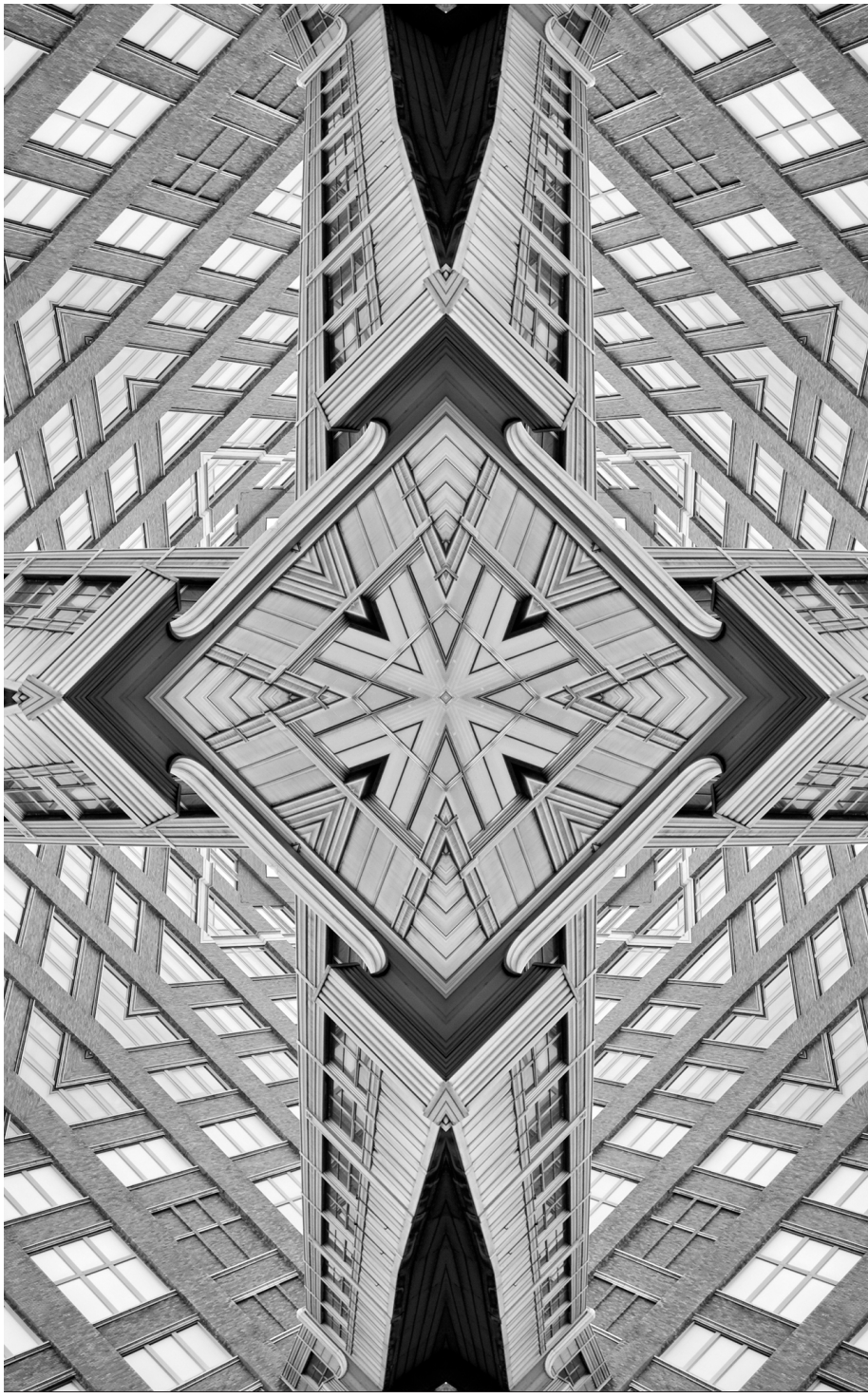
Issue Brief

ISSUE NO. 692
FEBRUARY 2024

ORF OBSERVER RESEARCH FOUNDATION



Fixing Cyber Vulnerabilities: An Agenda for the Quad

Rajeswari Pillai Rajagopalan

Abstract

The COVID-19 pandemic sparked rapid digitalisation worldwide, with work-from-home interactions, online payments, and online consultations for various services becoming acceptable practices. While this shift in the manner and nature of work brought enormous benefits, crucially in terms of access, it has also increased the kind of cyber security threats that countries face, with vulnerabilities felt particularly in the health and financial sectors. India and the Quadrilateral Security Dialogue (Quad) countries are especially vulnerable in these areas and other critical infrastructure, making it imperative to jointly address the weaknesses to build better cyber resilience in their respective jurisdictions. This brief presents an overview of the situation in the four countries and recommends measures to strengthen and streamline the cyber security agenda at the national and Quad levels.

