel, et.al., 2024).

A report from cybersecurity firm Sophos in 2021 revealed that 78 percent of businesses in India had fallen victim to ransomware attacks, highlighting the growing frequency of such cybercrimes. This trend is not confined to India; it has progressively affected countries across the Indo-Pacific region, many of which have been among the most frequent targets of ransomware attacks in recent years. Even more concerning is that these attacks are no longer limited to private companies; they are increasingly targeting critical infrastructure and key organisations that are vital to national security. This shift underscores the fact that the digital realm has become a battleground, posing significant risks to even the most secure and essential entities.

In November 2022, a wave of cyberattacks hit Vanuatu, a small island nation in the Pacific, severely disrupting its government networks and crippling vital services. This incident serves as a stark example of how ransomware can cause substantial damage, not only financially but also in terms of widespread chaos. A similar event occurred in 2020 when the Colonial Pipeline cyberattack led to significant fuel shortages on the East Coast of the United States, further illustrating the vulnerability of essential infrastructure.

Ransomware attacks are not merely about financial gain. They reveal the complex nature of the digital landscape, where such attacks can be driven by a combination of economic, political, and even military motives. As these threats continue to escalate, ransomware is increasingly being recognised as a major national security concern, with far-reaching impacts on both governments and businesses alike (Tiwari, 2023)

BRICS and the QUAD: Impact on Global Cybersecurity

Cybersecurity is increasingly becoming a major concern, not only for BRICS nations but for countries across the globe. As both governments and businesses become ever more reliant on interconnected infrastructures, commonly referred to as "smart" systems, these networks are emerging as prime targets for cyberattacks, particularly when essential services are at

risk. Regardless of the size of an organisation, whether it is a small business or a large corporation, the threats are substantial, as cybercriminals can disrupt operations or gain access to confidential information.

With the growing use of connected devices and online services, individuals are becoming more vulnerable to cyber risks, often without a clear understanding of the potential dangers. Many people remain unaware of how their personal data is collected and utilised, frequently without their explicit consent or knowledge, leaving them exposed to various forms of cybercrime and digital threats. As our lives become increasingly intertwined with the online world, these risks continue to escalate, affecting everyone from private individuals to major global organisations. (Belli et al., (n.d) Pg. no. 22-23)

The BRICS nations are Brazil, Russia, India, China, and South Africa—are becoming increasingly influential in both economic and political spheres. As their reliance on technology and the internet continues to grow, they are facing escalating cybersecurity threats, particularly those targeting critical infrastructure. These countries encounter similar challenges in cyberspace, including the malicious use of artificial intelligence, underscoring the need for greater collaboration in cybersecurity.

One successful approach adopted in other areas is the Information Sharing and Analysis Centre, which collects and disseminates intelligence on cybersecurity threats and vulnerabilities to help safeguard against attacks. In recent years, there has been growing interest in establishing a BRICS Information Sharing and Analysis Centre to strengthen cooperation in cybersecurity. However, the formation of such a group presents its own set of challenges. These include the complexities of coordinating efforts among member nations, securing adequate funding, building trust, overcoming language barriers, and navigating differing legal and regulatory frameworks.

Certain researchers, such as Belli, have explored the need for updated legislation on cyber defence and cyber warfare within BRICS nations. Others, including Wanglai, have emphasised the importance of forming a dedicated working group within BRICS to facilitate information exchange and best practices, as well as creating coordination points in each member country to tackle cybercrime. Despite these initiatives, there is still no single entity overseeing comprehensive cybersecurity collaboration among the BRICS nations (Malatji & Matli, (2023) pg. no. 116-117)

The Indo-Pacific region holds differing levels of significance for various nations, shaped by

their distinct interests and perspectives. Nevertheless, the four Quad nations India, Japan, Australia, and the United States share a common understanding of the region's importance in both geopolitical and economic terms. During the two thousand and tens, while each of these nations faced a range of cyber challenges, they collectively recognised China's growing assertiveness in cyberspace as a significant cybersecurity threat.

Until the year two thousand and fifteen, the United States sought to address China's expanding cyber capabilities by encouraging it to operate within a framework of global rules and standards. This approach was formalised with the United States-China Cyber Agreement, signed by Presidents Obama and Xi Jinping. Despite revelations that Chinese hackers had been monitoring India for more than a decade, the United States remained hopeful that it could curb China's ambitions in cyber espionage. However, in the years that followed, cybersecurity tensions between China and the Quad nations became increasingly pronounced.

