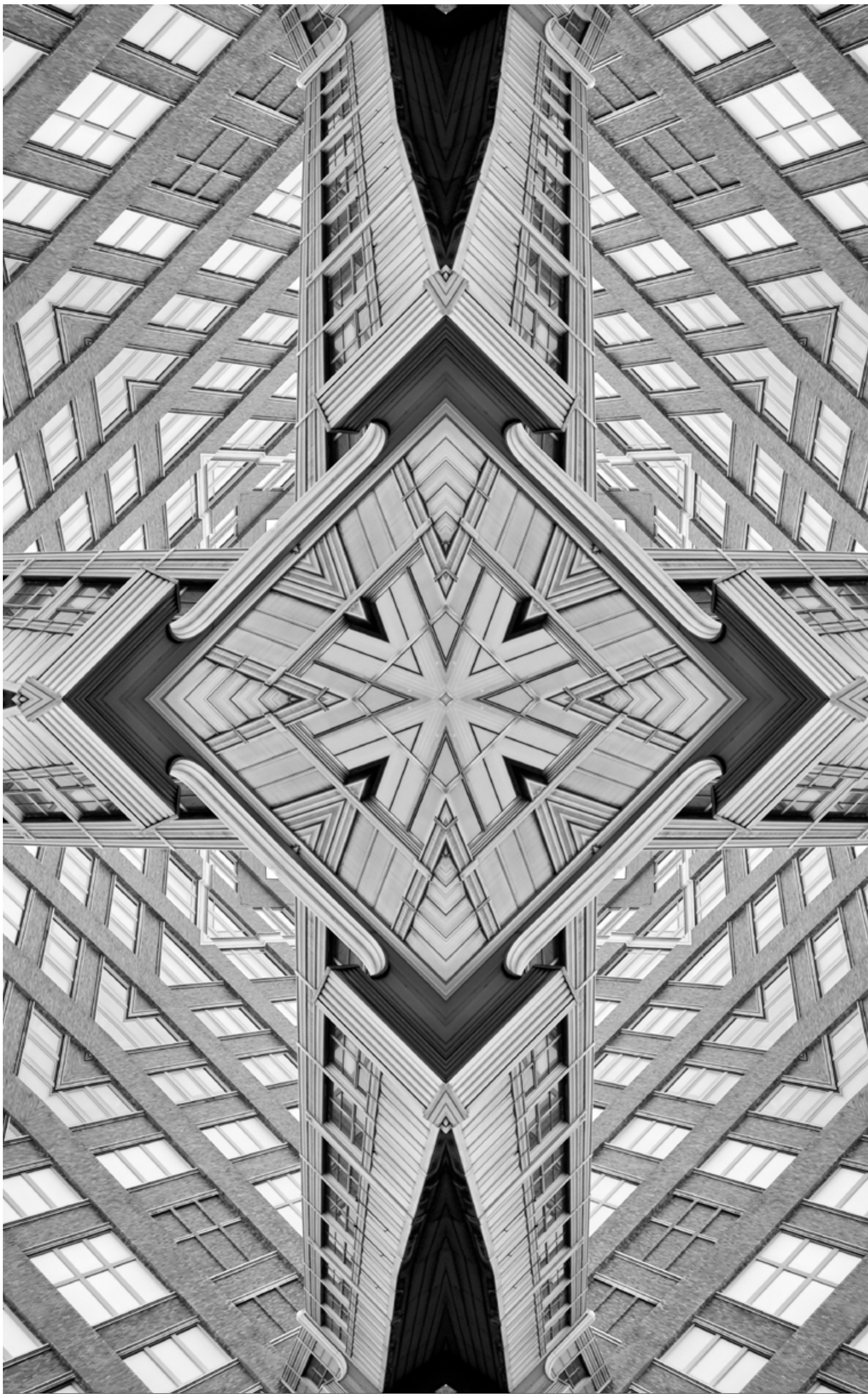
OBSERVER RESEARCH FOUNDATION

Issue Brief

ISSUE NO. 592
NOVEMBER 2022



Quad Vadis? A Risk Assessment of the Quad's Emerging Cybersecurity Partnership

Tobias Scholz

Abstract

The Quad's growing effort to shape international norms and rules in the Indo-Pacific is taking place in an environment fraught with multiple challenges. China's assertive rise as well as internal differences within the group pose significant risks to the plurilateral platform's mission of creating a free, open, and secure Indo-Pacific. Focusing on the Quad's cybersecurity cooperation, this brief examines the various internal and external risks that Quad countries are currently facing in their evolving partnership.