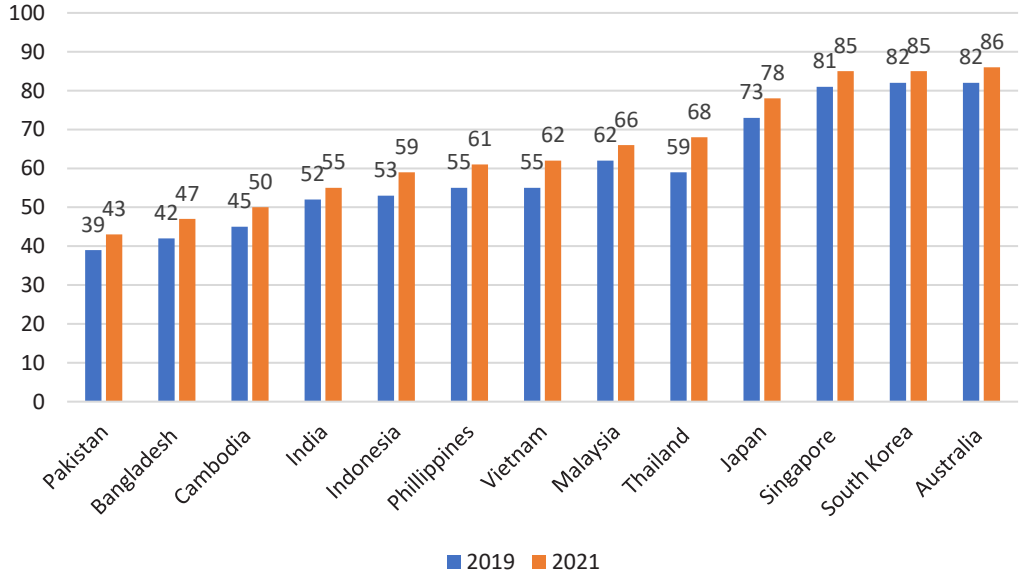
Attribution: Rajeswari Pillai Rajagopalan, "Fixing Cyber Vulnerabilities: An Agenda for the Quad," *ORF Issue Brief No. 692*, February 2024, Observer Research Foundation.

Introduction

In recent years, particularly following the COVID-19 pandemic, countries worldwide, including those in the Quadrilateral Security Dialogue (Quad; India, the US, Australia, and Japan), have embraced digital technologies and digitalisation at an accelerated pace. Amid rapid digitisation, work-from-home interactions, online consultations for various services, especially healthcare and medical delivery systems, and online education (edtech) opportunities have become more acceptable and accessible.

Notably, internet penetration in India and the broader Asia-Pacific region was underway long before the onset of the pandemic. Indeed, even before the pandemic forced greater digitisation worldwide, the Asia-Pacific region had the highest number of internet users. However, Europe and the Americas had better overall internet penetration rates.

Figure 1: Digital Trends in the Asia Pacific (2019 and 2021)



Source: GSM Association[1]

The number of internet users in the broader Asia-Pacific reached over 2.6 billion in 2022, with China and India contributing about half of this number.[2] Many users in the region are young and rely on mobile phones to access the

internet; the number of mobile internet users increased from 1,090 million in 2019 to 1,290 million in 2022.[3] Amid this expansive access and the growth of edtech, e-commerce, and fintech services (both before and due to the pandemic), the embrace of digital technologies will only likely expand. However, despite this growth in digital technologies, many countries are yet to institute effective cybersecurity measures to counter loopholes and vulnerabilities that have risen therein. The spike in the number of cybersecurity incidents, including on critical infrastructure (for instance, in the Quad countries), highlights the need to build cyber resilience to avoid such incidents. As the number of internet users grows, this problem will only intensify. As such, the Quad countries—particularly India, which is poised to lead the growth in internet users and currently has poor cybersecurity and weak cyber hygiene[a] practices—must address cyber vulnerabilities to build resilience through a concerted cyber security agenda.