In Japan, Chinese cyber-attacks on industrial and governmental sectors intensified political and economic mistrust. In the year two thousand and sixteen, it was revealed that a Chinese hacking group known as Bronze Butler had infiltrated Japanese companies for several years, exacerbating Japan's security concerns. Australia's anxieties regarding cybersecurity also deepened. The Foreign Policy White Paper of the year two thousand and seventeen not only addressed industrial espionage but also stressed the necessity of protecting critical infrastructure and countering misinformation. In the year two thousand and twenty, Prime Minister Scott Morrison publicly warned of the escalating threat posed by state-sponsored cyber-attacks against national institutions.

India's concerns over Chinese cyber threats grew significantly following the border clashes in the Galwan Valley in the year two thousand and twenty. In the months that followed, India experienced power outages, with investigations revealing that cyber-attacks were responsible for the disruptions, particularly in Mumbai, where a major attack occurred in October. Meanwhile, the United States remained the only Quad member with an official mechanism for publicly attributing responsibility for cyber-attacks. Since the establishment of the Cybersecurity and Infrastructure Security Agency in the year two thousand and seventeen, the United States has routinely identified Chinese threat actors as being responsible for various cyber-attacks, including espionage and assaults on critical infrastructure.

Ultimately, China's increasing assertiveness in cyberspace became the primary concern that unified the Quad nations. Their shared apprehensions drove them to strengthen their cooperation and prioritise cybersecurity when they reinforced their partnership in the year two thousand and twenty (Scholz, 2023).

Diverging Cybersecurity Approaches: BRICS vs. QUAD

Over the past ten years, digital security has become a key priority for BRICS nations, with a particular focus on cybersecurity. This journey began in the year two thousand and thirteen during the BRICS Summit in Durban, South Africa, where leaders acknowledged the growing importance of a secure and accessible cyberspace. The eThekwini Declaration underscored the need for globally recognised cybersecurity norms, standards, and practices.

A significant turning point came with Edward Snowden's revelations, which strengthened collaboration on digital policies among BRICS nations. Each country began developing its own cybersecurity strategy, introducing laws, policies, and regulations tailored to its specific priorities. In the year two thousand and fifteen, the BRICS Ufa Declaration formally solidified this partnership, leading to the establishment of a Working Group on Security in the Use of Information and Communication Technologies. This group was tasked with identifying effective solutions to common cybersecurity challenges and encouraging the exchange of information regarding information and communication technology policies and initiatives.

That same year, BRICS ICT ministers formally signed a Memorandum of Understanding to promote cooperation in science, technology, and innovation, further reinforcing their collaborative efforts. This agreement paved the way for various initiatives, including the BRICS Digital Partnership, the BRICS Partnership for a New Industrial Revolution, the Innovation BRICS Network, and the BRICS Institute of Future Networks. These initiatives have fostered a comprehensive approach to collaboration, integrating policy-making, technological advancement, and research.

Although BRICS nations initially held differing perspectives on cybersecurity, their views have increasingly aligned in recent years on key digital policy matters. Issues such as data protection, data security, the regulation of online content, and cybercrime have emerged as shared priorities, reflecting a collective commitment to shaping the digital future in a way that balances security, innovation, and national sovereignty (Manager, 2022).

During the Quad Leaders' Meeting on the twenty-fourth of May, two thousand and twenty-two, a commitment to strengthening cybersecurity and safeguarding digital ecosystems was reaffirmed. To enhance the security of software services and products, steps are being taken to establish common security practices among the Quad governments. Standard cybersecurity protocols for critical infrastructure are being developed, and the Quad Cyber Challenge is being introduced an initiative aimed at raising public awareness and encouraging better cybersecurity practices.

The Quad Cybersecurity Partnership is dedicated to bolstering capabilities and sharing vital information throughout the Indo-Pacific to enhance regional security. Since September two thousand and twenty-one, an extensive review of existing policies and guidelines has been undertaken to identify the most effective security measures for software services and critical infrastructure. While each Quad nation has its own distinct priorities and strategies, they share a unified goal: to strengthen cybersecurity. By implementing these strategies, significant progress can be made in securing digital environments.

