01/2023

#01

The Quad: Carved in Code

Collaborating to Deliver the Greatest Public Good

Ravi Nayyar

DIGITAL DIPLOMACY AND STATECRAFT WORKING PAPER

GIGA
German Institute for Global and Area Studies
Leibniz-Institut für Globale und Regionale Studien

DIGITAL DIPLOMACY AND STATECRAFT WORKING PAPER

Author

Ravi Nayyar is a PhD Scholar at the University of Sydney. His research concerns how critical software regulation fits into critical infrastructure regulation. He holds a BCom (Hons I) and LLB from the University of Sydney. He has worked in technology law and policy, including for the OECD. He has also written extensively on cyber law and policy.

Digital technologies are fundamentally transforming societies worldwide. The Global South is an important shaper of this change. “Digital Diplomacy and Statecraft” is a research project funded by the Federal Foreign Office. Under the lead of Prof. Amrita Narlikar, Prof. Jann Lay, and Prof. Christian von Soest, this initiative explores how digitalisation offers new opportunities, challenges, and instruments for foreign policy. Bringing together international experts and identifying prospects and threats of digitalization, the project analyses the drivers and consequences of digitalisation across the world regions. Through this research it aims to deliver useful impulses for German foreign policy and timely responses of (digital) diplomacy.

GIGA
German Institute for Global and Area Studies
Leibniz-Institut für Globale und Regionale Studien

The Quad: Carved in Code -
Collaborating to Deliver the Greatest Public Good

Abstract

This working paper explores the cooperation of the Quad governments (Japan, Australia, the United States and India) on tackling cyber-borne threats to (inter)national security. It will focus on their pledge to pursue certain minimum security standards for software procurement, arguing that this initiative is critical to the achievement of the Quad's agenda. It will first explain the context of the pledge, that is, cyber diplomacy by the Quad governments, before questioning the utility of this diplomacy as a means to meaningfully improve the cyber resilience of the regions at which it is targeted. The aforementioned pledge will be presented as the way forward for cyber diplomacy by the Quad countries because it targets a major source of the cyber resilience problem: software insecurity. The working paper will then critically analyse the policy merits of the pledge and find that it is necessary for uplifting software security, cyber resilience around the world and thus the fulfilment of the Quad's commitment to tackle security challenges emanating from the cyber domain. To build on this analysis, the pledge will be justified as a driver of the internal credibility of the Quad, making the four governments coalesce around implementing it and uplifting software security. This working paper will conclude by pointing to how the benefits of the pledge are easily transferable outside the Quad, helping position the grouping as a positive force for encouraging the cyber resilience of societies and economies.

Table of Contents

1. Introduction

The Quadrilateral Security Dialogue — also known as 'the Quad', comprising Japan, Australia, the United States and India — is no stranger to dealing with major risks to (inter)national security. It was born as a vehicle for its members to coordinate their humanitarian and disaster relief response to the Boxing Day Tsunami of 2004.[1] Around seventeen years later, the Quad Leaders drew an implicit parallel between the Tsunami and 'security challenges facing the region'.[2] They pledged to 'advance security and prosperity and counter threats to both in the Indo-Pacific and beyond'.[3] They committed to 'address shared challenges, including in cyber space', a clear recognition of cyber risks as major risks to (inter)national security.[4] That too, one backed by 'longstanding cooperation' on cyber resilience by the four countries.[5]

Such cooperation is vital. The criticality of cyberspace to modern societies and economies stems from their growing 'digital dependency'.[6] Digital technologies are a source of sizeable risks to national security.[7] The growth of these 'sprawling arrays of daunting complexity' that underpin modern life has not been accompanied by proportionate growth in their cyber resilience, leaving

[1] H.V. Pant & S. Mattoo, eds., 'The Rise and Rise of the 'Quad': Setting an Agenda for India', *Observer Research Foundation* (New Delhi, 23 Sep. 2021), 2, https://www.orfonline.org/wp-content/uploads/2021/09/ORF_SpecialReport_161_Quad-India-Agenda.pdf, accessed 9 Mar. 2023; J.R. Biden et al., *Quad Leaders' Joint Statement: "The Spirit of the Quad"* [media release] (12 Mar. 2021), para. 1, https://www.whitehouse.gov/briefing-room/statements-releases/2021/03/12/quad-leaders-joint-statement-the-spirit-of-the-quad/, accessed 10 Mar. 2023.

[2] Biden et al., *The Spirit of the Quad*, para. 1.

[3] Ibid, para. 2.

[4] Ibid, para. 3.

[5] The White House, *Fact Sheet: Quad Leaders' Summit* [media release] (24 Sep. 2021), para. 21, https://www.whitehouse.gov/briefing-room/statements-releases/2021/09/24/fact-sheet-quad-leaders-summit/, accessed 10 Mar. 2023. This working paper will define cyber resilience as '[t]he 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': R. Ross et al., 'Developing Cyber-Resilient Systems: A Systems Security Engineering Approach', *National Institute of Standards and Technology* (United States of America, Dec. 2021), 60, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2r1.pdf, accessed 3 Mar. 2023.

[6] L. Bernat, 'Enhancing the Digital Security of Critical Activities', *OECD* (Paris, 31 Aug. 2021), 4-5, https://goingdigital.oecd.org/data/notes/No17_ToolkitNote_DigitalSecurity.pdf, accessed 13 Mar. 2023; OECD, 'OECD Policy Framework on Digital Security', *OECD* (Paris, 14 Dec. 2022), 5, https://read.oecd.org/10.1787/a69df866-en?format=pdf, accessed 11 Mar. 2023.

[7] UNGA Res 199 (LVIII) (30 January 2004), Preamble paras 2, 5-6; UNGA 'Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security' UN GAOR 76th sess Preliminary List Item 96, UN Doc A/76/135 (2021), 7.

societies' cyber resilience 'systemically inadequate'.[8] The global interconnectivity of computer networks means that the exploitation of vulnerabilities in digital technologies deployed in one country can easily affect others.[9] As the Indian External Affairs Minister put it, 'in many ways, the Westphalian model of international relations is over for us in this era of technological interpenetration'.[10]

The Quad Cybersecurity Partnership ('QCP') was created in this context at the May 2022 Quad Leaders' Summit.[11] The QCP has four pillars: critical infrastructure protection, supply chain resilience, workforce development and software security standards.[12] In May 2022, the four governments pledged under the QCP to coordinate their procurement standards with respect to software security and thus use their 'collective purchasing power to improve the broader software development ecosystem so that all users can benefit'.[13] In May 2023, the governments specifically pledged under the QCP to incorporate certain 'high-level secure software development practices' in their government policy and procurement regulations, in addition to specifically including

[8] Office of the National Cyber Director (United States), 'A Strategic Intent Statement for the Office of the National Cyber Director', *The White House* (Washington, DC, 28 Oct. 2021), 6, https://www.whitehouse.gov/wp-content/uploads/2021/10/ONCD-Strategic-Intent.pdf, accessed 12 Mar. 2023; A. Attrey et al., 'Digital Enablers of the Global Economy: Background Paper for the CDEP Ministerial Meeting', *OECD* (Paris, 15 Nov. 2022), 13, https://read.oecd.org/10.1787/f0a7baaf-en?format=pdf, accessed 13 Mar. 2023.

[9] U.S. Government Publishing Office, 'Bolstering the Government's Cybersecurity: Lessons Learned from WannaCry', *U.S. Government Publishing Office* (Washington, DC, 15 Jun. 2017), 33-44, https://www.govinfo.gov/content/pkg/CHRG-115hhrg26234/pdf/CHRG-115hhrg26234.pdf, accessed 9 Mar. 2023; J. Ferris, *Behind the Enigma: The Authorised History of GCHQ, Britain's Secret Cyber Intelligence Agency* (Great Britain: Bloomsbury Publishing, 2020), 689-90; C. Martin, 'Cyber Realism in a Time of War', *Lawfare* [blog post] (2 Mar. 2022), para. 10, https://www.lawfareblog.com/cyber-realism-time-war, accessed 1 Mar. 2023; Australian Cyber Security Centre, 'ACSC Annual Cyber Threat Report 2021-22', *Australian Cyber Security Centre* (Canberra, 4 Nov. 2022), 31, https://www.cyber.gov.au/sites/default/files/2022-11/ACSC-Annual-Cyber-Threat-Report-2022.pdf, accessed 5 Mar. 2023.

[10] S. Jaishankar, 'EAM: Global Technology Summit 2022' [video], YouTube (29 Nov. 2022), https://www.youtube.com/live/MR-ebRUHMCU, accessed 9 Mar. 2023.

[11] A. Albanese et al., *Quad Joint Leaders' Statement* [media release] (24 May 2022), para. 25, https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/24/quad-joint-leaders-statement/, accessed 9 Mar. 2023.

[12] Ibid.