“The Quad countries—particularly India, which is poised to lead the growth in internet users and currently has poor cybersecurity and weak cyber hygiene practices—must address cyber vulnerabilities to build resilience through a concerted cyber security agenda.”

a Cyber hygiene is essentially a series of measures that individuals and institutions put in place to reduce cyber vulnerabilities in the form of cyberattacks, including ransomware and phishing attacks.

Cyber Security Incidents in India

In October 2023, media reports indicated that American cybersecurity firm Resecurity had discovered cybersecurity breaches that resulted in the personal information[b] of over 800 million Indian citizens being sold on the dark web. The cybersecurity firm's human intelligence division, HUNTER, stated that the perpetrators of the cyberattack were "willing to sell [the] entire Aadhaar and Indian passport database for $80,000."[4] Earlier, in November 2022, a cyberattack on the All India Institute of Medical Sciences (AIIMS) in New Delhi, a premier medical institution, impacted the hospital's outpatient and inpatient digital services (billing, report generation, and appointment scheduling).[5] The incident appeared to have been a ransomware attack, where the criminals who hacked into the system were reportedly asking for a ransom payment. The culprits allegedly accessed about 40 million patient profiles, including sensitive data and medical records. This likely also included the data of senior government officials who consulted AIIMS for treatment. Ransomware attacks involve perpetrators sending malicious software to obtain illegal access to the victim's data, locking it down, and demanding a ransom not to release it. In 2022, India saw a 53 percent increase in reported ransomware incidents compared to the previous year.[6] In another incident in November 2022, Central Depository Services (India) Limited noticed malware in some of its internal systems but ruled out any potential data breach.[7]

The number of cyberattacks targeting the Indian health sector has risen in recent years. CloudSEK, an AI company that monitors cyber threats, noted in an August 2022 report that, in 2021, the Indian healthcare sector saw the second highest number of attacks after the US; India experienced 7.7 percent of all attacks on the healthcare industry worldwide and 29.7 percent of all attacks in the Asia-Pacific region.[8] The report also noted that "the number of cyberattacks against the healthcare industry [worldwide] has increased by 95.34% in the first 4 months of 2022 as compared to the number of cyberattacks in 2021 during the same period." Indeed, in recent years, major tech companies like Cisco India, CrowdStrike, Cyware and Sophos India have cautioned the country on potential spikes in the number of cyberattacks directed at the healthcare industry.[9] Similarly, Cyfirma, a Singapore-based Goldman Sachs-backed cyber intelligence firm, reported in March 2021 that a Chinese state-backed hacking group, APT-10 (also known as Stone Panda), was targeting IT systems of major Indian COVID-19 vaccine developers such as Bharat Biotech and the Serum Institute of India.[10] Cyfirma also stated that major Indian pharmaceutical

b Individuals' names, phone numbers, addresses, Aadhaar numbers (an Indian national identity system), and passport information.

companies such as the Serum Institute, Bharat Biotech, Dr Reddy's Labs, and Abbot India were coming under cyberattacks by hackers based in Russia, China, and North Korea. The objective behind these attacks had been to get hold of critical vaccine research and trial data to gain a "competitive advantage over Indian pharmaceutical companies." The company detected 15 hacking campaigns—seven from Russia, four from China, three from North Korea, and one from Iran.

Earlier in November 2020, Microsoft noted the spikes in cyberattacks in the health sector came primarily from three non-state actors "targeting seven prominent companies directly involved in researching on vaccines and treatments for Covid-19." The targeted countries included Canada, France, India, South Korea, and the US.[11] Another cybersecurity company, Indusface, referred to the rise in cyberattacks in the health sector, saying that "there were more than 1 million cyber-attacks across Indusface's global healthcare clientele. Of these, 278,000 attacks were reported in India alone."[12] As such, protecting patients' medical and financial data has emerged as a critical challenge for the healthcare industry.

In addition to the healthcare industry, several other critical sectors, particularly the financial sector, were also targeted by cyberattacks. In 2023, India recorded 1,12,474 cybersecurity incidents,[13] with over 4.29 lakh cybersecurity incidents targeting financial institutions in the first half of 2023.

In a November 2022 report, CloudSEK also noted an uptick in cyberattacks on India's banking finance and insurance (BFSI) sector. The report stated that, in 2021, most BFSI cyberattacks were focused in North America, but the focus shifted towards Asia in 2022, and India was characterised as "the newfound hotbed for cyberattacks in Asia."[14] The BFSI sector had been identified as the "most targeted" sector in FY 2021-2022.[15] A comparison of the number of cyber events in 2021 and 2022 reveals that the US, India, and Brazil are among the top five nations dealing with BFSI cyberattacks.