Beyond national efforts, regional partners are being supported through the promotion of best practices, the improvement of product security, and the reinforcement of defences against cyber threats. Another key priority is ensuring that telecommunications infrastructure is built upon reliable and trustworthy vendors. In today's interconnected world, the importance of secure and resilient networks cannot be overstated. Efforts are being made to explore open and interoperable solutions that function seamlessly across all Quad nations.

These initiatives reflect a shared commitment to advancing cybersecurity, enhancing regional capabilities, and ensuring that the Indo-Pacific region is equipped with secure, transparent, and dependable digital infrastructure (Quad Senior Cyber Group Joint Cybersecurity Statement the American Presidency Project, n.d.)

India: The Bridge Between BRICS and the Quad

India's participation in the Quad forum alongside the United States, Japan, and Australia as well as its active role in the BRICS summit, highlights the country's evolving approach to 'multi-alignment'. However, viewing Indian foreign policy purely through the lens of 'alignment' tends to obscure the significant distinctions in India's relationships with major global powers (Mohan, 2022).

Within the Quad, India collaborates with fellow democratic nations the United States, Japan,

and Australia to address key security concerns, particularly in relation to maritime security and countering China's expanding influence in the Indo-Pacific region. These partnerships are centred on maintaining regional stability and upholding the balance of power.

Simultaneously, within BRICS, India works alongside other emerging economies, including China, to tackle pressing global challenges such as economic development and the creation of more inclusive frameworks for global governance. The emphasis here is on advocating for a multipolar world order, ensuring that nations from the Global South have a more substantial voice in shaping international affairs.

India's distinct significance lies in its ability to bridge these two spheres, acting as a link between the Global North, represented by the Quad, and the Global South, represented by BRICS. By leveraging its position in both alliances, India skilfully balances its security priorities with its commitment to economic cooperation and global equity, all while navigating complex geopolitical dynamics. This delicate equilibrium enables India to maintain strategic flexibility and exert considerable influence in shaping the future course of international relations (Kumar, 2024)

However, India's official stance on cyber governance has been somewhat ambiguous. While the country's position has evolved in its expression, the underlying sentiment reveals discomfort with the current internet governance framework, which is largely shaped by Western nations. This is particularly relevant as Western countries advocate for their commercial interests, viewing the internet as a free trade zone, whereas nations like India are still grappling with issues related to access and inclusion. As a result, India is keen to support a government-led system over a market-driven one. In a speech delivered by an Indian official at Netmundial in April 2014, the term "equinet" was used to describe the characteristics associated with the internet's original purpose.

These differing perspectives, while aimed at keeping the internet "free" and promoting it as a "global common good," have often placed India at odds with the United States, Europe, and other countries during international discussions on internet governance. It is reasonable to infer that the BRICS members share a similar viewpoint to India's, as they do not fully support the multi-stakeholder internet governance models championed by Western nations. Interestingly, despite the varied opinions on internet governance within the BRICS countries, some members of civil society remain optimistic that BRICS could offer a fresh perspective on global internet governance (Observer Research Foundation n.d.)

India's cyber policy aims to create a more robust and secure digital landscape within the country. It focuses on establishing a comprehensive regulatory framework, which includes the appointment of a Chief Information Security Officer (CISO) within organisations. The CISO would be responsible for overseeing cybersecurity concerns and ensuring that organisations allocate a designated budget for cybersecurity initiatives. Additionally, the policy has led to the establishment of a National Critical Information Infrastructure Protection Centre (NCIIPC) to manage and address emergencies relating to critical information infrastructure. The policy also mandates periodic audits to assess the effectiveness of existing security systems.