[13] Ibid.

certain minimum guidelines in said regulations.[14] These policy announcements collectively will be referred to by this working paper as 'the Pledge'.

The Pledge will be the focus of this working paper. Its thesis is that the Pledge is critical to the delivery of the Quad's agenda. The paper will first outline the Quad governments' cyber diplomacy more generally to provide context for the Pledge. It will question the utility of this diplomacy as a tool for meaningfully improving cyber resilience in the regions it is directed at, arguing that it is not appropriately targeted at a large source of the cyber resilience problem — software (in)security. The working paper will then present the Pledge as the way forward for cyber diplomacy by the four governments, critically analysing its policy merits and concluding that it is necessary for uplifting software security, cyber resilience across the world and thus the fulfilment of the Quad's commitment to tackle cyber-borne threats to (inter)national security.[15] It will build on that analysis by pointing to how the Pledge drives the Quad's internal credibility, making it core to the achievement of the Quad's agenda. The working paper will conclude by pointing to how the benefits of the Pledge are easily transferable outside the Quad, helping position the grouping as a positive force for encouraging the cyber resilience of societies and economies.

2. Existing Cyber Diplomacy by the Quad Countries

To understand the context of the Pledge, it is necessary to understand the cyber diplomacy conducted by the Quad countries more generally, which will now be explored.

2.A. Cyber Diplomacy by the Four Partners

2.A.1. Japan

The cyber diplomacy of Japan is led by its Ambassador in charge of Cyber Policy within the Ministry of Foreign Affairs ('MOFA'), Ambassador Hideo Ishizuki.[16] The work of the Ambassador is complemented by the International Strategy Group of the National Center of Incident Readiness and Strategy for Cybersecurity, a secretariat within Japan's Cybersecurity Strategic

[14] Quad Senior Cyber Group, 'Quad Cybersecurity Partnership: Joint Principles for Secure Software', *Department of the Prime Minister and Cabinet*, (Canberra, 20 May 2023), 2, https://www.pmc.gov.au/sites/default/files/resource/download/quad-joint-principles-secure-software.pdf, accessed 20 May 2023.

[15] Biden et al., *The Spirit of the Quad*, para. 3.

[16] Ministry of Foreign Affairs of Japan, *The 7th Japan – UK Bilateral Consultations on Cyber Issues* [media release] (7 Feb. 2023), para. 2, https://www.mofa.go.jp/press/release/press3e_000542.html, accessed 5 Mar. 2023.

Headquarters.[17] Japanese cyber diplomacy is guided by the country's 2021 strategy for cybersecurity.[18] Among its objectives is Japan strengthening 'International cooperation and collaboration', such as through capacity building initiatives and Japan's broader engagement in the Indo-Pacific.[19] This is echoed by Japan's 2022 *National Security Strategy* which commits the country to 'reinforce its comprehensive defense architecture by promoting efforts in… [areas including] cyber security' in order to grow Japan's deterrent capacity and that of 'like-minded countries'.[20]

Japan has bilateral engagement mechanisms with its Quad partners, France, the United Kingdom, Russia, the European Union and Israel.[21] At the multilateral level, Japan engages with ASEAN.[22] It participates in the ASEAN Regional Forum Inter-Sessional Meeting on Security of and in the Use of Information and Communication Technologies ('ARF ISM').[23] In addition, Japan joined NATO's Cooperative Cyber Defence Centre of Excellence in May 2023.[24] Japan is a member of the International Counter Ransomware Initiative ('ICRI').[25]

---

[17] National Center of Incident Readiness and Strategy for Cybersecurity, 'National Center of Incident Readiness and Strategy for Cybersecurity', *National Center of Incident Readiness and Strategy for Cybersecurity* (2023), para. 15, https://www.nisc.go.jp/eng/index.html, accessed 1 Mar. 2023.

[18] National Center of Incident Readiness and Strategy for Cybersecurity, 'Commitment to a Free, Fair and Secure Cyberspace', *National Center of Incident Readiness and Strategy for Cybersecurity* (2023), para. 15, https://www.nisc.go.jp/eng/index.html, accessed 1 Mar. 2023; The Government of Japan, 'Cybersecurity Strategy', *National Center of Incident Readiness and Strategy for Cybersecurity* (Tokyo, 28 Sep. 2021), https://www.nisc.go.jp/eng/pdf/cs-senryaku2021-en.pdf, accessed 5 Mar. 2023.

[19] The Government of Japan, *Cybersecurity Strategy,* 35-41.

[20] Ministry of Defense (Japan), 'National Security Strategy', *Ministry of Defense* (Tokyo, Dec. 2022), 21, 24, https://www.mod.go.jp/j/policy/agenda/guideline/pdf/security_strategy_en.pdf, accessed 6 Mar. 2023.

[21] Ministry of Foreign Affairs of Japan, 'Cybersecurity', *Ministry of Foreign Affairs of Japan* (7 Feb. 2023), https://www.mofa.go.jp/policy/page18e_000015.html, accessed 5 Mar. 2023.

[22] S. A. M. S. P. T. H. Sen, *Chairman's Statement of the 25th ASEAN-Japan Summit* [media release] (12 Nov. 2022), para. 10, https://www.mofa.go.jp/files/100425548.pdf, accessed 5 Mar. 2023.

[23] Ministry of Foreign Affairs of Japan, *ARF-ISM on ICTs Security 7th OESG* [media release] (28 Apr. 2021), https://www.mofa.go.jp/press/release/press22e_000052.html, accessed 8 Mar. 2023.

[24] NATO Cooperative Cyber Defence Centre of Excellence, *The NATO CCDCOE Welcomes New Members Iceland, Ireland, Japan, and Ukraine* [media release] (17 May 2023), https://ccdcoe.org/news/2023/the-nato-ccdcoe-welcomes-new-members-iceland-ireland-japan-and-ukraine/, accessed 8 May 2023.

[25] The White House, *International Counter Ransomware Initiative 2022 Joint Statement* [media release] (1 Nov. 2022), para. 1, https://www.whitehouse.gov/briefing-room/statements-releases/2022/11/01/international-counter-ransomware-initiative-2022-joint-statement/, accessed 8 Mar. 2023.

2.A.2. Australia

Australia regards cyberspace and critical technology as 'a foreign policy priority'.[26] Its diplomacy in this area is run by the Cyber Affairs and Critical Technology Branch at the Department of Foreign Affairs and Trade, which is headed by an Ambassador for Cyber Affairs and Critical Technology (the position was vacated by Dr Tobias Feakin at the end of 2022).[27] Australia's cyber and critical technology diplomacy is guided by the country's International Cyber and Critical Technology Engagement Strategy, which strives for, among other things, the development of 'secure, resilient and trusted technology' and 'technology foster[ing]… sustainable economic growth and development', such as by 'advocat[ing]… for open, resilient, diverse and competitive international technology markets and supply chains'.[28]

Australia has bilateral partnerships with countries including Singapore, Indonesia, India, the United Kingdom and South Korea.[29] At the multilateral level, Australia participates in the ARF ISM as well as the ARF's Open Ended Study Group on Confidence Building Measures.[30] It leads the ICRI's working group on disruption and chairs the International Counter Ransomware Task Force under the ICRI.[31] Australia runs a range of capacity building initiatives, including the Indo-Pacific-

[26] Department of Foreign Affairs and Trade (Commonwealth of Australia), 'Australia's International Cyber and Critical Tech Engagement', *Australia's International Cyber and Critical Tech Engagement* (7 Mar. 2023), para. 2, https://www.internationalcybertech.gov.au/, accessed 1 Mar. 2023.

[27] Department of Foreign Affairs and Trade (Commonwealth of Australia), 'Organisation Structure', *Department of Foreign Affairs and Trade* (Canberra, 6 Feb. 2023), https://www.dfat.gov.au/sites/default/files/dfat-org-chart-executive.pdf, accessed 1 Mar. 2023; R. Chirgwin, 'Australia's First Cyber Ambassador Moves on', *iTnews* (31 Jan. 2023), paras. 1-3, https://www.itnews.com.au/news/australias-first-cyber-ambassador-moves-on-590318, accessed 1 Mar. 2023.

[28] Department of Foreign Affairs and Trade (Commonwealth of Australia), 'Australia's International Cyber and Critical Technology Engagement Strategy', *Australia's International Cyber and Critical Tech Engagement* (Canberra, 21 Apr. 2021), 10-12, 70, 91-4, https://www.internationalcybertech.gov.au/strategy, accessed 1 Mar. 2023.

[29] Department of Foreign Affairs and Trade (Commonwealth of Australia), 'Partnerships and Agreements', *Australia's International Cyber and Critical Tech Engagement* (2022), https://www.internationalcybertech.gov.au/our-work/partnerships-and-agreements, accessed 12 Mar. 2023.

