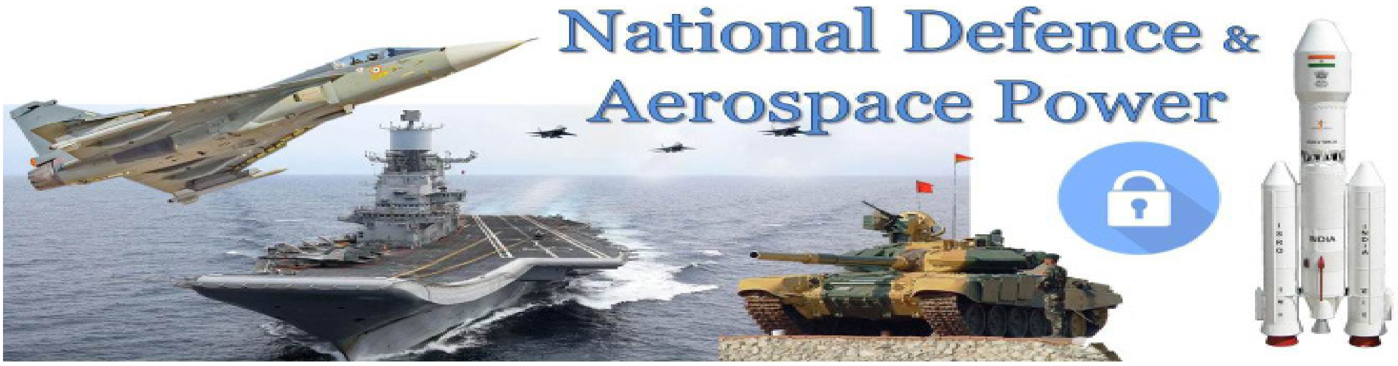
Centre for Air Power Studies



Centre for Air Power Studies ISSUE BRIEF

171/22

06 June 2022

ASSESSING QUAD'S CYBER AGENDA

Divyanshu Jindal

Research Associate, Centre for Air Power Studies

At the recently concluded Quad Leaders' Tokyo Summit, the four partner nations (India, Australia, Japan, and the US) highlighted the importance of cooperation in the cyber domain yet again. The leaders announced the plan to initiate the first-ever Quad 'Cybersecurity Day', and to coordinate capacity building programs in the Indo-Pacific under the 'Quad Cybersecurity Partnership'.[1] Quad cybersecurity will be guided by joint cyber principles to build resilience, and the Quad partners seek to improve their critical infrastructure defences through information sharing among national Computer Emergency Response Teams (CERTs). In addition, Quad will focus on the identification and evaluation of potential risks in supply chains for digitally enabled products and services, and on harnessing critical and emerging technologies to enhance the prosperity and security of the region.[2] While this presents a bird's-eye view of the emerging cyber cooperation dynamic between Quad nations, decoding national cyber policies and strategies can reveal the larger picture. This brief is meant to underline the important aspects of Quad partners' ambitions in cyberspace and estimate the future course for Quad in the cyber domain.

Quad cybersecurity will be guided by joint cyber principles to build resilience, and the Quad partners seek to improve their critical infrastructure defences through information sharing among national Computer Emergency Response Teams (CERTs).

Cyber In Quad: Developments and Achievements

Quad established the 'Critical and Emerging Technology Group' after the Virtual Quad Summit in March 2021,[3] which organized its work around 4 pillars: technical standards, 5G diversification and deployment, horizon-spanning, and technology supply chains.

In September 2021, the collaborative effort resulted in a statement—'Quad Principles on Technology Design, Development, Governance and Use'—at the first-ever in-person 'Quad Leaders' Summit'.[4] The statement underlined the partners' commitment to foster an 'open, accessible, and secure technology ecosystem, based on mutual trust and confidence'; and affirmed that technology should be designed, developed, governed, and used in ways that are shaped by democratic values, and respect for universal human rights. The statement also included commitments toward developing shared research and development agendas, joint capacity building, reducing barriers to data and knowledge sharing, developing competitive technology statements, countering misuse or abuse of technology for malicious activities and terrorist purposes, checking disinformation and keeping pace with changes in the global economy and innovation processes.