Attribution: Tobias Scholz, "*Quad Vadis?* A Risk Assessment of the Quad's Emerging Cybersecurity Partnership," *ORF Issue Brief No. 592*, November 2022, Observer Research Foundation.

Introduction

Various countries in the Indo-Pacific region are witnessing an increase in the number and intensity of their cybersecurity threats. Emerging challenges include threats to national security and international supply-chain vulnerabilities as well as the weaponisation of cyberspace by state and non-state actors. Responding to these challenges, the Quadrilateral Security Dialogue (or Quad, comprising India, Australia, Japan, and the US) is emerging as a key leader in shaping security norms and alignments. As one of several new plurilateral formats in the region, the Quad was initiated to meet growing international challenges in the Indo-Pacific, particularly those pertaining to China's rise as a great power.[1]

Choosing plurilateral cooperation as a means to achieve national cybersecurity interests bears as many promises as potential pitfalls. The fundamental reasons why plurilateral platforms can prove effective include their flexibility in shaping norms and standards, a relative simplicity of knowledge exchange, the presence of trust-building opportunities, and their possible deterrence effects. On the downside, however, earlier plurilateral platforms have rarely succeeded in shaping international politics in a significant way. From IBSA[2] to the Shanghai Cooperation Organisation (SCO), plurilateral cybersecurity efforts have had little geopolitical impact, if at all. Such previous experiences raise pertinent questions on the resilience of the Quad cybersecurity cooperation and possible challenges the platform is likely to encounter in the next years.

This brief analyses the geopolitical and geoeconomic risks in the Quad's cybersecurity cooperation. It begins with an overview of the dynamic cybersecurity threat landscape for Quad partners, followed by a brief history of Quad cybersecurity cooperation emphasising political decisions and underlying motivations. Building on the experience of other plurilateral platforms, a conceptual section then presents four ideal type risks for plurilateral diplomatic engagement. The brief then discusses four challenges to the Quad's future cybersecurity cooperation, and argues that addressing them requires the Quad to utilise risk prevention and risk management capabilities.

The Indo-Pacific: An Ocean of Cyber Challenges

Varying norms and national interests have resulted in different understandings of what constitutes the Indo-Pacific region. Despite these differences, nations that have subscribed to the concept share an understanding of the Indo-Pacific as a geopolitical and geoeconomic space. Among the first nations to officially recognise the Indo-Pacific concept were the four Quad countries.[3] While each of them was affected by different cyber challenges during the 2010s, all four identified China's heightened belligerence in cyberspace as a significant cybersecurity threat.

Until 2015, the United States strategy to deal with China's rising cyber capabilities and willingness to use them for coercive purposes was geared towards offering China an active role in a rules-based order. This idea was most significantly incorporated in the US-China Cyber Agreement between Barack Obama and Xi Jinping.[4] Months after the US had revealed that Advanced Persistent Threat Actor 30 (APT 30) had spied on Indian state secrets for 10 years, then President Obama still hoped to contain Chinese ambitions in global espionage.[5]

However, national cybersecurity challenges between China and all four Quad countries mounted in the following years. Chinese cyber espionage and cyber-attacks on key industrial enterprises and government agencies in Japan reinforced the political and economic distrust between the two nations.[6] In 2016, revelations that the Chinese threat actor Bronze Butler had attempted and successfully intruded Japanese companies for at least ten years, added to Japan's threat perception.

