Issue Brief
August 19, 2022

India's Cyber Security Policy:

Strategic Convergence and Divergence with Quad

Debopama Bhattacharya

Photo credit: Thitichaya Yajampa / Shutterstock

The rise in cyber-attacks across the Indo-Pacific and beyond has necessitated a robust and a common approach towards cyber-resilient information infrastructure in the region. The Quad has taken a good leadership role in this regard through the Joint Cyber Principles of Quad Cybersecurity Partnership. India has had a cyber-security policy since 2013 and has since been working to mitigate cyber threats at source. A nodal cyber-security agency, a strong regulatory framework, a center for protection of critical infrastructure, periodic audits, have all successfully built a strong cyber-security architecture in the country. The cyber-security policy of India shares many common principles with the Quad Joint Cyber Principles. India's already existent cyber-security architecture can help realize some of the Quad goals like that of sharing of intelligence across agencies and a collective cyber-security workforce. This issue brief analyzes the magnitude of cyber threats in the Indo-Pacific region, particularly within the Quad nations, the convergence and divergence of India's cyber-security policy with that of Quad and the importance of a shared cyber-security goal among the Quad nations.

The cyber domain in India expanded massively against the backdrop of the COVID-19pandemic to include a wide spectrum of Information and Communications Technology (ICT)-enabled devices and services. From vaccine administration to financial technology, a major transformation was seen in the Indian economy; much like a social plan with a focus on 'inclusive growth through ICT'. As such, the need for a secure cyber ecosystem became a foundational necessity. The National Cyber Security Policy of India was framed in 2013 with a vision to build a 'secure and resilient cyberspace' for all.[1] The policy facilitates seamless economic transactions in the cyberspace and helps achieve broader strategic goals like a 'free and open Indo-Pacific'.

With the increasing occurrence of malicious cyber activities across the Indo-Pacific, new and evolving security architecture is being witnessed in the region. The May 24 Tokyo Summit of the

Quadrilateral Security Dialogue (Quad) recognized the importance of cyber-security in the Indo-Pacific and the need for a coordinated approach to focus on cyber capacity building among the member-states.[2] India being an emerging economy and an important Quad nation also recognizes the importance of a robust cyber-security architecture as crucial to its national security as well as the security of the Indo-Pacific region.

> ***With the increasing occurrence of malicious cyber activities across the Indo-Pacific, a new and evolving security architecture is being witnessed in the region, and the importance of this was recognized at May 24 Tokyo Summit of the Quad.***

The Threat Landscape

Increased digitization and sophisticated technologies have unintentionally multiplied the potential entry points and scope of cyber-attacks. In March 2022, a suspected Pakistan-linked threat actor Transparent Tribe, also known as APT36, targeted the Indian government and military organizations by use of fake domains that mimicked legitimate organizations to deliver malware.[3] In January 2022, a major cyber-attack from the advanced persistent threat (APT) actor Blue Noroff, took place on cryptocurrency startups affecting various small and medium sized organizations in the U.S. and worldwide causing huge financial losses as reported by Kaspersky.[4] In November 2021, networks in the U.S. and Australia were attacked by ransomware, planted by suspected Iranian hackers to either disrupt the critical infrastructure or for a profit motive.[5] Earlier in April 2021, the U.S. faced a cyber-attack in which various federal agencies got compromised through vulnerabilities found in Pulse Connect Secure's virtual private networking (VPN) software.[6] In the same month, Japan faced a breach allegedly by threat actor Tick believed to be linked to China, through a compromised rental server in which several businesses and research institutes were affected, including the Japanese Aerospace Exploration Agency.[7] With the rising number of cyber threat actors operating in the Indo-Pacific either for cyber-espionage or profit motive, the transition to a cyber-resilient security architecture among the Quad nations with a common cyber-security goal can be witnessed.

Importance of a Shared Cyber-security Goal

Exploitation of the cyberspace by both state and non-state actors is an ongoing and ever increasing concern. The World Economic Forum's (WEF) Global Cybersecurity Outlook 2022, has reported a 151 percent increase in ransomware attacks in the first six months of 2021, and on average 31 percent increase over 2020, making it a top cyber risk concern.[8] Other cyber risk concerns cited by the report are social engineering and malicious insider activity among organizations; and identity theft and critical infrastructure failure among cyber leaders. An attack on the critical information infrastructure of nations, could cause large disruptions in the functioning of governments and extensive harm to the economy and security of the volatile Indo-Pacific region. A unified and coordinated approach through multilateral arrangements like the Quad would help in building a cyber-secure region.