[30] Department of Foreign Affairs and Trade (Commonwealth of Australia), 'Multilateral Engagement', *Australia's International Cyber and Critical Tech Engagement* (2022), para. 2, https://www.internationalcybertech.gov.au/our-work/multilateral-engagement, accessed 12 Mar. 2023.

[31] The White House, *Fact Sheet: The Second International Counter Ransomware Initiative Summit* [media release] (1 Nov. 2022), paras. 3-4, https://www.whitehouse.gov/briefing-room/statements-releases/2022/11/01/fact-sheet-the-second-international-counter-ransomware-initiative-summit/, accessed 28 Feb. 2023.

focused Cyber and Critical Tech Cooperation Program, and 'leads operational and technical cyber security engagement' in the region through the Australian Cyber Security Centre ('ACSC').[32]

2.A.3. United States

The United States' cyber diplomacy is coordinated by the Bureau of Cyberspace and Digital Policy within the U.S. Department of State.[33] It is led by the inaugural U.S. Ambassador at Large for Cyberspace and Digital Policy, Nathaniel C. Fick.[34] His functions include promoting: 'an open, interoperable, reliable, and secure… [ICT] infrastructure globally'; and capacity building efforts.[35] American cyber diplomacy is guided by a few documents. The United States released a cyber diplomacy strategy in 2011, which is driven by the 'immense potential' of digital technologies.[36] The *2023 NDAA* prescribes the country's 'International Cyberspace Policy' which commits the United States to, for instance, encourage the responsible development of digital products 'that strengthen a secure internet architecture'.[37] The fifth Pillar of the United States' cybersecurity strategy is devoted to its cyber diplomacy, seeking to 'forge international partnerships to pursue shared goals' and, in particular, work with American allies and partners to secure technology supply chains.[38] The United States' national security strategy refers to close cooperation with allies and partners on matters like critical infrastructure cyber resilience.[39] The American strategy for

---

[32] Australian Government, *Australia's Cyber Security Strategy*, 49; Department of Foreign Affairs and Trade (Commonwealth of Australia), 'Capacity Building', *Australia's International Cyber and Critical Tech Engagement* (2022), paras. 1-2, https://www.internationalcybertech.gov.au/our-work/capacity building, accessed 4 Mar. 2023.

[33] U.S. Department of State, 'Bureau of Cyberspace and Digital Policy', *U.S. Department of State* (3 Feb. 2023), para. 1, https://www.state.gov/bureaus-offices/deputy-secretary-of-state/bureau-of-cyberspace-and-digital-policy/, accessed 2 Mar. 2023.

[34] U.S. Department of State, 'Nathaniel C. Fick', *U.S. Department of State* (3 Feb. 2023), https://www.state.gov/biographies/nathaniel-c-fick/, accessed 2 Mar. 2023.

[35] *National Defense Authorization Act for Fiscal Year 2023* (USA), s. 9502(2)(B) ('*2023 NDAA*').

[36] The White House, 'International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World', *National Archives* (Washington, DC, May 2011), 4, https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf, accessed 1 Mar. 2023.

[37] *National Defense Authorization Act for Fiscal Year 2023* (USA), ss. 9501(a)-(b).

[38] The White House, 'National Cybersecurity Strategy', *The White House* (Washington, DC, 2 Mar. 2023), 29-33, https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf, accessed 10 Mar. 2023.

[39] The White House, 'USA National Security Strategy', *The White House* (Washington, DC, 12 Oct. 2022), 34, https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf, accessed 1 Mar. 2023.

the Indo-Pacific commits the government to: 'promote secure and trustworthy digital infrastructure'; and 'build… new regional initiatives to improve collective cybersecurity'.[40]

Bilaterally, the United States engages with countries including South Korea, Ukraine (such as through assistance and capacity building), its Quad partners and the European Union.[41] Multilaterally, the United States engages with ASEAN, including through the ARF ISM.[42] It convenes the ICRI and cooperates through the Abraham Accords with Israel, Bahrain, the United Arab Emirates and Morocco.[43] The United States' capacity building initiatives include the Digital

[40] The White House, 'Indo-Pacific Strategy of the United States', *The White House* (Washington, DC, 11 Feb. 2022) 13, 17, https://www.whitehouse.gov/wp-content/uploads/2022/02/U.S.-Indo-Pacific-Strategy.pdf, accessed 27 Feb. 2023.

[41] U.S. Department of State, *The 3rd U.S.-ROK Working Group Meeting on the DPRK Cyber Threat* [media release] (9 Mar. 2023), https://www.state.gov/the-3rd-u-s-rok-working-group-meeting-on-the-dprk-cyber-threat/, accessed 10 Mar. 2023; Office of the Spokesperson (United States), *U.S. Support for Connectivity and Cybersecurity in Ukraine* [media release] (10 May 2022), https://www.state.gov/u-s-support-for-connectivity-and-cybersecurity-in-ukraine/, accessed 1 Mar. 2023; Office of the Spokesperson (United States), *Joint Statement on Australia-U.S. Ministerial Consultations (AUSMIN) 2022* [media release] (6 Dec. 2022), para. 1, https://www.state.gov/joint-statement-on-australia-u-s-ministerial-consultations-ausmin-2022/, accessed 1 Mar. 2023; The White House, *Fact Sheet: The United States and India — Global Leadership in Action* [media release] (24 Sep. 2021), para. 5, https://www.whitehouse.gov/briefing-room/statements-releases/2021/09/24/fact-sheet-the-united-states-and-india-global-leadership-in-action/, accessed 21 Feb. 2023; Office of the Spokesperson (United States), *Joint Statement of the Security Consultative Committee ("2+2")* [media release] (11 Jan. 2023), para. 22, https://www.state.gov/joint-statement-of-the-security-consultative-committee-22/, accessed 11 Mar. 2023; Office of the Spokesperson (United States), *The 2022 U.S.-EU Cyber Dialogue* [media release] (21 Dec. 2022), https://www.state.gov/the-2022-u-s-eu-cyber-dialogue/, accessed 11 Mar. 2023; G. Raimondo et al., *U.S.-EU Joint Statement of the Trade and Technology Council* [media release] (16 May 2022), 22-26, https://www.commerce.gov/news/press-releases/2022/05/us-eu-joint-statement-trade-and-technology-council, accessed 2 Mar. 2023.

[42] Office of the Spokesperson (United States), *Co-Chairs' Statement on the Third ASEAN-U.S. Cyber Policy Dialogue* [media release] (3 Feb. 2023), para. 4, https://www.state.gov/co-chairs-statement-on-the-third-asean-u-s-cyber-policy-dialogue/, accessed 5 Mar. 2023.

[43] The White House, *ICRI Fact Sheet,* para. 1; A. Neuberger, 'The U.S. Government's Global Cyber Initiatives', *U.S. Department of State* (17 Nov. 2022), para. 5, https://www.state.gov/briefings-foreign-press-centers/global-cyber-initiatives, accessed 2 Mar. 2023; Department of Homeland Security (United States), *DHS Expands Abraham Accords to Cybersecurity* [media release] (2 Feb. 2023), paras. 1-2, https://www.dhs.gov/news/2023/02/02/dhs-expands-abraham-accords-cybersecurity, accessed 1 Mar. 2023.

Connectivity and Cybersecurity Partnership, work under its Indo-Pacific strategy and the 'Unhiding Hidden Cobra' training program to help tackle malicious cyber activity by the North Korean state.[44]

2.A.4. India

India's cyber diplomacy is run by the Cyber Diplomacy Division within the Ministry of External Affairs, headed by Muanpuii Saiawi, Joint Secretary, Cyber Diplomacy.[45] India's 2013 policy on cybersecurity directs the government '[to] enhance global cooperation' on the subject, including among executive and judicial stakeholders, and 'develop bilateral and multi-lateral relationships' on cyber policy matters.[46]

Bilaterally, India has Cyber (Policy) Dialogues and Joint Working Groups with a number of countries including its Quad partners.[47] It also engages with the European Union through the EU-India Trade and Technology Council.[48] India participates in multilateral fora including the: ARF ISM; (along with its Quad partners) United Nations Open-Ended Working Group on security of and in the use of information and

---

[44] U.S. Department of State, 'Digital Connectivity and Cybersecurity Partnership', *U.S. Department of State* (2021), para. 4, https://www.state.gov/digital-connectivity-and-cybersecurity-partnership/, accessed 12 Mar. 2023; Office of the Spokesperson (United States), *Department of State Cybersecurity Training Series Boosts Global Resilience Against Democratic People's Republic of Korea Malware* [media release] (7 Sep. 2022), https://www.state.gov/department-of-state-cybersecurity-training-series-boosts-global-resilience-against-democratic-peoples-republic-of-korea-malware/, accessed 10 Mar. 2023; Office of the Spokesperson (United States), *Marking One Year Since the Release of the Administration's Indo-Pacific Strategy* [media release] (13 Feb. 2023), paras. 74-5, https://www.state.gov/marking-one-year-since-the-release-of-the-administrations-indo-pacific-strategy/, accessed 3 Mar. 2023.