Australia's cybersecurity concerns in its 2017 Foreign Policy White Paper reached far beyond issues of industrial and political espionage by calling for protecting critical infrastructures, and fighting misinformation and media manipulation.[7] After the White Paper made a case for building a stronger cyber defence, then Prime Minister Scott Morrison in 2020 warned the Australian people of a possible state-sponsored cyber-attack targeting the country's national institutions.[8] India's alertness towards Chinese cybersecurity threats increased significantly after the border clashes in the Galwan Valley that began in May 2020. In the months after the initial skirmishes, India started experiencing power cuts. In Mumbai, where the biggest of such attacks took place in October 2020, local authorities identified the power outage as a result of malicious software.[9] Meanwhile, the US, of all Quad countries is the only one with a public attribution system. Since its launch in 2017, the Cybersecurity & Infrastructure

The Indo-Pacific: An Ocean of Cyber Challenges

Security Agency (CISA) has declared Chinese threat actors as being responsible for various cyber-attacks on US territory, including espionage, attacks on critical infrastructure, and influence operations.[10]

China's rising assertiveness in cyberspace is the one central element that united Quad nations before the group came together for closer cooperation in 2020. The following section introduces the progress that Quad cybersecurity cooperation has made over the past two years.

> "All four Quad countries were affected by different cyber challenges in the 2010s; today all of them view China's heightened belligerence in cyberspace as a significant threat."

The Emergence of the Quad as a Cybersecurity Actor

Cybersecurity cooperation has been a built-in feature of the Quad since the first informal gathering of foreign ministers at the sidelines of the United Nations General Assembly in September 2019. Only months after a serious cyber-attack on the Australian Parliament, which was believed to have originated in China,[11] cybersecurity cooperation was jointly seen as a political priority. The evolution of Quad cybersecurity cooperation has since been stimulated by three high-level meetings.[12]

During the first Quad Leaders' summit that took place virtually in March 2021, heads of government agreed on stronger cooperation on new technologies within the emerging strategic principle of a "Free and Open Indo-Pacific".[13] Further normative calls advocated for a secure, prosperous, inclusive, rules-based, international law-abiding, democratic, and healthy Indo-Pacific.[14] The meeting's key cybersecurity achievement was establishing a Quad Critical and Emerging Technologies Working Group. The group was formed to pave the way for planning a joint Quad approach as it was meant to develop a set of shared norms and standards as well as to identify shared priorities in telecommunications, supply chains, and public-private partnerships.[15]

Six months after the initial summit in March 2021, Quad leaders met again and reviewed the recommendations of the established working group.[16] They also designed the Quad Senior Cyber Group to coordinate cybersecurity matters within the Quad. The group now forms the core of the new Quad Cybersecurity Partnership and has two central functions. First, it provides a space in which it consults with different public and private stakeholders on matters like cyber standards, supply chains, and critical infrastructure resilience. Second, it is meant to utilise knowledge exchange mechanisms to drive the future cybersecurity agenda of the Quad.[17]

While the Quad Senior Cyber Group is coordinated by senior officials within the four governments, the Quad summit further resulted in the launch of several multistakeholder projects to foster cooperation on specific technologies. Most significantly, leaders agreed on a Track 1.5 dialogue on 5G standards and Open RAN technology to enhance security, interoperability, and openness in the telecommunications sector. The Quad nations also created a Semiconductor Supply Chain Initiative and two Technical Standards Contact Groups on Advanced Communications and Artificial Intelligence (AI), respectively. Finally, Quad leaders identified policy coordination in multilateral organisations such as the International Telecommunications Union (ITU) as important areas.

Including the ITU in their joint statement stands out, as this organisation was dominated by China in previous years and has recently played only a marginal role in US foreign policy.

The Quad Senior Cyber Group met for the first time in March 2022 and was led by member states' senior officials in-charge of coordinating national cyber security. The US statement following the meeting reflected a focus on protecting critical infrastructures and indicated an interest in extending cooperation in the Indo-Pacific region.[18] Subsequently, the recommendations were provided as input to the most recent Quad Leaders' Meeting in May 2022.

In the meeting, Quad leaders announced their intent on "improving the defense of our nations' critical infrastructure by sharing 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."[19] The declaration marks the final step of the Quad to establish direct lines of communication and cooperation between the relevant national nodal agencies dealing with cybersecurity.

Cooperating directly through CERTs and ministries instead of setting up joint facilities or secretariats illustrates the Quad's continuing self-perception as a platform. The Quad nations addressed the issue of increased areas of cooperation without introducing institutional mechanisms by defining leadership roles for each country. The meeting assigned Australia the responsibility for critical-infrastructure protection, India is tasked to coordinate supply-chain resilience and security, Japan's key focus is on workforce development, and the US will lead efforts on software security standards.[20]

The Quad leaders not only increased horizontal cooperation, but also introduced vertical partnerships. The meeting confirmed that the Quad will extend people-to-people connectivity through a Quad Cybersecurity Day and capacity building programs which shall be open to partners in the Indo-Pacific region.