The Joint Cyber Principles of the Quad Cybersecurity Partnership[9] recognize the risk that cyber threats pose to national security and therefore aim to strengthen the cyber-security architecture of the four Quad nations to be more resilient to cyber threats. It emphasizes on enhancing the 'collective

cyber security workforce' and 'pool of talented cyber professionals'. And focuses on intelligence sharing mechanisms, rapid identification, investigation and remediation by which attacks could be mitigated at the source. The four Quad nations have reaffirmed their vision of a 'free and open Indo-Pacific' in the latest summit by 'shared recognition' about the increasing complexity of cyber-attacks and the need for cooperation in pandemic response and climate change.[10] The leadership role for critical-infrastructure protection was given to Australia, India would lead in supply-chain resilience and security, Japan in workforce development while talent and software security standards would be led by the United States as per the latest dialogue.[11]

> ***The Joint Cyber Principles of the Quad Cybersecurity Partnership recognize the risk that cyber threats pose to national security and therefore aim to strengthen the cyber-security architecture of the four Quad nations to be more resilient to cyber threats.***

India's Cyber-security Policy and the Quad

The cyber-security policy of India converges with the Quad in its mission to build a secure and resilient cyberspace, a cyber-force of working professionals to prevent as well as respond to cyber-attacks and minimize damages from various threat vectors in the cyberspace.[12] The policy focuses on a well-coordinated approach through a combination of organizations, both public and private, people and technology. Along with this, it aims to create a culture of responsible user behavior in the cyberspace and respect user data privacy. It has stressed upon a global cooperation in this regard. A shared vision with Quad can be seen in leveraging relationships among the nations, an effective public-private partnership and collaborative engagements through technical and operational cooperation and contribution for enhancing security of the cyberspace.

> ***The World Economic Forum's Global Cybersecurity Outlook 2022, has reported a 151 percent increase in ransomware attacks in the first six months of 2021, and on average 31 percent increase over 2020, making it a top cyber risk concern.***

India's cyber-security framework is an evolving one which serves as a guide for individual sectors to design their own cyber-security policies. The Quad's cyber-security principles in a similar manner serve as an excellent guide for nations in the Indo-Pacific to build cyber resilience. The Quad intends to strengthen information-sharing among the Computer Emergency Response Teams (CERTs) of its members and exchange best practices and lessons learned among them. India's cyber-security policy has operationalized 24x7 national Level CERT-In to function as a nodal agency for cyber-security related matters. The "Quad Fellowship" would provide students from Quad countries an opportunity to pursue their career in STEM fields in the U.S. and bring together the finest minds of these countries to help innovate and research in technology.[13] The cyber-security policy of India similarly focuses on frontier technologies and

solution-oriented research. Quad members are committed to "responsible innovation" in critical and emerging technologies due to which the Critical and Emerging Technologies Working Group was launched in 2021.

India and Australia, earlier on February 12, 2020, in the Foreign Ministers' Cyber Framework Dialogue, in a joint statement reaffirmed their commitment to a free, open, secure, peaceful and an interoperable cyberspace and technologies adhering to international law.[14] The two nations also recognized bilateral cooperation in the areas of cyber governance, capacity building, critical technologies and more to further strengthen the India-Australia relationship. India has continued to deepen its strategic ties with fellow Quad member Japan through the "India-Japan Digital Partnership"[15] in technology cooperation in areas of 5G, startups, the ICT sector, cyber security among others. In the Fourth Annual U.S.-India 2+2 Ministerial Dialogue, held in April 2022, the two countries recognized the importance of an open, secure, interoperable and stable cyberspace; and confirmed their intent to work closely to counter the use of ICT for criminal purposes and the growing national cyber-security threats from both state and non-state actors.[16]

> ***The cyber-security policy of India converges with the Quad in its mission to build a secure and resilient cyberspace, a cyber-force of working professionals to prevent as well as respond to cyber-attacks and minimize damages from various threat vectors in the cyberspace.***

> ***A 'shared recognition' and a unified cyber response among the Quad members will offer a greater security in this regard and help in countering China's digital dominance in the Indo-Pacific.***

India's cyber policy aims to strengthen the regulatory framework in order to ensure a secure cyber ecosystem in the country. The framework encourages a Chief Information Security Officer (CISO) in all organizations who would be responsible for matters related to cyber security and also a specific cyber-security budget for organizations. As per the policy, a National Critical Information Infrastructure Protection Centre (NCIIPC) has been created, for response, resolution and crisis management of critical information infrastructure in the country and design security, development and use of information resources. The policy mandates a periodic audit and evaluation of the effectiveness of information security infrastructure with respect to the regulatory framework.

The Quad Cybersecurity Partnership on the other hand is a joint partnership rather than a regulatory framework, aiming to guide cyber-security cooperation and support across the Indo-Pacific region. The Quad initiated the first of its kind Quad Cybersecurity Day campaign to create cyber-security awareness by generating tips and information to the most vulnerable sections of the society. It will be launched in collaboration with industry, non-profit organizations, academia, and communities to increase its reach. The Quad's focus would also be on 5G and other advanced technologies in order to keep open and secure telecommunications technology among countries.

Conclusion

The cyberspace has no geographic limit. With the rise in critical and emerging technologies, a new world order can be seen where cyber-security is being prioritized. A 'shared recognition' and a unified cyber response among the Quad members will offer a greater security in this regard and help in countering China's digital dominance in the Indo-Pacific. The joint military exercise of the Quad, the Malabar, was widely viewed as a response to increased Chinese military dominance in the East and South China seas. Joint cyber principles in this rapidly changing threat environment, would help prevent cyber-attacks and deliver quick and effective response to any cyber incident in the region.