[45] Ministry of External Affairs (India), 'Organogram of the Ministry of External Affairs', *Ministry of External Affairs* (New Delhi, 22 Mar. 2023), https://www.mea.gov.in/Images/amb1/MeA_organograms_NW_23_22NN.pdf, accessed 22 Mar. 2023.

[46] Ministry of Electronics and Information Technology (India), 'National Cyber Security Policy -2013', *Ministry of Electronics and Information Technology* (New Delhi, 2 Jul. 2013), 4, 9, https://www.meity.gov.in/sites/upload_files/dit/files/National Cyber Security Policy (1).pdf, accessed 1 Mar. 2023.

[47] Ministry of External Affairs (India), 'Annual Report 2022', *Ministry of External Affairs* (New Delhi, 23 Feb. 2023), 270, https://mea.gov.in/Uploads/PublicationDocs/36286_MEA_Annual_Report_2022_English_web.pdf, accessed 1 Mar. 2023; Ministry of External Affairs (India), 'Annual Report 2021 | 2022', *Ministry of External Affairs* (New Delhi, 24 Feb. 2022), 231, https://mea.gov.in/Uploads/PublicationDocs/34894_MEA_Annual_Report_English.pdf, accessed 1 Mar. 2023.

[48] European Commission, *EU-India: New Trade and Technology Council to Lead on Digital Transformation, Green Technologies and Trade* [media release] (6 Feb. 2023), para. 4, https://ec.europa.eu/commission/presscorner/detail/en/IP_23_596, accessed 1 Mar. 2023.

communications technologies for 2021–2025; and Shanghai Cooperation Organisation.[49] India co-leads the ICRI working group on resilience.[50] India's capacity building work includes the establishment of Centres of Excellence and Institutes of Technology internationally and the Indian Technical and Economic Cooperation Programme which features courses on cyber resilience taught by Indian institutions.[51]

2.B. Is This Meaningful?

There are questions about whether this diplomacy meaningfully improves cyber resilience because of the continuing success of malicious cyber actors in targeting societies and economies in the Indo-Pacific and indeed the world at large.[52] There have been several breaches of cyber resilience at critical infrastructure assets around the world in recent years, spread across sectors including healthcare,[53]

[49] Ministry of External Affairs (India), *Annual Report 2022*, 270; 'UN OEWG 2021-2025 – International Law', *The Digital Watch Observatory* (2022), para. 2, https://dig.watch/event/un-oewg-2021-2025-2nd-substantive-session/un-oewg-2021-2025-international-law, accessed 1 Mar. 2023.

[50] The White House, *ICRI Fact Sheet,* para. 3.

[51] Indian Technical and Economic Cooperation Programme, 'Upcoming Courses', *Indian Technical and Economic Cooperation Programme* (5 Jan. 2023), https://www.itecgoi.in/upcoming_courses, accessed 1 Mar. 2023; S. Patil, 'India's Cyber Diplomacy', *India Perspectives* (New Delhi, 7 Oct. 2020), para. 5, https://www.indiaperspectives.gov.in/en_US/indias-cyber-diplomacy/, accessed 1 Mar. 2023.

[52] See, eg, European Union Agency for Cybersecurity, 'ENISA Threat Landscape 2022: (July 2021 to July 2022)', *European Union Agency for Cybersecurity* (Athens, 3 Nov. 2022), 7-20, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022, accessed 1 Mar. 2023; Australian Cyber Security Centre, *Annual Cyber Threat Report*, 5, 11; National Security Agency, 'NSA Cybersecurity Year in Review 2022' (Baltimore, 15 Dec. 2022), 2-3, https://media.defense.gov/2022/Dec/15/2003133594/-1/-1/0/0139_CSD_YIR22_FINAL_LOWSIDE_ACCESSIBLE_FINAL_V2.PDF, accessed 11 Mar. 2023; Cybersecurity and Infrastructure Security Agency, *CISA Urges Increased Vigilance One Year After Russia's Invasion of Ukraine* [media release] (23 Feb. 2023), https://www.cisa.gov/news-events/alerts/2023/02/23/cisa-urges-increased-vigilance-one-year-after-russias-invasion-ukraine, accessed 1 Mar. 2023.

[53] France24, 'French Hospital Suspends Operations after Cyber Attacks', *France24* (5 Dec. 2022), https://www.france24.com/en/france/20221205-french-hospital-suspends-operations-after-cyber-attacks, accessed 1 Mar. 2023.

financial services,[54] telecommunications[55] and managed services.[56] Governments from the Global South, such as Guadeloupe,[57] Vanuatu[58] and Papua New Guinea,[59] have been targeted in the not-too-distant past, stymieing the delivery of vital public services in those already vulnerable countries. The debilitating effects of such attacks make one question whether the aforementioned cyber diplomacy is 'cheap talk', not substantive action. The failure to robustly evaluate the effectiveness of counter-cybercrime capacity building work, which seeks to uplift the recipient jurisdiction's cyber resilience, does not help cyber diplomacy's case.[60]

On the other hand, criticising cyber diplomacy using breach statistics can be argued to be unfair. Cyber risk itself is a highly uncertain type of risk and subject to a myriad of drivers, including human frailty, technical vulnerabilities in software or hardware, and shortcomings in the controls of

[54] F. Payão, 'Banco BRB Sofre Ataque de Ransomware e Acaba Chantageado', *tecmundo* (6 Oct. 2022), https://www.tecmundo.com.br/seguranca/250306-banco-brb-sofre-ataque-ransomware-acaba-chantageado.htm, accessed 2 Mar. 2023.

[55] C. Cimpanu, 'Cyberattack Brings down Vodafone Portugal Mobile, Voice, and TV Services', *The Record* (8 Feb. 2022), https://therecord.media/cyberattack-brings-down-vodafone-portugal-mobile-voice-and-tv-services/, accessed 4 Mar. 2023.

[56] A. Martin, 'Multiple Government Departments in New Zealand Affected by Ransomware Attack on IT Provider', *The Record* (6 Dec. 2022), https://therecord.media/multiple-government-departments-in-new-zealand-affected-by-ransomware-attack-on-it-provider/, accessed 5 Mar. 2023.

[57] AP News, 'Guadeloupe Government "Large-Scale" Cyberattack', *AP News* (23 Nov. 2022), https://apnews.com/article/caribbean-puerto-rico-guadeloupe-government-and-politics-0e299e596db2ba25971c947a8f831a61, accessed 5 Mar. 2023.

[58] S. Weigand, 'Government of Vanuatu Offline since Early November in Suspected Ransomware Attack', *SC Media* (12 Dec. 2022), https://www.scmagazine.com/news/ransomware/the-government-of-vanuatu-offline-since-early-november-in-suspected-ransomware-attack, accessed 5 Mar. 2023.

[59] RNZ, 'PNG Government System Hit by Ransomware Attack', *RNZ* (29 Oct. 2021), https://www.rnz.co.nz/international/pacific-news/454467/png-government-system-hit-by-ransomware-attack, accessed 5 Mar. 2023.

[60] United States Government Accountability Office, 'Federal Agency Efforts to Address International Partners' Capacity to Combat Crime', *United States Government Accountability Office* (Washington, DC, 1 Mar. 2023), 25-29, https://www.gao.gov/assets/gao-23-104768.pdf, accessed 4 Mar. 2023.

suppliers.[61] Especially key drivers are the intent and capability of a variety of threat actors.[62] The sheer interconnectivity of computer networks, as highlighted above, and an absence of meaningful metrics make it harder to assess cyber risks.[63] These factors can be argued to make it unfair to attribute breaches of cyber resilience in a jurisdiction to any one factor, such as cyber diplomacy aimed at helping that jurisdiction become more cyber-resilient.

2.C. The Way Forward: Targeting Software Insecurity

The above discussion on cyber diplomacy by the Quad governments and its utility, however, concerns 'cobwebs', not the 'spider'. That is, it is centred around breaches of cyber resilience continuing to occur, rather than going after a major cause of those breaches in the first place: software insecurity.[64] While (as per section 2.A.) the Quad countries' cyber diplomacy seeks to drive cooperation to assure the cyber resilience of digital technologies and infrastructure, official statements very rarely mention software security. In fact, it was only in 2023 (several months after

[61] O. Renn, 'White Paper on Risk Governance: Toward an Integrative Framework', in O. Renn & K.D. Walker, eds., *Global Risk Governance: Concept and Practice using the IRGC Framework* (The Netherlands: Springer, 2008) cited in K. Quigley, C. Burns & K. Stallard, '"Cyber Gurus": A Rhetorical Analysis of the Language of Cybersecurity Specialists and the Implications for Security Policy and Critical Infrastructure Protection', *Government Information Quarterly*, 32/2 (2015), 110, https://doi.org/10.1016/j.giq.2015.02.001.