Finally, the Quad is increasingly showing a willingness to deepen its cooperation towards specific cybersecurity challenges. At the sidelines of UNGA 2022, Quad foreign ministers announced that the platform will now more closely coordinate its efforts in fighting ransomware.[21] While concrete measures remained missing in the statement, senior officials of Quad members now have a strong mandate that could potentially evolve into institutional mechanisms.

Risks of Plurilateral Diplomacy

Plurilateral platforms such as the Quad consist of "at least three but a limited number of sovereign nation states that jointly coordinate political or economic demands toward the international system or parts of it while maintaining a minimum degree of institutionalisation and delegation."[22] This section discusses past challenges faced by other plurilateral platforms to identify potential categories of political risk that they are susceptible to.

A central problem for plurilateral platforms is *internal credibility*. The SCO offers a suitable example for this instance. Led by China and Russia, the platform made quick advances on cybersecurity cooperation in the early 2010s. Russia proactively pushed for mechanisms and norms of international information security which elevated the SCO to a serious institution in this field.[23] However, with India's and Pakistan's accession to the SCO, the organisation was not able to maintain this momentum. Instead of further shaping the international cybersecurity debate, the SCO's international security aspirations proved to be without credibility for an environment in which key geopolitical competitors China, India, and Pakistan were involved in the decision-making process. Distrust and hedging tactics among member states have locked in the SCO as a credible actor for cybersecurity cooperation.

Plurilateral platforms also fail to reach their goals when they lack *external credibility*. Dissatisfied with a US-dominated Internet, the IBSA nations India, Brazil, and South Africa pitched an alternative. The platform was initially well positioned to balance the US through South-South cooperation as it was formed by three key rising powers in Africa, Asia, and South America. IBSA realised that a Committee for Internet-Related Policy (CIRP) could position the platform as a leader of the Global South by calling for "improving the quality of peoples' lives everywhere."[24] However, IBSA nations underestimated the effort needed to convince other countries of CIRP. After CIRP failed to find the necessary support in the UN, the proposal had to be withdrawn. Excluding other nations from developing an alternative model to Internet governance and supposing international support of the Global South without including many of its nations had a negative effect on IBSA's credibility.

BRICS, for its part, provides evidence of how *internal conflict* among members in one policy area can limit the overall productivity of the platform. The group that includes Brazil, Russia, India, China, and later South Africa came together mostly to challenge international financial and trade institutions. In its first years, the group had a modicum of success even though some of its members had fundamental bilateral issues with another. After the Sino-Indian border crisis at Doklam in 2017, however, BRICS countries found it increasingly difficult to agree on shared points of view. Animosities had outgrown the will to seriously cooperate on global challenges and significantly impaired the ability of BRICS to formulate policy solutions in global governance.

Finally, plurilaterals can lose or change their function as a result of *external shocks*. One example that stands out is the Group of Eight (G8), a platform that had been designed by Western powers to find solutions to global challenges. In the early 2000s, the G8 remained a space for informal exchange on international issues such as trade, energy, and terrorism. Yet, when the global financial crisis erupted in 2007, neither the G8 nor other countries believed that the platform would be suitable to address the situation. A more inclusive G20 platform was formed and the G8 lost its status as a platform for international financial and trade issues.

> “The key challenges for plurilateral forums are internal credibility, external credibility, internal conflict, and external shocks.”

The Quad's Four Biggest Cyber Risks

Initiating the Quad gave member countries a sense of optimism about maximising their national cybersecurity through cooperation. However, there are good reasons for Quad countries to proceed with caution and foresight. Applying the previously introduced ideal types of risks for plurilateral platforms, Quad countries must be aware of the following potential risk scenarios.

Risk 1: Internal credibility. Multi-alignment strategies of Quad countries may decrease credibility.