Other critical infrastructures in India have also come under cyberattack, including the airline industry, oil and gas and power sectors, and technology companies, but most of these attacks were contained before any damage could occur.[16]

Importantly, irrespective of whether these attacks lead to data or financial loss, the more critical issue is the ability of perpetrators to crack the Indian cybersecurity system despite India's security efforts. This also reflects the still inadequate protection measures accorded to the critical information infrastructure in India. The government needs to step up its data protection efforts through additional measures to prevent such frequent cyberattacks. The absence of awareness of cyber risks among users and the use of old, legacy technologies are among the factors that add to the vulnerabilities. India also needs to study the evolving tactics, techniques, and procedures of hackers and criminals to prevent such attacks.

"Irrespective of whether cyberattacks lead to data or financial loss, the more critical issue is the ability of perpetrators to crack the Indian cybersecurity system despite India's security efforts. This also reflects the still inadequate protection measures accorded to the critical information infrastructure in India."

Rising Instance of Cyber Incidents in the Quad Countries

Notably, the increasing cyber vulnerabilities and cyber security incidents are not unique to India. This is precisely why cybersecurity cooperation needs to be accelerated among like-minded partners, such as the Quad countries (which have also experienced intense cyberattacks in recent months).

In August 2023, Japan's National Center of Incident Readiness and Strategy for Cybersecurity (NISC) admitted that hackers had infiltrated the institute for many months. Although the Japanese government has not officially identified the source, the Chinese military is suspected to be behind the security breach.[17] In another attack on Japan's critical infrastructure, it was reported in November 2023 that Japan's space agency had come under cyberattack, but the agency clarified that "the information the hackers accessed did not include anything important for rocket and satellite operations."[18] Along with security breaches, Japan is also seeing a growth in the number of ransomware attacks, with the National Police Agency reporting a total of 230 ransomware attacks in 2022,[19] with an 87 percent increase in the number of such attacks in Q1-Q2 of 2022 compared to the previous year.[20] In July 2023, the Port of Nagoya, the largest port in terms of volume, came under a ransomware attack that resulted in a two-day halt of all operations, impacting the exports and imports for many industries, including that of automobile manufacturer Toyota and its partners and suppliers.[21] Along with Japan's automobile industry, medical centres have been particularly targeted.[22] Although the financial aspects of data breaches remain a concern, the "biggest impact" for Japan from cyberattacks was the reported 58 percent data loss.[23]

According to the Australian Cyber Security Centre's 2023 annual threat report, Australia experienced many data breaches, resulting in millions of Australians "having their information stolen and leaked on the darkweb."[24] According to the 2023 annual report, Australia witnessed about 94,000 cybercrime incidents in FY 2022-23, a 23 percent increase from the previous year. A cybercrime was reported every six minutes on average in FY 2022-23, compared to seven minutes on average in the previous year. The top three cybercrimes against individuals were identity fraud, online banking fraud, and online shopping fraud, and against businesses were email compromises, business email compromise fraud, and online banking fraud. The annual threat report released in November 2023 stated a spike in the average cost per cybercrime to AUD 6,000 for small businesses, AUD 97,200 for medium businesses, and AUD 71,600 for large businesses. This meant an increase of 14 percent in terms of the average cost of cybercrime. It also added that the total publicly reported

common vulnerabilities and exposures[c] increased to 20 percent in FY 2022-23. The Australian government has also recognised that the risk of cyber threats continues to grow, with "a greater interest from state actors in Australia's critical infrastructure."[25]

The US is also experiencing significant cyber threat incidents. In its 2023 Annual Threat Assessment, the US Intelligence Community highlighted China's cybercrimes as "the broadest, most active and persistent cyber espionage threat" facing both the US government and the private sector.[26] The growing military-civilian fusion has helped China use the resources at its disposal to undertake what the report highlights as major cyber espionage activities that have included "compromising telecommunications firms, providers of managed services and broadly used software, and other targets potentially rich in follow-on opportunities for intelligence collection, attack, or influence operations." Similarly, data from the Microsoft Digital Defense Report (2022) showed that the US was the most targeted country across multiple cybercrime actors, including Russia, China, Iran and North Korea.[27] Notably, the US healthcare sector accounted for 28 percent of all cyberattacks on the industry in 2021, the most globally.[28]