[62] T. Uren, 'Give Me E2EE or Give Me Death: PLUS: Beware the Tiny Stick of Regulation', *Seriously Risky Business* (2 Mar. 2023), para. 25, https://srslyriskybiz.substack.com/p/give-me-e2ee-or-give-me-death, accessed 3 Mar. 2023; See, eg, Australian Securities and Investments Commission, 'Report 429: Cyber Resilience: Health Check', *Australian Securities and Investments Commission* (Canberra, 19 Mar. 2015), 46-9, https://download.asic.gov.au/media/3062900/rep429-published-19-march-2015-1.pdf, accessed 28 Feb. 2023; Australian Government, *Cyber Security Strategy 2020*, 12-14.

[63] See, eg, United States Government Accountability Office, 'Actions Needed to Better Secure Internet-Connected Devices', *United States Government Accountability Office* (Washington, DC, 1 Dec. 2022), 40-1, https://www.gao.gov/assets/gao-23-105327.pdf, accessed 26 Feb. 2023; United States Government Accountability Office, 'Agencies Need to Assess Adoption of Cybersecurity Guidance', *United States Government Accountability Office* (Washington, DC, 9 Feb. 2022), 15-16, 27-9, 37, https://www.gao.gov/assets/gao-22-105103.pdf, accessed 2 Mar. 2023; Cyber Safety Review Board (United States), 'Review of the December 2021 Log4j Event', *Cybersecurity and Infrastructure Security Agency* (Washington, DC, 11 Jul. 2022), v, https://www.cisa.gov/sites/default/files/publications/CSRB-Report-on-Log4-July-11-2022_508.pdf, accessed 12 Mar. 2023; *Better Cybercrime Metrics Act 2022* (USA), s. 2(2).

[64] See, eg, European Commission, 'Commission Staff Working Document: Impact Assessment Report Accompanying the Document Proposal for a Regulation of the European Parliament and of the Council on Horizontal Cybersecurity Requirements for Products with Digital Elements and amending Regulation (EU) 2019/1020', *EUR-Lex* (Brussels, 15 Sep. 2022), 6, https://eur-lex.europa.eu/resource.html?uri=cellar:af2401a4-34e9-11ed-9c68-01aa75ed71a1.0001.02/DOC_1&format=PDF, accessed 28 Feb. 2023.

the founding of the QCP) that Japan and the United States signed a memorandum of understanding on cyber resilience which was reported to include a commitment to harmonise security standards in government procurement of software.[65]

Governments' failure to pay due attention to software security as an issue is curious because malicious cyber actors increasingly exploit vulnerabilities in the software which runs societies and economies to spy on and/or disrupt them.[66] They are enabled by the systemic inadequacy of software security.[67] They are increasingly targeting software supply chains as a reliable vector en route to compromising critical infrastructure assets.[68] The systemic consequences of such targeting were evident in the NotPetya and WannaCry attacks of 2017 that devastated the Ukrainian state and economy, and the British healthcare system, respectively, and were enabled by the exploitation of vulnerabilities in the Windows operating system.[69] And yet, software vendors like Microsoft continue to (knowingly) market code which is littered with vulnerabilities without being held meaningfully accountable, placing the responsibility for remediating damage from exploitation of those vulnerabilities on end-users, including governments.[70]

---

[65] Nikkei Asia, 'Japan, U.S. to Agree on Security Standards for Government Software: Nishimura and Mayorkas to Sign Memorandum on Cooperation for Cybersecurity', *Nikkei Asia* (5 Jan. 2023), para. 1, https://asia.nikkei.com/Politics/International-relations/Japan-U.S.-to-agree-on-security-standards-for-government-software, accessed 4 Mar. 2023; Department of Homeland Security, *Readout of Secretary Mayorkas's Meeting with Japanese Minister Nishimura* [media release] (6 Jan. 2023), para. 1, https://www.dhs.gov/news/2023/01/06/readout-secretary-mayorkass-meeting-japanese-minister-nishimura, accessed 15 Mar. 2023.

[66] Australian Cyber Security Centre, *Annual Cyber Threat Report,* 11; Agence Nationale de la Sécurité des Systèmes d'Information, 'Cyber Threat Overview 2022', *Agence Nationale de la Sécurité des Systèmes d'Information* (Paris, 15 Jan. 2023), 25-7, https://www.cert.ssi.gouv.fr/uploads/CERTFR-2023-CTI-002.pdf, accessed 1 Mar. 2023.

[67] Attrey et al., *Digital Enablers of the Global Economy*, 13.

[68] European Union Agency for Security, *ETL 2022*, 27, 31.

[69] A. Greenberg, *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers* (United States: Doubleday, 2019), 1; N. Perlroth, *This Is how They Tell Me the World Ends* (United States: Bloomsbury Publishing, 2021), 389, 402; L. J. Trautman & P. C. Ormerod, 'WannaCry, Ransomware, and the Emerging Threat to Corporations', *Tennessee Law Review*, 86 (2019), 528; W. Smart (United Kingdom), 'Lessons Learned Review of the WannaCry Ransomware Attack', *NHS England* (London, 1 Feb. 2018), 8, 10, https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf, accessed 2 Mar. 2023.

[70] See, eg, Office of the National Cyber Director (United States), *Strategic Intent Statement*, 607; J. Easterly & E. Goldstein, 'Stop Passing the Buck on Cybersecurity: Why Companies Must Build Safety into Tech Products', *Foreign Affairs* (1 Feb. 2023), paras. 3, 7, https://www.foreignaffairs.com/united-states/stop-passing-buck-cybersecurity, accessed 1 Mar. 2023; J. Chong, 'Bad Code: The Whole Series', *Lawfare* (4 Nov. 2013), para. 4,

Therefore, cyber diplomacy must involve much more work to assure — in partnership with software vendors — the security of the software that economies and societies depend on to function, both in its development and over its lifecycle. This work should be given momentum by multiple governments — including EU countries, the United States and OECD countries — backing the regulation of software security, including through the creation of a 'duty of care' for software vendors.[71]

The Pledge is the way forward for cyber diplomacy by the Quad because it is targeted at the issue of software security. This paper will now explain why that is the case and thus why the Pledge is core to fulfilling the Quad's agenda, namely its commitment to address challenges to (inter)national security that arise from the cyber domain.[72]

3. The Pledge

The Pledge is defined in *Joint Cybersecurity Principles* that were released at the Quad Leaders' Summit in May 2022 and *Joint Principles for Secure Software* released at the Quad Leaders' Summit in May 2023.[73] Committing to 'jointly align the development of software security frameworks for government software procurement', the governments seek to leverage their 'collective purchasing power' to drive 'market change in software security' and uplift cyber

https://www.lawfareblog.com/bad-code-whole-series, accessed 3 Mar. 2023; The White House, *National Cybersecurity Strategy,* 4-5; N. Reiff, '10 Biggest Software Companies: MSFT, ORCL, and SAP Lead the 10 Biggest Software Companies List', *Investopedia* (28 Feb. 2023), https://www.investopedia.com/articles/personal-finance/121714/worlds-top-10-software-companies.asp, accessed 2 Mar. 2023; European Commission, *Impact Assessment,* 7, 9-10; G. de Salins, 'Understanding the Digital Security of Products: An In-Depth Analysis', *OECD* (Paris, 9 Feb. 2021), 5, 6, 52, https://www.oecd-ilibrary.org/docserver/abea0b69-en.pdf?expires=1679552648&id=id&accname=guest&checksum=D03505E9BD4AB041A6D6A76FA7EC15C6, accessed 1 Mar. 2023.

[71] European Commission, 'Proposal for a Regulation of the European Parliament and of the Council on Horizontal Cybersecurity Requirements for Products with Digital Elements and amending Regulation (EU) 2019/1020', *EUR-Lex* (Brussels, 15 Sep. 2022), 1-2, https://eur-lex.europa.eu/resource.html?uri=cellar:864f472b-34e9-11ed-9c68-01aa75ed71a1.0001.02/DOC_1&format=PDF, accessed 1 Mar. 2023; OECD Council, 'Recommendation of the Council on the Digital Security of Products and Services', *OECD* (Paris, 26 Sep. 2022), Preamble paras. 7, 9, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0481, accessed 27 Feb. 2023; The White House, *National Cybersecurity Strategy*, 19.

[72] Biden et al., *The Spirit of the Quad*, para. 3.