In contrast, the Quad Cybersecurity Partnership follows a different approach. Rather than being a regulatory framework, it is primarily a collaborative initiative aimed at enhancing cybersecurity cooperation across the Indo-Pacific region. A key component of the Quad's efforts is the Quad Cybersecurity Day campaign, which seeks to raise awareness of cybersecurity issues and provide guidance and support to vulnerable communities. This initiative is being launched in partnership with businesses, non-profit organisations, educational institutions, and local communities to ensure a wide-reaching impact. The Quad is also placing a strong emphasis on safeguarding telecommunications technology, particularly in light of the expansion of 5G and other advanced technologies, to ensure a secure and open digital landscape among its member nations (Bhattacharya, (2022) pg. no. 3-4)

India's stance on the Quad and BRICS ought to be informed by a realistic appraisal of its national interests. The Quad constitutes a vital platform for responding to China's assertive behaviour in the Indo-Pacific, whilst BRICS offers a unique opportunity to engage with a diverse group of emerging economies and shape the global agenda. India's success in navigating this complex landscape will depend on its ability to leverage its distinctive position as a bridge between these two competing blocs. By fostering dialogue and cooperation, India can contribute to the creation of a more stable and equitable global order (Garnayak, 2024).

Rising Cybersecurity Threats in the Indo-Pacific

The Indo-Pacific region, home to some of the world's fastest-growing economies, is rapidly advancing its digital infrastructure. As these markets expand, the influence of multinational

technology companies referred to as "cyber kingmakers" is becoming increasingly evident. These companies, wielding power akin to that of nation-states in the digital sphere, are poised to have a significant impact on which entities succeed in shaping the region's online environment.

At the same time, nations in South and Southeast Asia are aligning more closely with the United States, while China is establishing itself as a prominent contender in the global power struggle. These countries are leveraging their strategic importance to safeguard their interests, and may compel multinational corporations to recognise their "digital sovereignty," particularly in sectors such as cloud computing, artificial intelligence, digital currencies, and governance.

As elections face growing threats from cyberattacks, technology companies that manage critical digital infrastructure are playing an increasingly vital role in protecting democratic systems. Election interference, ranging from disinformation campaigns to direct attacks on electoral systems, poses a significant threat not only to the integrity of elections but also to the stability of governments and societies (SentinelOne, 2024). In Cambodia's 2018 election, a Chinese organisation known as TEMP. Periscope allegedly gained access to the National Election Commission. Targeting both governmental bodies and pro-democracy supporters, they employed spear-phishing and surveillance techniques, raising serious concerns about foreign interference in domestic elections. In 2021, New Zealand's intelligence agencies attributed a cyberattack on parliamentary entities to Advanced Persistent Threat 40 (APT40), a group linked to China. This incident marked a significant escalation in Chinese cyber intrusions into Western political institutions. That same year, Chinese cyber groups particularly APT31 were reported to have accessed email accounts within the UK Parliament. During the same period, hackers connected to China breached the UK Electoral Commission, underlining Beijing's interest in Britain's democratic infrastructure. Between May and October 2021, Chinese hackers infiltrated Indian government offices, extracting more than 5.49GB of data underscoring China's intent to gather intelligence on the internal affairs of other nations (India Today, 2024).

Japan has revealed that over 200 cyberattacks in the past five years, targeting the nation's national security and advanced technology information, have been linked to the Chinese hacking group MirrorFace. The National Police Agency's investigation into these attacks, which took place between 2019 and 2024, uncovered that they were part of a coordinated

effort by China to acquire confidential data. The cyberattacks affected a range of targets, including Japan's Foreign and Defence ministries, its space agency, and individuals such as politicians, journalists, and private companies involved in cutting-edge technology. Japan is now urging government agencies and businesses to bolster their cybersecurity measures (Yamaguchi, 2025).

North Korea has become an increasing cybersecurity threat in the Indo-Pacific region, largely due to its growing cyber capabilities, which it uses to support its military and nuclear ambitions. In 2023, the Federal Bureau of Investigation (FBI) identified the Lazarus Group, a hacking organisation linked to the North Korean government, as responsible for stealing $100 million in cryptocurrency from Harmony Horizon, a cross-chain bridge for Ethereum. The same group was also behind the theft of $41 million in cryptocurrency from Stake, an online casino platform. In July 2023, Jenny Jun, a Research Fellow at Georgetown University's Center for Security and Emerging Technologies, testified before the House Foreign Affairs Committee Subcommittee on the Indo-Pacific. She emphasised that North Korea regularly utilises its cyber capabilities for a variety of national objectives, including stealing cryptocurrency to fund its nuclear and missile programmes and conducting espionage on organisations researching COVID-19 (Wiley, 2024).