"The growing military-civilian fusion has helped China use the resources at its disposal to undertake major cyber espionage activities that have included "compromising telecommunications firms, providers of managed services and broadly used software, and other targets potentially rich in follow-on opportunities for intelligence collection, attack, or influence operations."

c Common vulnerabilities and exposure is a programme overseen by the MITRE Corporation, funded by the US Department of Homeland Security. It is essentially a registry that identifies and catalogues known information security-related vulnerabilities and weaknesses, which provide attackers easy access to data or systems in general. For more, see Arfan Sharif, "What is CVE? Common Vulnerabilities & Exposures," *CrowdStrike*, December 8, 2022, https://www.crowdstrike.com/cybersecurity-101/common-vulnerabilities-and-exposures-cve/

Cyber defence is already an urgent priority for the Quad countries, especially in deterring Russia and China. Indeed, the Quad Leaders' joint statements already contain some actionable points.[d] Still, the cybersecurity realities facing India, Japan, Australia, and the US are the ideal context for Quad cooperation on cybersecurity issues. The four countries can take specific measures at the national and organisational level, but there is also scope for the collective implementation of some strategies as a starting point before such cooperation is expanded to involve like-minded partners beyond the Quad.

National/Organisational Level

***Strengthening resilience measures*:** This involves enhancing one's ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources. This should involve measures like developing a comprehensive response plan, building a cybersecurity improvement roadmap, building detection and response capabilities, and building awareness by educating users on escalating threats and instilling better cyber hygiene practices.

***New institutional measures*:** Establishing new institutional measures such as information security officers (ISOs) and cyber security officers (CSOs) at the industry/organisation level are essential to ensure adherence to industry standards; compliance is key. Such officers can take the lead in putting in place processes and institutions that could issue certifications based on compliance and adapting good practices such as cybersecurity awareness within institutions. These can include training and simulation exercises with real-life scenarios so that organisations familiarise themselves with the cyber threats they may need to tackle. They can also conduct mock activities, with the ISO/CSO planning such exercises, to educate all employees in an organisation about better cyber hygiene practices and raise awareness about various emerging threats and cybersecurity-related advisories as issued by the Indian Computer Emergency Response Team (CERT-In), India's nodal cybersecurity agency. It should be the responsibility of the ISO/CSO to relay such advisories to the organisation, ensure that all

d Some of the collaborative measures that the Quad leaders have highlighted over the past few years include strengthening regional capacity and resilience to cyber incidents and threats. The Quad Cyber Challenge, for instance, is meant to generate greater awareness and assist participants across the Indo-Pacific to safeguard against online threats. To enhance cyber defence, the four countries have also engaged in developing Quad Joint Principles for Secure Software and the Quad Joint Principles for Cyber Security of Critical Infrastructures. They have also formulated a guiding framework for addressing supply chain security and resilience. See, The White House, "Quad Leaders' Joint Statement," May 20, 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2023/05/20/quad-leaders-joint-statement/; The White House, "Quad Joint Leaders' Statement," May 24, 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/24/quad-joint-leaders-statement/

understand the seriousness and priority of threats, and inform the organisation about what steps might be taken if an incident occurs.

***Adopting innovative solutions*:** India and its Quad partners should consider specific innovative solutions to its cybersecurity challenge. One potential solution is cyber insurance or cyber liability insurance. Cyber insurance covers various cybersecurity issues, including ransomware and business interruptions from cybersecurity incidents. This may incentivise institutions to establish credible incident-response capabilities. Such capabilities would involve steps like how to respond to an attack to minimise the damage and vulnerabilities, who should be informed and point of contact in the event of an attack, and identifying initial steps to mitigate the adverse effects. Once an attack has been dealt with, the next step is estimating the scale of loss and getting the systems and data back on track. This could involve monitoring whether backups are in place on a cloud or other means and restoring the data. Cloud storage will require securing and periodic assessment of the cloud systems for any gaps in security controls. Another methodology that is gaining some traction is adopting the zero-trust model, which requires all users to be authenticated and authorised before accessing data and resources.[29] This includes all the staff within an organisation, but this programme takes no one or "nothing for granted." Generally, the assumption is that vulnerabilities and weaknesses are outside the organisational network and tend to overlook or ignore any potential weak links in the system. But in several critical infrastructure security areas, such as nuclear security, there is a particular emphasis on insider threats or people who may be inside the system with all the knowledge of the organisation's strengths and weaknesses, who may become vulnerabilities. In this context, any unusual cyber behaviour can be a red flag. Adopting this approach includes "identifying critical data, mapping the flow of this data, logical and physical segmentation, and constant endpoint monitoring with automated threat detection and response capabilities."[30]

***Give up the 'Not My Organisation' approach*:** In today's highly digitised world, it is no longer a question of if but when an organisation will face a cyberattack. As such, organisations should be prepared with a mindset of continuous learning and improvement of processes and policies while ensuring compliance. Also, new training modules should be devised, with training material continually updated based on learnings from incidents that may have happened elsewhere and how these were tackled.