[73] Commonwealth of Australia et al., 'Quad Cybersecurity Partnership: Joint Principles', *Department of Home Affairs* (Canberra, 24 May 2022), paras. 5-7, https://www.homeaffairs.gov.au/cyber-security-subsite/files/qscg-joint-principles.pdf, accessed 2 Mar. 2023; Quad Senior Cyber Group, *Joint Principles for Secure Software*, 2.

resilience across their economies and the software ecosystem as a whole.[74] They aim to 'promote and strengthen a culture where software security is by design and default'.[75] They also commit to 'establishing minimum cybersecurity guidelines for governments to guide their… procurement… of software'.[76]

Specifically, as part of the Pledge, the Quad governments have committed to acquire software meeting certain 'high-level secure software development practices' that echo the categories of controls that are recommended for software developers and vendors by the National Institute of Standards and Technology ('NIST'): 'Prepare the Organization'; 'Protect the Software'; 'Produce Well-Secured Software'; and 'Respond to Vulnerabilities'.[77] The four governments have also committed to incorporate certain 'minimum guidelines' into their procurement standards for software or 'products containing software':

1. Require self-attestation by the software producer, unless a third-party certification is provided, stating that the software's development complies with secure software development practices.
2. Encourage the software developer to report to a respective national vulnerability disclosure program that includes a reporting and disclosure process.[78]

It should be noted that the commitments of the Quad regarding software security extend to more areas than just government procurement. The *Joint Principles for Secure Software* convey the Quad governments' intent to 'where necessary… build policy frameworks' that 'encourage' software developers and suppliers to follow the aforementioned secure software development practices.[79] They also will create 'rigorous and predictable mechanisms to ensure software products function securely and as intended'.[80] This foreshadows the creation of specific regulatory frameworks for the security of software marketed to citizens of the Quad countries generally, rather than merely procurement regulations. Indeed, this echoes the policy of the United States

[74] Ibid.

[75] Quad Senior Cyber Group, *Joint Principles for Secure Software*, 2.

[76] Ibid.

[77] Ibid; M. Souppaya, K. Scarfone & D. Dodson, 'Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities', *National Institute of Standards and Technology* (United States, Feb. 2022), 4, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-218.pdf, accessed 1 Mar. 2023.

[78] Quad Senior Cyber Group, *Joint Principles for Secure Software*, 2.

[79] Ibid.

[80] Ibid.

being to advocate for the imposition of liability on negligent software vendors.[81] In addition, the Quad governments have flagged their intent to implement specified controls to assure the security of their deployment of software.[82] Looking beyond software, the Quad has also committed to align and implement software security standards for managed service providers, and digital goods and services more generally.[83]

This paper is, however, focused on the Pledge because of the economic and regulatory lever this will provide the four governments to drive change in the broader software ecosystem.[84] Additionally, this paper does not address standards for the cyber resilience of technology service providers because these providers have received a significant amount of attention from government agencies[85] and are, to varying degrees, regulated under critical infrastructure laws.[86] Software security, on the other hand, has not received as much or as specific attention, creating an opportunity for this working paper to contribute to the literature.

The policy merits of the Pledge as core to the delivery of the Quad's agenda will now be critically analysed.

3.A. The Criticality of the Pledge

The Pledge's criticality to the fulfilment of the Quad's mission is because of three factors: societies' inherent dependence on secure software; the suboptimal state of software security; and the worsening threat environment for software supply chains. Each component enlivens the security dimension of the Quad as detailed above.

[81] The White House, *National Cybersecurity Strategy*, 20-1.

[82] Quad Senior Cyber Group, *Joint Principles for Secure Software*, 2-3.

[83] Commonwealth of Australia et al., *Joint Cybersecurity Principles*, para. 6.

[84] Ibid, para. 7.

[85] See, eg, European Union Agency for Cybersecurity, 'ENISA Threat Landscape for Supply Chain Attacks', *European Union Agency for Cybersecurity* (Athens, 29 Jul. 2021), 6-12, 15-25, https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks, accessed 5 Mar. 2023.

[86] See, eg, *Security of Critical Infrastructure Act 2018* (Australia) ss. 9(1)(d), 12F; *Parliament and Council Directive 2022/2555 on Measures for a High Common Level of Cybersecurity across the Union, Amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and Repealing Directive (EU) 2016/1148 (NIS 2 Directive)* [2022] OJ L 333/80, art. 2(1), Annex II 9.

3.A.1. Societies' Inherent Dependence on Secure Software

All societies depend on digital technologies, and thus secure software enabling the latter, to thrive.[87] The United States President's National Security Telecommunications Advisory Committee referred to 'software [being] at the foundation of nearly every interaction in today's society'.[88] Software is 'ubiquitous and found in all information and communications technology', making it more than merely a pillar of a modern society.[89]

Therefore, the Quad governments' seeking to use their leverage as major buyers in software markets to uplift software security would benefit all stakeholders whom those markets serve. If governments make their own purchase of, for instance, remote monitoring and management software conditional on a vendor securing their build environments (as defined by the National Security Agency),[90] vendors wanting to sell that software to governments would work to make it harder for malicious actors to infiltrate their build environments and leverage that access to weaponise the software against its users. Vendors' improvement in their overall cyber resilience would yield positive externalities for all users because that software would be less likely an attack vector.

To continue the example, such positive externalities would be of most consequence for societies where operators of critical infrastructure assets use that remote monitoring and management software.[91] With software generally being 'foundational' for these national security-critical assets, they would be less vulnerable to compromise through that particular software product, the vital services

[87] See, eg, de Salins, *An In-Depth Analysis,* 9-10.

[88] President's National Security Telecommunications Advisory Committee (United States), 'Software Assurance in the Information and Communications Technology and Services Supply Chain', *Cybersecurity and Infrastructure Security Agency* (Washington, DC, 2 Nov. 2021), 48, https://www.cisa.gov/sites/default/files/publications/NSTAC Report to the President on Software Assurance.pdf, accessed 2 Mar. 2023.

[89] U.S. Department of Commerce & U.S. Department of Homeland Security, 'Assessment of the Critical Supply Chains Supporting the U.S. Information and Communications Technology Industry', *U.S. Department of Homeland Security* (Washington, DC, 25 Feb. 2022), 33, https://www.dhs.gov/sites/default/files/2022-02/ICT Supply Chain Report_2.pdf, accessed 4 Mar. 2023.

[90] National Security Agency, Cybersecurity and Infrastructure Security Agency & Office of the Director of National Intelligence, 'Securing the Software Supply Chain: Recommended Practices for Developers', *U.S. Department of Defense* (Washington, DC, 1 Sep. 2022), 4-5*,* 27, https://media.defense.gov/2022/Sep/01/2003068942/-1/-1/0/ESF_SECURING_THE_SOFTWARE_SUPPLY_CHAIN_DEVELOPERS.PDF, accessed 4 Mar. 2023.

[91] OECD Council, 'Recommendation of the Council on Digital Security of Critical Activities', *OECD* (Paris, 11 Dec. 2019), Preamble para. 6, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0456, accessed 1 Mar. 2023; J.J. Chung, 'Critical Infrastructure, Cybersecurity, and Market Failure', *Oregon Law Review*, 96(2) (2018), 452.

they provide to society less prone to disruption and society more resilient.[92] The pursuit of software security through the Pledge aligns with the Quad countries calling for 'proper cyber security safeguards' for critical infrastructure assets in light of the interconnectivity and interdependence of those assets, and their commitment to uplift the security of technology supply chains serving those assets.[93] Indeed, the Quad governments recognised the major uplift in critical infrastructure cyber resilience, which will result from their coordinated implementation of baseline software security standards, including through their procurement regulations.[94]

Therefore, the vitality of software security to societies' very functioning grounds the policy merits of the Pledge and its linkage with the Quad's agenda, namely its seeking to mitigate risks to (inter)national security that emanate from the cyber domain.[95]

3.A.2. Worsening Threat Environment for Software Supply Chains

Governments must work together to uplift software security because of the increased weaponisation of societies' inherent dependence on software.[96] For example, the SolarWinds and Kaseya attacks exploited vulnerabilities in software vendors' systems in order to co-opt the channels normally used to push software updates in order to distribute malware to the vendors' customers.[97] The SolarWinds attack was espionage attributed to the Russian state.[98] The Kaseya

[92] Cybersecurity and Infrastructure Security Agency Information and Communications Technology Supply Chain Risk Management Task Force, 'Information and Communications Technology Supply Chain Risk Management Task Force Year 2 Report: Status Update on Activities and Objectives of the Task Force', (Washington, DC, 17 Dec. 2020), 7, https://www.cisa.gov/sites/default/files/publications/ict-scrm-task-force_year-two-report_508.pdf, accessed 3 Mar. 2023.

[93] Commonwealth of Australia et al., *Joint Principles*, paras. 2-3.

[94] Ibid, para. 5.

[95] Biden et al., *The Spirit of the Quad*, para. 3.