The United States is by far the most powerful cybersecurity actor among the Quad countries. Besides its membership in the Quad, the United States is also part of AUKUS[25] and the Five Eyes intelligence alliance, while maintaining strong bilateral security partnerships with countries like Australia and the Philippines. As the United States is opting for a multi-alignment strategy, India might also deprioritise further Quad integration and instead seek to diversify its regional cybersecurity partnerships outside of Quad. If regional cybersecurity cooperation continues to fragment, the Quad can become susceptible to losing its status as a security coalition in the Indo-Pacific.

As the Quad is the only security platform that has the potential to be a regional leader in setting cybersecurity norms and standards, a solution could be to transform it into a cybersecurity alliance. While a security alliance in conventional domains appears unrealistic for various reasons, the promise of mutual assistance in defending against international cyber-attacks can significantly increase internal and external credibility. In the beginning, this can include a rapid response mechanism through which Quad nations immediately support an attacked member through satellite Internet access, when Internet availability is affected through the attack.

Risk 2: External credibility. Regional distrust of Quad's geopolitical intentions can lead to a legitimacy deficit.

Many countries in the region regard the Indo-Pacific concept as a diplomatic instrument designed to isolate China. For some, such a call for division might even stand in paradigmatic opposition to the powerful narrative of the "Asian century".[26] If Quad countries are aiming to succeed in convincing regional players of their version of a free, open, and secure Indo-Pacific, they must make an offer to countries in the region. In other words, Quad countries have to prove to their regional partners that they are not securitising the Indo-Pacific for their own good, but instead offer cybersecurity solutions for all of them.

The Quad can increase its regional recognition by establishing Track 1.5 and Track 2 networks with other regional forums, most significantly ASEAN.[27] There is a growing recognition within ASEAN, that cybersecurity capacity building is a quality that must be encouraged beyond national borders. An ASEAN-Quad cybersecurity capacity building programme could be a starting point for regional outreach. Establishing a cybersecurity warning mechanism among ASEAN and Quad CERTs could be central for trust and confidence building.

Risk 3: Internal conflict. Disagreements over the role of Big Tech may affect trust.

All four Quad countries are currently dissatisfied with how its partners wish Big Tech companies to be regulated. India has in recent years shown great aversion to US-based social media companies' norms on online freedom of speech and even more significantly on the access of local data and standards for international routing.[28] In one incident, the Twitter country office in New Delhi was even raided as part of a police investigation. In another incident in 2020, Australia clashed so massively with Facebook, that the company threatened to pull out of Australia. Two observers of the 2021 Quad summit pointedly summarised, "While the unity on display at the Quad summit was an impressive show of strength, it was also an incomplete picture that masked growing friction among members on several elemental technology issues such as cross-border data flows, data privacy, payments, digital taxation, competition, e-commerce, and law enforcement."[29] If such disagreements remain unsolved, they may cause hardly reconcilable trust deficits among the member states.

Diverging opinions on the role of US-based technology companies in other Quad markets are essentially a matter of trade as well as technology norms and practices. To deal with such issues, the European Union (EU) has already set up a bilateral Trade and Technology Council with the United States and India, respectively. The Track 2 Quad Tech Network offers an existing space that can be elevated to a more formal forum on technology and trade issues.[30]

The Quad's Four Biggest Cyber Risks

Risk 4: External shock. A more assertive China could probe the effectiveness and belie expectations.

As the institutional mechanisms of the Quad are still evolving and have yet to be tested, a major cyber-attack originating in China could catch the partners by surprise and evoke internal tensions. Such a scenario is, e.g., imaginable when an attacked Quad country wants other Quad nations to attribute a cyber-attack, but in response its partners prefer to first gain additional cyber-forensic confirmation. If a delayed attribution confers a heavy security, economic, or status cost on the impacted country, this Quad member might lose trust in its partners and their platform.

In their further integration, Quad members must remain cautious and serious over the aspirations that their decisions set free. For example, a joint attribution system of cyber-attacks could work properly only if the rules of attribution are clear. Instead of relying too heavily on cyber defence cooperation, the Quad could first turn to capacity-building solutions that increase the resilience of its members.

> “As the Quad is the only security platform that can be a regional leader in setting cybersecurity norms and standards, it could be transformed into a cybersecurity alliance.”