The summit launched the 'Quad Senior Cyber Group' for having 'leader-level experts' to advance work between industry and government in areas including adoption and implementation of shared cyber standards, promoting the development of secure software and trustworthy digital infrastructure, and building workforce and talent.

The first Quad Leaders' summit placed cybersecurity cooperation on a priority agenda for the four partners (beside AI and 5G).[5] The group emphasized bringing together the expertise from member nations to drive domestic and international best practices to bolster critical-infrastructure resilience against cyber threats. More significantly, the summit launched the 'Quad Senior Cyber Group' for having 'leader-level experts' to advance work between industry and government in areas including adoption and implementation of shared cyber standards, promoting the development of secure software and trustworthy digital infrastructure, and building workforce and talent.

In a February 2022 joint statement—'Quad Co-operation in the Indo-Pacific'—released by the US Secretary of State and the Foreign Ministers of Governments of Australia, India, and Japan, the partners welcomed the progress on the practical cooperation in countering disinformation and cybersecurity.[6] The statement highlighted Quad's aim to ensure resilient cybersecurity and coordinate efforts across the Indo-Pacific for addressing the growing threats of cybercrime (especially ransomware). It also underlined that Quad seeks to help regional nations in capacity building for implementing the 'UN Voluntary Framework for Responsible State Behaviour in Cyberspace', along with appreciating the US' new exchange programs in the field of cybersecurity and countering disinformation. Recently in March, the Quad's Senior Cyber Group held its first meeting[7] and deliberated on opportunities to extend cybersecurity cooperation, strengthen cyber resilience, and safeguard critical infrastructure. The group framed a 'Work Plan', aimed to further the collaboration among the member nations, and with partners and industry in the region.

National Cyber Strategies and Policies: An Assessment

As a mini-lateral grouping, mapping Quad's vision in the cyber domain can be done through an assessment of each member's international and domestic cyber policy frameworks. Except for India which is due to release an updated National Cyber Security Strategy soon (the last version was released in 2013), the recent national strategies by Australia, Japan and the US can give an indication of the objectives and strategies adopted by the governments.

US' strategies in the cyber domain have evolved and added a newer perspective to its 'deterrence' and 'denial' policies. The Department of Defence (DoD) advocates 'persistent engagement' as a key strategy that seeks to occupy adversaries and deny them the time and resources to carry out cyberattacks.

USA

The Cyberspace Solarium Commission—created in 2019 to establish cybersecurity policy solutions—launched its report in March 2020.[8] It advocated for a 'layered cyber deterrence' strategic approach for cybersecurity that viewed deterrence as an 'enduring American strategy' in cyberspace.[9] It is following a strategic approach to achieve the end state that includes three strategies-

a) Shaping behaviour by working with partners to influence how parties act in cyberspace.

b) Denying benefits by securing critical networks and working to create systemic security.

c) Resiliency in cyberspace and imposing costs by retaliating against malicious actors.

In recent years, US' strategies in the cyber domain have evolved and added a newer perspective to its 'deterrence' and 'denial' policies. The Department of Defence (DoD) advocates 'persistent engagement' as a key strategy that seeks to occupy adversaries and deny them the time and resources to carry out cyberattacks.[10] This strategy promotes the primacy of 'Defend Forward' (DF) concept in US' cyber strategic considerations that aims to disrupt or halt malicious cyber activity at its source. The DF based concept has been articulated in all US cyber strategies since the Command vision for US Cyber command (2018) to the Solarium Commission.[11]

While denial can be achieved by preventing an adversary from launching successful attacks by building partner capabilities through coordinated policies, deterrence can be achieved by influencing adversaries' behaviours by highlighting the weightage of united cyber capabilities of the partner nations. As adversaries in the cyber domain mostly linger at the threshold of waging a significant cyber catastrophe (without actually causing it), the concept of 'Cyber Resilience' has gained currency in recent years. Cyber resilience-based deterrence means having systems in place that minimize the impact of cyberattacks, sustaining operations throughout and post-attack, and recovering and adapting to new conditions after the event.