Quad Level

***Strengthen digital connectivity*:** The Quad partners should consider ways and means to strengthen regional digital connectivity by engaging in tech outreach to bridge the digital divide and ensure the whole region can enjoy the economic and social benefits of such access. Indeed, the Quad can do much to strengthen digital connectivity in the broader Indo-Pacific region, as recognised in the 2022 Quad Leaders' Joint Statement.[31] Yet, digital connectivity in the region is still quite uneven. This is an area where the Quad should advance its cooperation with smaller Indo-Pacific powers. This is especially important because, in the context of the intensifying US-China tech war, countries in the region have felt the need for alternatives at the domestic and regional levels, but not every country may have the wherewithal to develop their domestic alternatives. Therefore, finding alternative digitisation options involving Australia, Japan, the US, and India is important for the region. This could emerge as an important piece of the agenda shaping the Quad's collective work in the Indo-Pacific region and working with smaller developing countries to develop genuinely global cybersecurity rules.

***Importance of collective action*:** Addressing the growing number of cybersecurity threats collectively is likely more effective than a series of isolated actions by individual countries. Therefore, building a coalition to take on cybercrime perpetrators is advisable. This would include building regional digital resilience, instituting better cybersecurity practices, and enabling trusted value-based supply chains that remove disruptions and vulnerabilities to enhance digitalisation.

***Sharing of critical intelligence*:** Sharing of threat and vulnerability intelligence to prevent a cybersecurity incident can be done through institutions like the Computer Emergency Response Team (CERT). This could be a collaborative venture among the four cybersecurity organisations in Japan, Australia, the US, and India. Once institutionalised through periodic engagements, it could be expanded to involve other like-minded partners. Similarly, sharing information on new tactics, trends, and targets of cyberattacks and the incident response to these cyberattacks is also vital in stepping up cyber preparedness.[e] This could further expand to Quad training programmes, tabletop exercises, and simulation exercises playing out various contingencies while helping the relevant parties identify ways and means to deal with such crimes.

e In fact, "sharing of threat information, identifying and evaluating potential risks in supply chains for digitally enabled products and services, and aligning baseline software security standards for government procurement, leveraging our collective purchasing power to improve the broader software development ecosystem so that all users can benefit" is already an outcome at the 2022 Quad Leaders' Summit meeting. See White House, "Quad Joint Leaders' Statement," May 24, 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/24/quad-joint-leaders-statement/

Recommendations

***Quad threat and vulnerability index*:** Creating a threat and vulnerability index at the Quad level could prove helpful. This is not necessarily to be distributed publicly, but it can be shared among cybersecurity agencies of the four countries. At the Quad level, studying each other's training modules and seeing if some issues and processes can be incorporated usefully for individual and collective action would be helpful.

***Establish linkage between defence cyber institutions*:** Cyber, like outer space, has also become integral in the conventional security domain, with deep involvement in conventional military operations. Dedicated military cyber institutions have emerged in India and the three Quad partner countries. Developing dialogue mechanisms between the Indian Defence Cyber Agency and its counterparts in the other Quad countries—on driving the defence cyber strategy, to serve as a coordinating body, and create effective linkages between the civilian departments, military, and the private sector—can help strategise and maximise strategic options while minimising vulnerabilities in the military cyberspace.

***Focus on governance measures*:** The lack of consensus has become a significant impediment in instituting new global governance measures. The Quad can create processes that include all countries, irrespective of their growth levels or technology access, to build consensus through smaller coalitions. An inclusive approach requires the broad-based participation of countries. Widening participation in the current state of global politics will likely make it more challenging to reach consensus, but agreement achieved in several smaller groupings can be brought to a larger platform for a more effective multilateral process. This might also allow countries like India, with a foot in the developed and emerging world, to narrow down perceptional differences between the two sides. Countries that are relatively well developed in these technologies but also understand the concerns of the developing world may be in a better position to help address the legitimate concerns of the developed and developing worlds. For instance, India can present the perspective of the Global South to the Quad.