Strengthening Regional Cyber Resilience: The Role of BRICS and the QUAD

The recent BRICS summit underscored the growing significance of technological cooperation, particularly in artificial intelligence (AI), as a driving force for digital economies. China, as a leader in AI development, has spurred growing interest among other BRICS nations to bolster their capabilities in this area. The UAE, recognised for its focus on AI and high readiness in the field, has contributed further expertise to enhance the group's technological strength. AI-powered innovations present BRICS with the potential to strengthen its competitive edge in offering digital solutions, particularly within the Indo-Pacific region. In response, the Quad nations may need to accelerate their own AI strategies to match BRICS' advancements, as AI rapidly becomes a cornerstone of the global digital economy.

The focus on AI also intersects with discussions on cybersecurity, with Russia and China advocating for state-controlled cyberspaces. The summit highlighted the importance of cybersecurity standards and digital sovereignty. These initiatives could challenge the efforts

led by the Quad, positioning BRICS as a serious competitor in the global cybersecurity arena. Notably, the summit also addressed the need for safeguards to protect national data systems, which will directly influence the security of digital networks across the Indo-Pacific region. In turn, the Quad may need to strengthen its collaborative cybersecurity initiatives to counter the increasingly sophisticated strategies being devised by BRICS.

BRICS reaffirmed its commitment to advancing digital economies through initiatives such as the New Development Bank's (NDB) digital transformation programmes, which aim to improve digital infrastructure across emerging economies. The NDB, also known as the BRICS Development Bank, plays a key role in financing infrastructure and sustainable development. The summit also highlighted cooperation in blockchain and fintech, signalling BRICS' growing influence in shaping the digital economy of the Indo-Pacific. As BRICS continues to expand, its impact in sectors such as digital payment technologies and secure 5G networks is expected to increase, posing a direct challenge to the Quad's position. Companies like Huawei are at the forefront of 5G development within BRICS, while Quad nations must prioritise the enhancement of security and transparency in their own 5G networks to maintain competitiveness.

The Quad's model of digital openness also faces challenges. To retain its influence in the Indo-Pacific region, the Quad may need to develop more definitive policies that strike a balance between digital sovereignty and openness (Sabzal, 2024). By harmonising regulations and implementing standard practices, the Quad nations can establish a more unified and efficient approach to managing cyber incidents, reduce administrative burdens, and achieve improved security outcomes at lower costs. Aligning regulations can strengthen global collaboration, contributing to a more resilient and secure digital environment that protects critical infrastructure and enables a swift and coordinated response to cyber incidents. Standards play a vital role in this process, as they provide a consistent and widely recognised foundation for cybersecurity practices, foster interoperability, and enhance cooperation among nations (Patil, 2025).

In contrast, BRICS has been working to assert national control over cyberspace, with initiatives aimed at reducing dependence on US-led technological systems. With an expanding membership and a growing focus on AI and cybersecurity, BRICS is crafting a multifaceted strategy that could rival the Quad's influence in the region. This evolving landscape highlights the need for a deeper understanding of how digitalisation is reshaping

geopolitics in the Indo-Pacific.

Both BRICS and the Quad are leveraging technology as a tool for geopolitical leverage, though in differing ways. BRICS, with its commitment to a multipolar world, seeks to promote dialogue between civilisations and improve digital access in underserved regions, particularly in Africa. In contrast, the Quad aims to strengthen its position in the Indo-Pacific and counterbalance China's growing influence. In this competition, BRICS agreements tend to be more binding due to the multilateral relationships among its members, while Quad agreements are generally more flexible.

China's central role within BRICS shapes the group's agenda, often positioning itself against Western influence. The Quad, in turn, seeks to counter China's assertiveness in the Indo-Pacific, with India playing a key role in maintaining a balance between competition and collaboration within both alliances (Kumar, 2024). From a practical perspective, both alliances have their own unique principles, strategies, and goals. Each member of the QUAD and BRICS has joined the coalition based on their national interests, with India being the only country that is a member of both groups. India's ambitions are challenging to decipher because of its ambiguous approach in its interactions with both alliances (Sabzal, 2024).