Australia

In April 2021, the Australian government launched a 'Cyber and Critical Technology International Engagement Strategy, aiming to guide its international engagement to reach the goal of a safe, secure, and prosperous Australia, the Indo-Pacific, and the world.[12] The strategy backs Australia as a regional cybersecurity leader, with a significant increase in investments, accepts the feedback from businesses and the community on the progress of Australia's cybersecurity (2016); and stimulated private sector investment in the domestic cybersecurity industry.

At the Quad level, Australia has promoted the 'Quad Tech Network' initiative to promote Track-2 research and public dialogue on cyber and critical technology issues relevant to the Indo-Pacific region.

The Australian government announced an AUD 1.35 billion 'Cyber Enhanced Situational Awareness and Response' (CESAR) package in June 2020, which sought to invest AUD 62.3 million towards national situational awareness capability.[13] These efforts highlighted the growing significance of the cyber domain in Australia's national governance objectives as well as its regional and international standing.

The Industrial Advisory Panel Report on Australia's 2020 Cyber Security Strategy had recommended that the government should establish clear consequences for those targeting Australia and Australians, strengthen end-to-end resilience, and work with industry in shaping international cyber security standards.[14] The report highlighted stakeholder support for increased use of threat blocking technology like Telstra's 'Cleaner Pipes initiative', following the UK's 'Active Cyber Defence' programme as a best practice model, which seeks to 'protect the majority of people in the UK from the harm caused by the majority of the cyberattacks in the majority of the time'.[15]

In addition, Australia has been active in promoting people-to-people exchanges as well. For example, at the Quad level, Australia has promoted the 'Quad Tech Network' initiative to promote Track-2 research and public dialogue on cyber and critical technology issues relevant to the Indo-Pacific region.[16]

Japan

As a leading tech innovator, Japan has a big stake in ensuring the absence of conflict in cyberspace. However, Japan has faced increasing cyberattacks on its industries which has threatened its cyber-dependent economy. It released its updated Cyber Security Strategy in September 2021, which identified an urgent need for reinforcing cybersecurity measures at all levels of Japanese society and in all aspects of technological development.[17] However, unlike the US' defend forward and persistent engagement strategies, Japan remains legally restricted from enhancing its capabilities in cyberspace. As Article 9 of the Japanese constitution provides for the renunciation of war, Japan can only use tangible force in response to a cyberattack and cannot exert its influence beyond its territory.[18] As cyberspace is transnational and borderless, this presents a dilemma for Tokyo and stifles its cyber prowess, which has resulted in an overly defensive Japanese approach in the cyber domain.

Japan remains legally restricted from enhancing its capabilities in cyberspace. As Article 9 of the Japanese constitution provides for the renunciation of war, Japan can only use tangible force in response to a cyberattack and cannot exert its influence beyond its territory.

In recent years, Japan has also observed strained relations with neighbours (Russia, China, South Korea, and North Korea) over various issues. As increasing Chinese militarisation and assertive policies in the Indo-Pacific loom large in Japanese strategic considerations, Tokyo seeks partnerships in the region. This makes closer cooperation in the Quad framework a necessity for Japan. This is visible beyond Quad as well as reflected in the statement of former Japanese premier Shinzo Abe in November 2021, that "Japan should cooperate with AUKUS (Australia-UK-US) partners on AI and cyber capabilities."[19] The trilateral partnership of AUKUS envisions gaining advanced cyber capabilities and countering adversaries in the information domain among key objectives for western interests, which looks favourable to join for Japan.

India

It has been argued that while India had previously been hesitant to join US-sponsored infrastructure initiatives with Australia and Japan, India's stance has undergone an adjustment in recent years.[20] As India-China tensions gained new peaks over Chinese incursions and infrastructure construction in Indian territory; troop-build at the border; persistent cyberattacks and cyber espionage campaigns[21] on India's critical infrastructure and cyberspace, Quad framework cooperation became important for Indian strategic outlook.

India signed its first detailed agreement for cooperation with the US in 2016, which has been followed by similar agreements with Australia and Japan in 2020. India's partnership with Australia and Japan is essential for capacity building in cyber-enabled critical technologies among other key areas. India has signed a Cyber and Critical Technology Partnership with Australia and a cybersecurity agreement with Japan which promotes cooperation in key areas like 5G and AI.[22] The partnership with the US has gained greater significance as India accelerates to develop its semiconductor ecosystem. This highlights that India's stance on cybersecurity policy and strategic considerations will invariably be influenced by its Quad partners.