Conclusion

Cybersecurity has become an increasingly sensitive issue affecting the national security of many countries. Democracies are particularly at risk because of their open nature. Until now, democracies have attempted to handle this on their own, but there is a slow realisation that this is no longer viable, leading to greater efforts at coordination. The Quad countries have begun to appreciate the usefulness of collective action in this regard. These efforts are in the early stages, but the four countries recognise the need for joint action because they face a common threat with implications across multiple sectors, including development, health, economy and national security.

Rajeswari Pillai Rajagopalan *is the Director of the Centre for Security, Strategy and Technology (CSST) at ORF.*

Endnotes

1 *Digital Societies in Asia Pacific: Progressing Towards Digital Nations*, GSM Association, August 2022, https://www.gsma.com/asia-pacific/wp-content/uploads/2022/08/Digital-Societies-in-APAC-FINAL.pdf

2 Leander von Kameke, "Internet Usage in the Asia-Pacific Region - Statistics & Facts," Statista, August 31, 2023, https://www.statista.com/topics/9080/internet-usage-in-the-asia-pacific-region/#editorsPicks

3 "Digital Societies in Asia Pacific: Progressing Towards Digital Nations"

4 Kanishka Sarkar, "Massive Dark Web Data Leak Exposes India to Digital Identity Theft and Financial Scams, Warns Resecurity," *CNBC TV18*, October 31, 2023, https://www.cnbctv18.com/technology/massive-dark-web-data-leak-exposes-india-to-digital-identity-theft-and-financial-scams-warns-resecurity-18196331.htm

5 Aishwarya Dabhade, "AIIMS Cyberattack Exposes the Vulnerability of Indian Healthcare," *Moneycontrol*, November 25, 2022, https://www.moneycontrol.com/news/india/aiims-cyberattack-exposes-the-vulnerability-of-indian-healthcare-9599771.html

6 Computer Emergency Response Team (CERT-IN), *India Ransomware Report 2022*, https://www.cert-in.org.in/PDF/RANSOMWARE_Report_2022.pdf

7 "Clearing at CDSL Back to Normal Post Cyber Attack," *The Economic Times*, November 21, 2022, https://economictimes.indiatimes.com/markets/stocks/news/cdsl-completes-fridays-pending-settlement-after-a-cyber-attack/articleshow/95645396.cms

8 Aastha Mittal, Hansika Saxena, and Isha Tripathi, "Increased Cyber Attacks on the Global Healthcare Sector," CloudSEK, August 18, 2022, https://assets-global.website-files.com/635e632477408d12d1811a64/63cfd7034745927b1c74ca2a_Increased-Cyber-Attacks-on-the-Global-Healthcare-Sector-WhitePaper-CloudSEK%20(1).pdf

9 Nandita Vijay, "Indian Healthcare to Prioritize Cyber Security and Put in Place Robust Data Privacy Framework," www.pharmabiz.com, November 2, 2021, https://www.pharmabiz.com/NewsDetails.aspx?aid=143687&sid=1

10 Krishna N. Das, "Chinese Hackers Target Indian Vaccine Makers SII, Bharat Biotech, Says Security Firm," *Reuters*, March 1, 2021, https://www.reuters.com/world/china/chinese-hackers-target-indian-vaccine-makers-sii-bharat-biotech-says-security-2021-03-01/

11 Tom Burt, "Cyberattacks Targeting Health Care Must Stop," Microsoft Blog, November 13, 2020, https://blogs.microsoft.com/on-the-issues/2020/11/13/health-care-cyberattacks-covid-19-paris-peace-forum/

12 Ashish Srivastava "AIIMS Delhi: Held to Ransom by Cyber Attack," *The New Indian Express*, November 28, 2022, https://www.newindianexpress.com/cities/delhi/2022/nov/28/aiims-delhi-held-to-ransomby-cyber-attack-2522960.html

13 "Cyber Attacks Targeted 36 Government Websites in 2023," *PTI*, August 3, 2023, https://www.cnbctv18.com/india/government-websites-hacked-cyber-attacks-in-2023-rajeev-chandrasekhar-17421901.htm

Endnotes

14 CloudSEK, "Cyber Threats Targeting Global Banking & Finance Customers," November 14, 2022, https://www.cloudsek.com/whitepapers-reports/cyber-threats-targeting-global-banking-finance-customers