Outlook

Addressing each of these risks requires political will, timing, and a shared awareness of how to deal with challenges and potential setbacks. The Quad must act decisively and self-reflectively if it is to maximise the benefits of a unified and sustainable security partnership.

What distinguishes the Quad from other plurilateral platforms such as BRICS and IBSA is its unified belief in China as a geopolitical threat. As this shared belief is not likely to completely disappear within the next 50 years, the Quad countries have a realistic opportunity to shape many of the norms, standards, and institutional mechanisms as well as strategic imperatives for the digital Indo-Pacific in the decades to come. To succeed, the Quad must remain aware of its internal diversity and external pressures. If it wants to be a regional leader on cybersecurity efforts, the Quad Cybersecurity Partnership must make a credible offer for peace, prosperity, and stability in the entire Indo-Pacific region.

This brief is an expanded version of an essay published in ORF's Digital Debates 2022. *The author thanks Sameer Patil and Sarah Bressan for their comments on earlier versions of this article. All shortcomings are solely those of the author.*

Tobias Scholz *is a PhD Candidate at King's College London and National University of Singapore.*

Endnotes

1 A plurilateral platform is a "political instrument by at least three but a limited number of sovereign nation states that jointly coordinate political or economic demands toward the international system or parts of it while maintaining a minimum degree of institutionalization and delegation"; Harsh V. Pant and Tobias Scholz, "BRICS: Expiring Political Relevance and Inspiring New Coalitions," in *Handbook on Global Governance and Regionalism*, ed. Jürgen Rüland and Astrid Carrapatoso (Cheltenham, UK & Northhampton, MA, USA: Edward Elgar Publishing, 2022), 149–60, forthcoming.

2 IBSA is a plurilateral platform consisting of India, Brazil, and South Africa.

3 Australian Government, *2017 Foreign Policy White Paper: Opportunity, Security, Strength* (Canberra: Department of Foreign Affairs and Trade, 2017), https://www.dfat.gov.au/sites/default/files/2017-foreign-policy-white-paper.pdf

4 Mark Bryan F. Manantan, "Advancing Cyber Diplomacy in the Asia Pacific: Japan and Australia," *Australian Journal of International Affairs 75*, no. 4 (2021): 432–59, https://www.tandfonline.com/doi/full/10.1080/10357718.2021.1926423

5 *Council on Foreign Relations*, "APT 30," https://www.cfr.org/cyber-operations/apt-30

6 Stefan Soesanto, "A One-Sided Affair: Japan and the People's Republic of China in Cyberspace (Hotspot Analysis)," ETH Zürich, 2020, https://www.research-collection.ethz.ch/bitstream/handle/20.500.11850/389371/Cyber-Reports-2020-01-A-one-sided-Affair.pdf

7 Australian Government, *2017 Foreign Policy White Paper: Opportunity, Security, Strength*.

8 "Australia Cyber Attacks: PM Morrison Warns of 'sophisticated' State Hack", *BBC News*, June 19, 2020, https://www.bbc.com/news/world-australia-46096768

9 Ritvick AB, "Maha Min Speaks in Assembly, Says Mumbai Blackout Was Cyber Attack," *TheQuint*, March 4, 2021, https://www.thequint.com/news/india/maharashtra-minister-nitin-raut-speaks-in-assembly-says-mumbai-blackout-was-cyber-attack

10 CISA, *China Cyber Threat Overview and Advisories* (Washington, D.C.: CISA, 2022), https://www.cisa.gov/uscert/china

11 Peter Hartcher, "Farewell Tech Utopia: How Governments Are Readying the Web for War", *The Sydney Morning Herald*, February 18, 2019, https://www.smh.com.au/national/farewell-tech-utopia-how-governments-are-readying-the-web-for-war-20190218-p50yhh.html

12 For the purpose of this article, the following paragraphs do only point to the Quad cybersecurity partnership and do not include cooperation in other areas relating to emerging technologies.