Looking ahead, the impact of emerging technologies, such as post-quantum computing and widespread AI, will further shape the geopolitical landscape. While opportunities for collaboration between BRICS and the Quad may arise, it is more likely that the two factions will increasingly find themselves at odds, each advancing its own digital initiatives. This competition is expected to significantly influence the future of digital geopolitics in the Indo-Pacific region. (Kumar, 2024).

Recommendations for Advancing Cybersecurity Governance in the Indo-Pacific

Safeguarding Critical National Infrastructure (CNI) remains a key priority across the regions examined. This is typically achieved either by revising existing cybersecurity standards or by broadening them to cover sectors beyond the essential CNI to better protect supply chains. As these requirements evolve, international companies and cybersecurity professionals must navigate the varying and often inconsistent regulations across different regions. Further research is needed to explore the different definitions of CNI and the specific cybersecurity needs associated with each sector.

A widespread shortage of cybersecurity experts and the urgent need for improved skills training is a shared issue in all the regions studied. In response, several regions have introduced various initiatives, many of which share common goals such as attracting talent, diversifying the workforce, and fostering international collaboration. For example, frameworks such as the NICE Cybersecurity Workforce Framework in the United States or the European Cybersecurity Skills Framework (ECSF) have been implemented to standardise the terminology used to describe cybersecurity roles. However, there is insufficient data on the effectiveness of these initiatives in significantly reducing the cybersecurity workforce gap in measurable terms. Further investigation is necessary to determine which approaches are most successful in addressing this issue (Global Approaches to Cyber Policy, Legislation and Regulation, n.d.).

Although countries may adopt different strategies, there is a shared recognition that cyberspace is a critical domain for both national security and international relations. Events such as the Russian invasion of Ukraine, concerns about foreign surveillance, and the growing demand for regime security highlight the shifting dynamics of global cybersecurity. These changes suggest that nations are pursuing various approaches to develop and leverage their cyber capabilities. While not all countries disclose the motives behind their efforts to advance their cyber capabilities, their actions indicate that current global guidelines for responsible state conduct in cyberspace are insufficient to ensure compliance.

To effectively counter cyber threats posed by state actors, it is vital to invest in cyber capabilities. It is perhaps understandable that there is a reliance on cyber capabilities to uphold international laws and standards, especially given that military power is essential for enforcing these frameworks.

For cyber capabilities to genuinely serve as effective diplomatic tools, it is crucial for countries to clarify their intentions. Similar to military strength, building cyber capabilities without transparency can create uncertainty, often resulting in a lack of trust. While no nation is required to disclose every detail of its cybersecurity systems, it is essential for countries to demonstrate their commitment to the United Nations' global framework for responsible state conduct in cyberspace. This can be achieved by clearly defining their cyber policies, implementing strong oversight, and fostering open communication with both international and domestic partners. These initiatives not only enhance the operational effectiveness of cybersecurity measures but also contribute to the broader stability and

security of the global cyber landscape. As nations strengthen their cyber strategies, building trust through confidence-building measures becomes a crucial element (Cyber Capabilities in the Indo-Pacific: Shared Ambitions, Different Means? n.d.)

Navigating the Future of Cybersecurity Cooperation in the Indo-Pacific

Monash University has teamed up with the Oceania Cyber Security Centre (OCSC) to launch a programme designed to strengthen cybersecurity across the Indo-Pacific region. The Post-Quantum Cryptography in the Indo-Pacific Programme (PQCIP) aims to equip organisations and government bodies in 11 nations with the essential skills required to protect against future cyber threats from quantum computers. The initiative will focus on countries such as Malaysia, Indonesia, Papua New Guinea, and others in the region, offering free training on advanced cryptography techniques.

Associate Professor Ron Steinfeld, the Project Director at Monash University's Faculty of Information Technology, emphasised the critical role of encryption in protecting data from breaches. As quantum computers evolve, they may have the potential to undermine existing encryption methods. "We're seeing a concerning rise in cyberattacks and data breaches," Steinfeld said, stressing the need for Indo-Pacific nations to address current cyber threats while also preparing for the challenges presented by future developments in quantum technology.

The PQCIP will adopt a comprehensive approach, providing tailored education, thorough assessments of existing cybersecurity frameworks, and expert guidance to help these countries bolster their defences against both current and future threats. This initiative reflects the region's growing recognition of the importance of cybersecurity in an increasingly digital world (Apdr, 2022).