15 Hansika Saxena, Benila Susan Jacob, and Anshuman Das, "Global Banking & Finance: Threats Facing Customers," CloudSEK, https://assets-global.website-files.com/635e632477408d12d1811a64/63d3a2739332c0c5134beb12_Global-Banking-Finance-threats-facing-customers-Organic2%20(2).pdf

16 "AIIMS Hit by Ransomware Attack: 7 Other Big Hackings that Hurt Indian Businesses," *Gadgets Now (Times of India Group)*, November 27, 2022, https://www.gadgetsnow.com/slideshows/aiims-hit-by-ransomware-attack-7-other-big-hackings-that-hurt-indian-businesses/photolist/95793675.cms

17 Graham Cluley, "Japan's Cybersecurity Agency Admits it was Hacked for Months," Bitdefender, August 30, 2023, https://www.bitdefender.com/blog/hotforsecurity/japans-cybersecurity-agency-admits-it-was-hacked-for-months/

18 "Japan Space Agency Hit with Cyberattack, Rocket and Satellite Info Not Accessed," *Reuters*, November 29, 2023, https://www.reuters.com/technology/cybersecurity/japan-space-agency-hit-with-cyberattack-this-summer-media-2023-11-29/

19 Shimpachi Yoshida, "Ransomware Attacks Surge More than 50% in Japan in 2022," *The Asahi Shimbun*, February 6, 2023, https://www.asahi.com/ajw/articles/14832967

20 "Japan Saw 87% Increase in Ransomware Attacks in First Half of 2022," *Japan Times*, September 15, 2022, https://www.japantimes.co.jp/news/2022/09/15/national/crime-legal/ransomeware-attacks-rise/

21 Yukana Inoue, "No Longer a 'Catastrophe,' Japan's Cybersecurity Could Still Improve," *Japan Times*, July 13, 2023, https://www.japantimes.co.jp/news/2023/07/13/national/japan-cybersecurity-improvements-ransomware/

22 Mikoto Hata, "Japanese Hospitals Increasingly at Risk of Cyberattacks," *The Japan News*, September 26, 2021, https://japannews.yomiuri.co.jp/society/crime-courts/20210926-33177/; "11 Hospitals in Japan Hit by Ransomware Attacks Since 2016," *The Japan News*, Asian News Network, December 30, 2021, https://asianews.network/11-hospitals-in-japan-hit-by-ransomware-attacks-since-2016/

23 *State of Incident Response: Asia Pacific*, Kroll, October 2022, https://www.kroll.com/-/media/kroll/pdfs/publications/apac-state-of-incident-response-2022.pdf

24 Australian Signals Directorate and Australian Cyber Security Centre, *ASD Cyber Threat Report 2022-2023*, https://www.cyber.gov.au/sites/default/files/2023-11/asd-cyber-threat-report-2023.pdf

25 Renju Jose and Byron Kaye, "Australia Says Hacks Surging, State-Sponsored Groups Targeting Critical Infrastructure," *Reuters*, November 16, 2023, https://www.reuters.com/technology/cybersecurity/australia-says-state-sponsored-cyber-groups-targeting-critical-infrastructure-2023-11-15/

Endnotes

26 Office of the Director of National Intelligence, "Annual Threat Assessment of the US Intelligence Community," February 6, 2023, https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf

27 Microsoft, "Microsoft Digital Defense Report 2022," https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE5bUvv?culture=en-us&country=us

28 Mittal, Saxena, and Tripathi, "Increased Cyber Attacks on the Global Healthcare Sector"

29 Andjela, "Cybersecurity Innovation as the Backbone of Digital Transformation," Innovation Cloud, https://innovationcloud.com/blog/cybersecurity-innovation-as-the-backbone-of-digital-transformation.html

30 Andjela, "Cybersecurity Innovation as the Backbone of Digital Transformation"

31 The White House, "Quad Joint Leaders' Statement," May 24, 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/24/quad-joint-leaders-statement/

Images used in this paper are from Getty Images/Busà Photography.

ORF OBSERVER RESEARCH FOUNDATION

Ideas . Forums . Leadership . Impact

20, Rouse Avenue Institutional Area,
New Delhi - 110 002, INDIA
Ph. : +91-11-35332000. **Fax :** +91-11-35332005
E-mail: contactus@orfonline.org
Website: www.orfonline.org