[96] T. Herr et al., 'Breaking Trust: Shades of Crisis across an Insecure Software Supply Chain', *Atlantic Council* (Washington, DC, 26 Jul. 2020), 25, https://www.atlanticcouncil.org/wp-content/uploads/2020/07/Breaking-trust-Shades-of-crisis-across-an-insecure-software-supply-chain.pdf, accessed 1 Mar. 2023.

[97] K. Beaumont, 'Kaseya Supply Chain Attack Delivers Mass Ransomware Event to US Companies', *DoublePulsar* [blog post] (3 Jul. 2021), para. 2, https://doublepulsar.com/kaseya-supply-chain-attack-delivers-mass-ransomware-event-to-us-companies-76e4ec6ec64b, accessed 11 Mar. 2023; Mandiant, 'Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims with SUNBURST Backdoor', *Mandiant* (10 May 2022), para. 7, https://www.mandiant.com/resources/blog/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor, accessed 1 Mar. 2023.

[98] The White House, *Fact Sheet: Imposing Costs for Harmful Foreign Activities by the Russian Government* [media release] (15 Apr. 2021), para. 11, https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/, accessed 3 Mar. 2023.

attack was executed by a ransomware group based in Russia, a country where organised cybercrime groups function as state proxies and were assessed as a likely threat to Western critical infrastructure assets.[99] These are but a few of the factors behind why the 'threat environment for software is virtually impossible to anticipate', an issue exacerbated by software supply chain attacks being estimated to have at least quadrupled in 2021 relative to 2020.[100]

In 2022, governments themselves warned of the escalated threat to software supply chains. The ACSC noted threat actors paying attention to the 'supply chain as a priority target and vector for compromise'.[101] Of particular concern were attempts to leverage pervasively-deployed software as an attack vector, and the speed by which malicious state actors and cybercriminals exploit reported critical vulnerabilities.[102] The Cybersecurity and Infrastructure Security Agency ('CISA') offered a similar warning in relation to highly sophisticated threat actors more generally.[103] The European Union Agency for Cybersecurity predicted malicious, well-resourced state-backed actors and cybercriminals alike to increasingly have the intent and capability to target software supply chains.[104] French authorities referred to software supply chain attacks as '[continuing] to pose a

[99] National Counterintelligence and Security Center, 'Kaseya VSA Supply Chain Ransomware Attack', *Director of National Intelligence* (10 Apr. 2021), https://www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/Kaseya VSA Supply Chain Ransomware Attack.pdf, accessed 2 Mar. 2023; Perlroth, *This Is How*, 365; Cybersecurity and Infrastructure Security Agency et al., 'Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure', *U.S. Department of Defense* (Washington, DC, 20 Apr. 2022), 8, https://media.defense.gov/2022/Apr/20/2002980529/-1/-1/1/JOINT_CSA_RUSSIAN_STATE-SPONSORED_AND_CRIMINAL_CYBER_THREATS_TO_CRITICAL_INFRASTRUCTURE_20220420.PDF, accessed 2 Mar. 2023; F. Bajak, 'How the Kremlin Provides a Safe Harbor for Ransomware', *Associated Press News* (17 Apr. 2021), https://apnews.com/article/business-technology-general-news-government-and-politics-c9dab7eb3841be45dff2d93ed3102999, accessed 2 Mar. 2023; U.S. Department of the Treasury, *Treasury Sanctions Russia with Sweeping New Sanctions Authority* [media release] (15 Apr. 2021), para. 14, https://home.treasury.gov/news/press-releases/jy0127, accessed 12 Mar. 2023.

[100] President's National Security Telecommunications Advisory Committee (United States), *Software Assurance,* 20; E. Orzel, 'Software Supply Chain Attacks: 2021 in Review', *Aqua Blog* [blog post] (25 Jan. 2022), para. 4, https://blog.aquasec.com/software-supply-chain-attacks-2021, accessed Mar. 2023.

[101] Australian Cyber Security Centre, *Annual Cyber Threat Report,* 65.

[102] Ibid, 58-9.

[103] Cybersecurity and Infrastructure Security Agency, 'Defending against Software Supply Chain Attacks', *Cybersecurity and Infrastructure Security Agency* (26 Apr. 2021), 5, https://www.cisa.gov/sites/default/files/publications/defending_against_software_supply_chain_attacks_508_1.pdf, accessed 1 Mar. 2023.

[104] European Union Agency for Security, *ETL 2022*, 27, 30-1.

systemic risk'.[105] Governments, including Quad governments (as gauged from the *Joint Principles* and the authorship of the above warnings), are well-aware of the increased threat to national security via the compromise of software supply chains. That governments recognise the need for them to mount a robust policy response is underlined by the frankness of the language in these quotes.

The Quad itself carried this forward in 2023, with the *Joint Principles for Secure Software* beginning with the following sentence: 'The Quad partners recognize the security risks posed by lack of adequate controls to prevent tampering with the software supply chain by adversarial and non-adversarial threats'.[106]

These factors enliven the (inter)national security rationale for the Pledge, particularly when Google seconded the above warnings by considering software supply chain security to be 'one of the most critical national security risks facing government worldwide'.[107] The Pledge is thus core to the Quad delivering on its overarching mission to tackle cyber-borne threats to (inter)national security.[108]

3.A.3. Suboptimal State of Software Security

The gravity of the threat landscape is exacerbated by the suboptimal state of software security. The Atlantic Council defined it in 2020 as 'inadequate and, in some critical respects, getting worse'.[109] A year later, the MITRE Corporation said software supply chain security measures lacked 'systemic integrity'.[110] In early 2023, the Director of CISA explicitly called out technology vendors for marketing software which renders end-users as the vendors' 'crash test dummies… with real-word consequences'.[111] Indeed, the very launch of the *Joint Principles for Secure Software* at a Quad Leaders' Summit in May 2023, with 'the goal… to significantly reduce the

[105] Agence Nationale de la Sécurité des Systèmes d'Information, *Cyber Threat Overview 2022*, 30.

[106] Quad Senior Cyber Group, *Joint Principles for Secure Software*, 2.

[107] Google, 'Perspectives on Security: Volume One: Securing Software Supply Chains', *Google* (8 Dec. 2022), 6, https://services.google.com/fh/files/blogs/perspectives_on_security_volume_one_digital.pdf, accessed 2 Mar. 2023.

[108] Biden et al., *The Spirit of the Quad*, para. 3.

[109] Herr et al., *Breaking Trust*, 6.

[110] C. Clancy et al., 'Deliver Uncompromised: Securing Critical Software Supply Chains', *MITRE* (United States, 29 Jan. 2021), i, https://www.mitre.org/sites/default/files/2021-11/prs-21-0278-deliver-uncompromised-securing-critical-software-supply-chain.pdf, accessed 2 Mar. 2023.

[111] J. Easterly, 'CISA Director Easterly Remarks at Carnegie Mellon University', *Cybersecurity & Infrastructure Security Agency* (Washington, DC, 27 Feb. 2023), paras. 12, 15, 22, https://www.cisa.gov/cisa-director-easterly-remarks-carnegie-mellon-university, accessed 2 Mar. 2023.

number and potential impact of software vulnerabilities', underlines the degree of the software security problem.[112] These statements capture how the policy stakes for governments to act have only grown in recent years.

The need for governments to enact legal standards like procurement regulations (in the manner of the Pledge) in order to uplift software security arises due to the inadequacy of market forces to do so.[113] Vendors remain more concerned with the speed by which they can get software ready for sale and its functionality than investing in a secure software development life cycle ('SDLC').[114] In the European Union, for instance, this has meant only half of technology vendors have 'a systematic approach to secure [digital] product development'.[115] That is an indictment of extant incentive structures, as was the European Commission's estimate that enacting mandatory security standards for the development of all software would reduce the attack surface for digital technology by a third.[116] It is thus little wonder that the United States went as far as advocating the imposition of liability on negligent software vendors.[117] The Pledge itself is targeted at raising the security of vendors' SDLCs, with the governments referring to their commitment as 'integrating secure software practices throughout the software lifecycle'.[118] This is complemented by how the Quad seeks to 'promote and strengthen a culture where software security is by design and default'.[119]

The need for governments to re-shape these incentive structures is accentuated by structural features of the software ecosystem that make it even more prone to compromise.

Firstly, software supply chains are inherently complex and populated by actors with varying attitudes to software development.[120] For example, from 1 January to 30 June 2022, Mandiant observed enterprises, on average, to have '244 unique technology vendors and business

---

[112] Quad Senior Cyber Group, *Joint Principles for Secure Software*, 2.

[113] G. de Salins, 'Enhancing the Digital Security of Products: A Policy Discussion', *OECD* (9 Feb. 2021), 12, https://www.oecd-ilibrary.org/docserver/cd9f9ebc-en.pdf?expires=1679558080&id=id&accname=guest&checksum=5BE96FFD158E0E2A7D46C8CCE6CC9DAE, accessed 2 Mar. 2023.