13 The White House, *Quad Leaders' Joint Statement: 'The Spirit of the Quad'* (Washington, D.C.: The White House, 12 March 2021), https://www.whitehouse.

gov/briefing-room/statements-releases/2021/03/12/quad-leaders-joint-statement-the-spirit-of-the-quad/

14 Joe Biden, Narendra Modi, Scott Morrison, and Yoshihide Suga, "Our four nations are committed to a free, open, secure and prosperous Indo-Pacific region", *The Washington Post*, March 13, 2022, https://www.washingtonpost.com/opinions/2021/03/13/biden-modi-morrison-suga-quad-nations-indo-pacific/.

15 The White House, *Fact Sheet: Quad Summit* (Washington, D.C.: The White House, 12 March 2021), https://www.whitehouse.gov/briefing-room/statements-releases/2021/03/12/fact-sheet-quad-summit/

16 Rajeswari Rajagopalan, "The Growing Tech Focus of the Quad", *The Diplomat*, July 9, 2022, https://thediplomat.com/2022/07/the-growing-tech-focus-of-the-quad/

17 The White House, *Fact Sheet: The Quad Summit.*

18 The White House, *Statement by National Security Council Spokesperson Emily Horne on Quad Senior Cyber Group Meeting* (Washington, D.C.: The White House, 25 March 2022), 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/

19 The White House, *Quad Joint Leaders' Statement* (Washington, D.C.: The White House, 24 May 2022), https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/24/quad-joint-leaders-statement/

20 The White House, *FACT SHEET: Quad Leaders' Tokyo Summit 2022* (Washington, D.C.: The White House, 24 May 2022), https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/23/fact-sheet-quad-leaders-tokyo-summit-2022/

21 Ministry of External Affairs, Government of India, *Quad Foreign Ministers' Statement on Ransomware* (New Delhi: Government of India, 23 September 2022), https://www.mea.gov.in/bilateral-documents.htm?dtl/35749/Quad+Foreign+Ministers+Statement+on+Ransomware

22 Pant and Scholz, "BRICS: Expiring Political Relevance and Inspiring New Coalitions".

23 Eneken Tikk and Mika Kerttunen, "Parabasis: Cyber-Diplomacy in Stalemate," *Norsk Utenrikspolitisk Institutt*, 2018, https://www.nupi.no/en/publications/cristin-pub/parabasis-cyber-diplomacy-in-stalemate

24 Dushyant Singh, "India's Proposal for a United Nations Committee for Internet-Related Policies (CIRP)" (speech, New York City, 2011), IT for Change, https://itforchange.net/indias-proposal-for-a-united-nations-committee-for-internet-related-policies-cirp

25 A security platform between Australia, the United Kingdom, and Australia.

Endnotes

[26] Among the authors that have contributed in popularising such narratives are Parag Khanna's *The Future Is Asian* (New York: Simon and Schuster, 2019) and Kishore Mahbubani's *Has China Won?: The Chinese Challenge to American Primacy* (United Kingdom: Hachette, 2020). Their approaches vocalise an aspirational future in Asia without geopolitical conflict. While Mahbubani builds his argument on a predicted Western decline and the need for South-South solidarity to reduce global inequalities, Khanna's work exclusively focuses on the economic growth trajectories in a connected and economically liberal Asia.

[27] Aakriti Bachhawat, Danielle Cave, Jocelinn Kang, Rajeswari Pillai Rajagopalan and Trisha Ray, *Critical Technologies and the Indo-Pacific : A New India-Australia Partnership*, ASPI & ORF (Policy Brief Report No. 39/2020), 2020, https://www.orfonline.org/research/critical-technologies-and-the-indo-pacific-policy/ have already suggested Quad Plus formats in the field of technology cooperation, an idea complementary to the ideas above.

[28] Sameer Patil, "Flexing Quad Strength on Fintech and Cybersecurity", *Financial Express*, December 10, 2021, https://www.financialexpress.com/opinion/flexing-quad-strength-on-fintech-and-cybersecurity/2348178/

[29] Mark Linscott and Anand Raghuraman, "How to Leverage the Quad to Counter China's Digital Sinosphere", *Atlantic Council*, May 17, 2021, https://www.atlanticcouncil.org/blogs/new-atlanticist/how-to-leverage-the-quad-to-counter-chinas-digital-sinosphere/

[30] See e.g., Trisha Ray et al., *The Digital Indo-Pacific: Regional Connectivity and Resilience* (QTN Series) (Acton: National Security College at the Australian National University, 2021): 39.

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