Tackling disinformation requires a collaborative, multinational approach. Working closely with partner nations is vital not only for amplifying the effectiveness of these efforts but also for presenting a united front against harmful activities. Local knowledge, trusted by the communities it serves, is essential for enhancing the impact of these initiatives. As technology and global geopolitical dynamics evolve, future strategies for information warfare must be adaptable, cooperative, and innovative. This means staying alert, responding swiftly to threats, and fostering global collaboration to tackle emerging challenges. Countries can only effectively combat the growing issue of disinformation and

protect the integrity of information worldwide by working together (Hanson et al., 2024).

Conclusion

The evolving cyber landscape in the Indo-Pacific region has underscored the urgent need for robust cybersecurity measures and international cooperation. Both BRICS and the Quad have emerged as key players in the development of global cybersecurity norms, but their approaches reflect differing geopolitical and ideological priorities. BRICS seeks to create independent cybersecurity initiatives that align with its broader strategic objectives, focusing on digital sovereignty and multipolar governance. In contrast, the Quad advocates for a liberal, rules-based digital framework, promoting open and interoperable cybersecurity standards to enhance regional resilience.

India's role as a bridge between these two groups underscores its strategic importance in fostering cybersecurity cooperation. With its dual membership, India has the opportunity to mediate between differing perspectives, encouraging collaboration to address cyber threats such as state-sponsored attacks, ransomware, and disinformation campaigns. However, managing its relationships with both BRICS and the Quad requires careful diplomacy to navigate complex geopolitical tensions.

The rising frequency of cyber threats targeting critical infrastructure, elections, and private enterprises highlights the need for stronger regional cybersecurity measures. The proposal to establish a BRICS-Quad cybersecurity forum offers a promising opportunity to promote transparency, build trust, and develop joint defence strategies in the digital domain. Furthermore, investments in strengthening cyber capabilities, developing skills, and embracing emerging technologies such as AI and quantum cryptography will be essential for enhancing cyber resilience across the Indo-Pacific.

Ultimately, the future of cybersecurity governance in the Indo-Pacific will be shaped by the shifting power dynamics between BRICS and the Quad. While competition between these alliances is inevitable, areas of common interest, such as combating cybercrime and securing critical digital infrastructure, offer opportunities for cooperation. By adopting a collaborative and forward-thinking approach, regional actors can strengthen cybersecurity resilience and ensure a secure and open digital future.

References

- Apdr. (2022). Future-proofing cybersecurity in the Indo-Pacific region - APDR. APDR. https://asiapacificdefencereporter.com/future-proofing-cybersecurity-in-the-indo-pacific-region/?
- Belli, L. et.al. (n.d.) CyberBRICS: Cybersecurity regulations in the BRICS countries (By Sergio Suchodolski & Sizwe Snail; L. Belli, Ed.) https://cyberbrics.info/wp-content/uploads/2020/11/CyberBRICS-Book-FINAL-author-version-1.pdf
- Bhattacharya, D. (2022). India's Cyber Security Policy: Strategic Convergence and Divergence with Quad [Issue Brief] pg.no. 3-4. https://www.isdp.eu/wp-content/uploads/2022/08/Brief-Aug-19-2022-Debopama_.pdf
- Cyber capabilities in the Indo-Pacific: shared ambitions, different means? (n.d.). Royal United Services Institute. https://www.rusi.org/explore-our-research/publications/commentary/cyber-capabilities-indo-pacific-shared-ambitions-different-means?
- Garnayak, S. (2024, July 23). India's delicate dance: Balancing geopolitical ambitions in the Quad and BRICS. The Central Wire. https://thecentralwire.com/opinion/indias-delicate-dance-balancing-geopolitical-ambitions-in-the-quad-and-brics/
- Global approaches to cyber policy, Legislation and Regulation. (n.d.). Royal United Services Institute. https://www.rusi.org/explore-our-research/publications/special-resources/global-approaches-cyber-policy-legislation-and-regulation?
- Hanson, R., et.al. (2024). The Future of Indo-Pacific Information Warfare: Challenges and Prospects from the Rise of AI. RAND. https://www.rand.org/pubs/research_reports/RRA2205-1.html?
- Hurel, L.M. et.al., (2024). Cyber Capabilities in the Indo-Pacific: Shared Ambitions, Different Means? Royal United Services Institute. https://rusi.org/explore-our-research/publications/commentary/cyber-capabilities-indo-pacific-shared-ambitions-different-means
- India Today. (2024, October 29). Spy games: When Chinese hackers targeted foreign polls, governments. https://www.indiatoday.in/world/story/spy-games-when-chinese-hackers-targeted-foreign-polls-governments-2625122-2024-10-29