Way Ahead

For the four Quad partners, the cyber domain serves as one of the most significant arenas for cooperation. It is an open secret that for western partners, Quad is an essential mechanism for countering China in the Indo-Pacific, with India expected to be a significant element of this concept. For India (similar to Japan, Australia, and the US), threats emerging from an increasingly authoritarian and assertive China remain a concern, especially when considering that India is the only Quad member sharing a physical border with China. As the western partners emphasize cyberspace governed by 'principles and norms', 'democracy', and respect for universal human rights, Quad serves as an avenue to pull India closer. New Delhi has for long made efforts to balance the two sides (the eastern bloc led by China and Russia, and the western bloc led by the US and the EU) in the cyber domain. However, national interests would compel India to attain technological competencies at an accelerated rate, essential for domestic economic growth and safety. Considering how the Russia-Ukraine war has pushed Russia closer to China[23] and isolated it from any access to European and American technological innovation industries[24], India might have to choose between upping its competency in cyberspace by choosing closer collaboration with partners from the West or trying to maintain the hedging strategy and depending on indigenous capacity building. Meanwhile, the West will look to entice India with the benefits of closer cooperation.

India accelerates to develop its semiconductor ecosystem. This highlights that India's stance on cybersecurity policy and strategic considerations will invariably be influenced by its Quad partners.

It has been suggested that the three Quad partners signatory to the Convention on Cybercrime should 'prod' India to join them as the first step toward harmonization of national laws and collective agreements on cyber issues.[25] Further, Quad's initiatives aimed at creating a 'human capital network' to foster cross-border collaboration, and joint exercises to increase cyber resilience would be prospects hard to ignore in India's decision-making circles.[26]

To counter China, Quad also seeks to provide the Indo-Pacific region with alternative ways for technological capacity building and reset the international standards and order for technology. Efforts toward this end are already visible with the Biden administration focusing to secure semiconductor supply chain networks[27] and successes in drawing away partners from Chinese companies like Huawei (including India which has formally rejected Chinese firms from conducting 5G trials)[28].

As cyber resilience is now an important aspect of national cyber strategies in the US and Australia (and Japan having pursued cyber defence as the primary policy), India's cyber strategy too might adopt some of the strategies of its Quad partners. This will make Quad a significant partnership to promote policies and concepts in the cyber domain, with four major cyber-capable and cyber-dependent economies working from a shared threat perspective. Unlike in conventional domains, collaboration in cyber can present more realizable

National interests would compel India to attain technological competencies at an accelerated rate, essential for domestic economic growth and safety.

avenues for success in the short term. The successes from cyber cooperation can then percolate into other spheres.

Notes:

[1] The White House, “Quad Joint Leaders’ Statement”, https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/24/quad-joint-leaders-statement. Accessed on May 26, 2022.

[2] Ibid.

[3] Ministry of External Affairs Government of India, "First Quad Leaders’ Virtual Summit", https://mea.gov.in/press-releases.htm?dtl/33601/First+Quad+Leaders+Virtual+Summit. Accessed on May 10, 2022.

[4] The White House, “Quad Principles on Technology Design, Development, Governance, and Use", https://www.whitehouse.gov/briefing-room/statements-releases/2021/09/24/quad-principles-on-technology-design-development-governance-and-use/. Accessed on May 15, 2022.

[5] The White House, “Fact Sheet: Quad Leaders’ Summit", https://www.whitehouse.gov/briefing-room/statements-releases/2021/09/24/fact-sheet-quad-leaders-summit. Accessed on May 15, 2022.

[6] United States Department of State, “Joint Statement on Quad Cooperation in the Indo-Pacific", https://www.state.gov/joint-statement-on-quad-cooperation-in-the-indo-pacific/. Accessed on May 17, 2022.

[7] The White House, “Statement by National Security Council Spokesperson Emily Horne on Quad Senior Cyber Group Meeting", https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/statement-by-national-security-council-spokesperson-emily-horne-on-quad-senior-cyber-group-meeting. Accessed on May 17, 2022

[8] Cyberspace Solarium Commission, “Cyberspace Solarium Commission Report”, https://www.solarium.gov/report. Accessed on May 5, 2022.