The Indian cyberspace too is expanding, with sophisticated technologies, digital solutions, more ICT services and financial technology, etc., influencing the economy positively and thereby catalyzing growth. The cyber policy of India and Quad cyber-security principles emphasize the importance of fundamental values and principles, adoption of global best practices in ICT and a rules-based international order. This is the key to creation of a robust cyber-security architecture in the Indo-Pacific to help combat cyber threats in the region, in harmony with the global cyber-security ecosystem.

Author –

Debopama Bhattacharya *is a cyber-security analyst. She was previously a cyber-security researcher at the Strategic Technologies Centre, Manohar Parrikar Institute for Defence Studies and Analyses, New Delhi. She is a graduate in Electronics and Instrumentation Engineering from GNIT, India and is currently pursuing a Master's degree in Political Science. Her interest areas include cyber security, artificial intelligence and other emerging technologies.*

About ISDP

The Institute for Security and Development Policy is a Stockholm-based independent and non-profit research and policy institute. The Institute is dedicated to expanding understanding of international affairs, particularly the interrelationship between the issue areas of conflict, security and development. The Institute's primary areas of geographic focus are Asia and Europe's neighborhood..

www.isdp.eu

Endnotes

1 "National Cyber Security Policy -2013," Ministry of Electronics & Information Technology, Government of India, July 2, 2013, https://www.meity.gov.in/sites/upload_files/dit/files/National%20Cyber%20Security%20Policy%20%281%29.pdf.

2 Media Center, Bilateral/Multilateral Documents, "Quad Joint Leaders' Statement," Ministry of External Affairs, Government of India, May 24, 2022, https://www.mea.gov.in/bilateral-documents.htm?dtl/35357/Quad+Joint+Leaders+Statement.

3 Asheer Malhotra, Justin Thattil and Kendall McKay, "Transparent Tribe campaign uses new bespoke malware to target Indian government officials," CISCO Talos, March 29, 2022, https://blog.talosintelligence.com/2022/03/transparent-tribe-new-campaign.html.

4 Seongsu Park and Vitaly Kamluk, "The BlueNoroff cryptocurrency hunt is still on," Securelist by Kaspersky, January 13, 2022, https://securelist.com/the-bluenoroff-cryptocurrency-hunt-is-still-on/105488/.

5 National Cyber Awareness Systems, Alerts, "Iranian Government-Sponsored APT Cyber Actors Exploiting Microsoft Exchange and Fortinet Vulnerabilities in Furtherance of Malicious Activities," Cybersecurity and Infrastructure Security Agency, November 17, 2021, https://www.cisa.gov/uscert/ncas/alerts/aa21-321a.

6 National Cyber Awareness Systems, Alerts, "Exploitation of Pulse Connect Secure Vulnerabilities," Cybersecurity and Infrastructure Security Agency, April 20, 2021, https://www.cisa.gov/uscert/ncas/alerts/aa21-110a.

7 "Chinese military seen behind Japan cyberattacks," *The Japan Times*, April 20, 2021, https://www.japantimes.co.jp/news/2021/04/20/national/chinese-military-japan-cyberattacks/.

8 "Global Cybersecurity Outlook 2022," World Economic Forum in collaboration with Accenture, Insights Report, January 2022: 13-14, https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2022.pdf.

9 "Quad Cybersecurity Partnership: Joint Principles," Ministry of Foreign Affairs of Japan, May 23, 2022, https://www.mofa.go.jp/files/100348060.pdf.

10 Statements and Releases, "FACT SHEET: Quad Leaders' Tokyo Summit 2022," The White House, May 23, 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/23/fact-sheet-quad-leaders-tokyo-summit-2022/.

11 Ibid.

12 "National Cyber Security Policy -2013," Ministry of Electronics & Information Technology, Government of India, July 2, 2013, https://www.meity.gov.in/sites/upload_files/dit/files/National%20Cyber%20Security%20Policy%20%281%29.pdf.

13 Statements and Releases, "Joint Statement from Quad Leaders," The White House, September 24, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/09/24/joint-statement-from-quad-leaders/.

14 Joint Media Statement, Melbourne, "Joint Statement on the Inaugural India-Australia Foreign Ministers' Cyber Framework Dialogue," February 12, 2022, https://www.foreignminister.gov.au/minister/marise-payne/media-release/joint-statement-inaugural-india-australia-foreign-ministers-cyber-framework-dialogue.

15 "Brief Note on India-Japan Bilateral Relations," Ministry of External Affairs, Government of India, February 2020, https://mea.gov.in/Portal/ForeignRelation/India-Japan_Bilateral_Brief_feb_2020.pdf.

16 Media Note, Office of the Spokesperson, "Fourth Annual U.S.-India 2+2 Ministerial Dialogue," US Department of State, April 11, 2022, https://www.state.gov/fourth-annual-u-s-india-22-ministerial-dialogue/.