• Kumar, S. (2024). Indo-Pacific Strategies of BRICS and the Quad: Digitalization as a Geopolitical tool – analysis. Eurasia Review. https://www.eurasiareview.com/19112024-indo-pacific-strategies-of-brics-and-the-quad-digitalization-as-a-geopolitical-tool-analysis/?

• Malatji, M. & Matli, W. (2023). The Potential Benefits and Challenges of a BRICS+ Agency for Cybersecurity Intelligence Exchange, Journal of Information Security and Cybercrimes Research, Volume 6 Issue (2) file:///C:/Users/power/Downloads/2419-Manuscript%20(Without%20Author%20Details)%20_-21352-1-10-20240109.pdf

• Manager, C. (2022). Cybersecurity convergence in the BRICS countries. CyberBRICS. https://cyberbrics.info/cybersecurity-convergence-in-the-brics-countries/?

• Mohan, C. R. (2022, July 6). Between the BRICS and the Quad: India's new internationalism. Institute of South Asian Studies, National University of Singapore. https://www.isas.nus.edu.sg/papers/between-the-brics-and-the-quad-indias-new-internationalism/

• OBSERVER RESEARCH FOUNDATION. (n.d.). orfonline.org. https://www.orfonline.org/article/lessons-from-brics-developing-an-indian-strategy-on-global-internet-governance

• Patil, S. (2025, March 12). Strengthening the Quad's regulatory diplomacy on cybersecurity. orfonline.org. https://www.orfonline.org/research/strengthening-the-quad-s-regulatory-diplomacy-on-cybersecurity

• Quad Senior Cyber Group Joint Cybersecurity Statement | The American Presidency Project. (n.d.). https://www.presidency.ucsb.edu/documents/quad-senior-cyber-group-joint-cybersecurity-statement?

• Sabzal, N. (2024, October 5). Indian ambiguity between QUAD and BRICS. Modern Diplomacy. https://moderndiplomacy.eu/2024/10/05/indian-ambiguity-between-quad-and-brics/

• Scholz, T. (2023). Quad Vadis? A risk assessment of the QUAD's emerging cybersecurity partnership. Orfonline.org. https://www.orfonline.org/research/quad-vadis-a-risk-assessment-of-the-quad-s-emerging-cybersecurity-partnership

• SentinelOne. (2024) . Pinnacle One Exec Brief | Cyber Gray Zone risks in the Indo-Pacific. SentinelOne. https://www.sentinelone.com/blog/pinnacleone-execbrief-cyber-gray-zone-risks-in-the-indo-pacific/

• Tiwari, S. (2023). Ransomware: A Wake-Up Call for Cybersecurity in the Indo-Pacific, The Diplomat https://thediplomat.com/2023/01/ransomware-a-wake-up-call-for-cybersecurity-in-the-indo-pacific/

• Yamaguchi, M. (2025). Japan links Chinese hacker MirrorFace to dozens of cyberattacks targeting security and tech data | AP News. AP News. https://apnews.com/article/japan-police-cyberattack-china-government-68adcb293b2931da4c30ca0279720124

ABOUT THE AUTHOR

Shivangi Shrivastava is currently pursuing her Ph.D. at IIS (Deemed to be University), Jaipur, Rajasthan, with a focus on Indian foreign policy and the strategic role of the Quad in the Indo- Pacific region. Alongside her research, she also serves as a visiting faculty member at the university. Her work explores key issues such as maritime security, nuclear dynamics involving Russia, North Korea, and Iran, and connectivity initiatives like the Asia-Africa Growth Corridor as a counter to China's Belt and Road Initiative. She has published in reputed journals including the South India Journal of Social Sciences and IIS University Journal of Social Sciences, and have contributed chapters to edited volumes on undersea cable security and geopolitical challenges.