[9] Ibid.

[10] United States Congressional Research Service, *Cybersecurity: Deterrence Policy*, by Chris Jaikaran, R47011, (Washington D.C.: US Congressional Research Service).

[11] Ibid.

[12] Australian Government Department of Home Affairs, “*Cyber Security Strategy*”, https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy. Accessed on May 12, 2022.

[13] Ibid.

[14] Australian Government Department of Home Affairs, “*Cyber Security Strategy Industry Advisory Panel”*, https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/industry-advisory-panel. Accessed on May 14, 2022.

[15] U.K. Cabinet Office ,“Government Cyber Security Strategy: 2022 to 2030”, https://www.gov.uk/government/publications/government-cyber-security-strategy-2022-to-2030. Accessed on May 11, 2022.

[16] The Australian National University, “Quad Tech Network”, https://nsc.crawford.anu.edu.au/department-news/18328/quad-tech-network. Accessed on May 22, 2022.

[17] International Trade Administration "Japan-Country Commercial Guide", https://www.trade.gov/country-commercial-guides/japan-cybersecurity. Accessed on May 08, 2022.

[18] Kohei Takahashi et al., "Building Cooperation: Cyber, Critical Technology and National Security" (Canberra: National Security College The Australian National University, 2021), p. 9.

[19] Kiyoshi Takenaka, "Ex-Japan PM Abe Calls for Tokyo's Cooperation with AUKUS in AI, Cyber," *Reuters,* November 19, 2021, https://www.reuters.com/world/asia-pacific/ex-japan-pm-abe-calls-tokyos-cooperation-with-aukus-ai-cyber-2021-11-19. Accessed on May 15, 2022.

[20] Zheng Haiqi and Claudia Chia, The New Era of the Quad: Opportunities for India-US Cooperation, (Singapore: National University of Singapore, 2021), p. 4.

[21] Sameer Patil and Kishika Mahajan, Expanding Chinese Cyber-Espionage Threat against India, Observer Research Foundation, April 18, 2022, https://www.orfonline.org/expert-speak/expanding-chinese-cyber-espionage-threat-against-india. Accessed on May 15, 2022.

[22] Australian Government Department of Home Affairs, n. 16.

[23] "Ukraine Crisis Pushes Russia and China into a Closer Embrace" *Financial Times*, February 13, 2022, https://www.ft.com/content/38984025-9f1b-492f-933d-57da44fcc16. Accessed on May 15, 2022.

[24] The German Council on Foreign Relations, "Russia's Technological Isolation", https://dgap.org/en/research/publications/russias-technological-isolation. Accessed on May 15, 2022.

[25] Martijn Rasser, Networked: Techno- Democratic Statecraft for Australia and the QUAD (Canberra: Australian National University, 2021), p. 12.

[26] Ibid.

[27] "President Biden Appeals for Big Cash Infusion to US Semiconductor Industry", *Business Standard*, March 2, 2022, https://www.business-standard.com/article/international/president-biden-appeals-for-big-cash-infusion-to-us-semiconductor-industry-122030201030_1.html. Accessed on May 8, 2022.

[28] "Huawei and ZTE Left out of India's 5G Trials" BBC News, May 5, 2021, https://www.bbc.com/news/business-56990236. Accessed on May 18, 2022.

Centre for Air Power Studies

The Centre for Air Power Studies (CAPS) is an independent, non-profit think tank that undertakes and promotes policy related research, study and discussion on defence and military issues, trends, and development in air power and space for civil and military purposes, as also related issues of national security. The Centre is headed by Air Marshal Anil Chopra PVSM AVSM VM VSM (Retd).

Centre for Air Power Studies
P-284, Arjan Path, Subroto Park, New Delhi 110010
Tel: +91 11 25699130/32, Fax: +91 11 25682533

Editor: Dr Shalini Chawla e-mail: shaluchawla@yahoo.com
Formatting and Assistance: Mr Mohit Sharma, Ms Mahima Duggal and Mr Rohit Singh

The views expressed in this brief are those of the author and not necessarily of the Centre or any other organisation.