[114] European Commission, *Impact Assessment*, 11.

[115] Ibid, 39.

[116] Ibid, 51.

[117] The White House, *National Cybersecurity Strategy*, 20-1

[118] Quad Senior Cyber Group, *Joint Principles for Secure Software*, 2.

[119] Ibid.

[120] De Salins, *A Policy Discussion*, 10.

relationships' each.[121] These actors are spread across geographies and at least some of them may neither reasonably invest in a robust SDLC nor be legally required to specifically do so.[122] As this complexity increases, so does the difficulty for stakeholders, including vendors, to map vulnerabilities across their software supply chains and remedy them, encouraging a larger attack surface for software end-users.[123] Exacerbating matters is the absence of a 'standard method for software development'. [124] In this regard, the 'conflicting incentives' and regulatory inconsistencies that define software supply chains [125] provide threat actors with several vulnerabilities to exploit. In laying down standards for vendors to be eligible for lucrative government procurement in terms of establishing and maintaining a secure SDLC,[126] the Pledge will help promote uniformly robust practices and controls that prioritise security in the software ecosystem. In particular, it will stimulate investment in secure SDLCs by vendors because they will otherwise be unable to attest to government customers, or receive third-party certification, that they follow secure software development practices (as will be required per the Pledge).[127]

Secondly, there is a misallocation of responsibility for assuring software security.[128] Vendors tend to incorporate (open source) software written by third parties into their own code ('direct dependencies') without performing robust due diligence and are thus reckless as to the risks that they introduce for their end-users.[129] Stakeholders may also be unable to compel third-party party

[121] Mandiant, 'The Defender's Advantage: Cyber Snapshot Issue 2', *Mandiant* (17 Oct. 2022), 12, https://mandiant.widen.net/s/j2qvgwwhmm/defenders-advantage-cyber-snapshot-report-issue-2, accessed 1 Mar. 2023.

[122] U.S. Department of Commerce & U.S. Department of Homeland Security, *Assessment*, 34-5; De Salins, *A Policy Discussion*, 10; National Security Agency, Cybersecurity and Infrastructure Security Agency & Office of the Director of National Intelligence, *Recommended Practices for Developers*, 4-5*,* 27.

[123] Google, *Perspectives on Security*, 6.

[124] President's National Security Telecommunications Advisory Committee (United States), *Software Assurance,* 15.

[125] Ibid, 16.

[126] Quad Senior Cyber Group, *Joint Principles for Secure Software*, 2; Commonwealth of Australia et al., *Joint Cybersecurity Principles*, para. 6.

[127] Ibid.

[128] De Salins, *A Policy Discussion*, 12; OECD Council, *Digital Security of Products and Services*, Preamble para. 9.

[129] President's National Security Telecommunications Advisory Committee (United States), *Software Assurance,* 13, 17; Herr et al., *Breaking Trust*, 25; R. Kikas et al., 'Structure and Evolution of Package Dependency Networks', paper presented to the 2017 IEEE/ACM 14th International Conference on Mining Software Repositories (MSR), Buenos Aires (20 - 21 May 2017), 103, https://www.computer.org/csdl/proceedings-article/msr/2017/07962360/12OmNyRPgq5, accessed 2 Mar. 2023; ; A. Smith et al., 'Mitigating ICT Supply Chain Risks with Qualified Bidder and Manufacturer Lists: Recommendations on the Use of Qualified Lists and Considerations for the Evaluation of Supply Chain Risks',

code authors to disclose their security practices or promptly resolve vulnerabilities.[130] In turn, malicious actors can compromise software downstream through the third-party code incorporated into that final product, something about which they already 'have no qualms'.[131] Given that the standards to be laid down by the Pledge, as above, will include those for vulnerability management, it will incentivise vendors to more carefully regulate their use of third-party code and assure that patches are promptly issued for their own products to resolve vulnerabilities stemming from their direct dependencies. If governments require software vendors to demonstrate a capability to check risks from third-party code, this will also drive vendors to perform (more robust) due diligence of these direct dependencies and their authors. End-users will benefit from vendors being required to disclose (at least) the direct dependencies of their products through software bills of materials (specifically mentioned by the Pledge), given that this will help them more swiftly identify and manage their own software supply chain risks.[132] One should also note that the Quad governments have specifically committed to acquire software from vendors that 'maintain adequate records of the details and supply chain relationships of the various components used in each release'.[133] This would require vendors to better map out their software supply chains, understand the direct and transitive dependencies of their code, and work with upstream members of their software supply chains to better manage risks therefrom.

Therefore, with the failure of market forces to incentivise meaningful investment by vendors in their SDLCs as well as structural issues in the software ecosystem, there is a need for governments to intervene. This intervention ought to leverage their procurement regulations, that is, the

Cybersecurity & Infrastructure Security Agency (Washington, DC, Apr. 2021), 19, https://www.cisa.gov/sites/default/files/publications/ICTSCRMTF_Qualified-Bidders-Lists_508.pdf, accessed 10 Mar. 2023.

[130] President's National Security Telecommunications Advisory Committee (United States), *Software Assurance,* 13, 16.

[131] R. Alderfer et al. (United States), 'Report on Recommended Best Practices to Improve Communications Supply Chain Security', *Federal Communications Commission* (Washington, DC, Sep. 2022), https://www.fcc.gov/file/23839/download, accessed 1 Mar. 2023.

[132] Quad Senior Cyber Group, *Joint Principles for Secure Software*, 2; Commonwealth of Australia et al., *Joint Cybersecurity Principles*, para. 6; National Telecommunications and Information Administration (United States), 'SBOM at a Glance', *National Telecommunications and Information Administration* (Washington, DC, 2021), 1, https://ntia.gov/sites/default/files/publications/sbom_at_a_glance_apr2021_0.pdf, accessed 2 Mar. 2023.

[133] Quad Senior Cyber Group, *Joint Principles for Secure Software*, 2.

economic incentives provided by their purchasing power in software markets, an approach which the United States champions in particular.[134]

All in all, societies' inherent dependence on software to function, the growing threats to their security via software supply chain compromises and the suboptimal state of software security necessitate the Pledge as a tool to help the Quad 'address shared [security] challenges, including in cyber space'.[135]

That said, there is a narrative against the Pledge which its critics can raise.

3.B. Potential Narrative against the Pledge

Critics can argue that the Pledge is an attempt by the four governments to distort software markets to suit their own interests, rather than those of the Indo-Pacific or the world at large. This narrative has three planks, namely that the Pledge is: contrary to multilateralism and multi-stakeholderism in technology governance; weaponising software dependencies; and securitising technology supply chains.

3.B.1. Contrary to Multilateralism and Multi-Stakeholderism in Technology Governance

Critics can argue that the world's first-, third- and fifth-largest economies, aided by Australia, will use the Pledge to assert hegemony over technology supply chains, thus seeing to undermine multilateralism in technology governance.[136] The governments themselves refer to the sheer size of their purchasing power as a lever for exerting influence over software markets.[137] They have not committed to coordinate with, for instance, the members of the Global South in developing software security standards. This can encourage the perception of the Pledge, and indeed the Quad, as not catering to the needs of the more vulnerable members of the international community. This narrative can riff with the Chinese(-aligned) narrative about the Quad itself as an 'exclusionary bloc' designed to work 'against' and 'contain' China.[138]

---

[134] The White House, *National Cybersecurity Strategy*, 22; Exec. Order No. 14,028, 86 Fed. Reg. 26,633, 26,637-41 (17 May 2021).

[135] Biden et al., *The Spirit of the Quad*, para. 3.

[136] ANI, 'India Becomes 5th Largest Economy in World: A Perspective', *ANI* (17 Sep. 2022), para. 1, https://www.aninews.in/news/world/asia/india-becomes-5th-largest-economy-in-world-a-perspective20220917025023/, accessed 1 Mar. 2023.

[137] Commonwealth of Australia et al., *Joint Principles*, para. 5.

[138] See, eg, S. Haidar & A. Krishnan, 'Quad Foreign Ministers Take Aim at Russia and China: The Joint Statement that Refers to Both the Ukraine Conflict and the Situation in the South and East China Seas, Draws Criticism from Russia

Critics of the Pledge can also allege it to be bypassing the very multi-stakeholder vision for technology governance which the Quad governments claim to champion.[139] By using their purchasing power to shape vendor behaviour, the Quad can be accused of acting contrary to their goal of 'sustained engagement in standards development processes' that involve stakeholders other than governments.[140] The Pledge can be viewed as unilateral action to assert government influence over technology and the Internet, echoing what Western governments accuse authoritarian states like China of doing.[141] The Pledge can be argued to have an insular purpose: bolstering technology supply chains 'on which our [Quad countries'] critical infrastructure provider[s] rely', rather than supply chains serving the world at large.[142]

The Quad governments can be viewed as bypassing even the industry-driven standardisation which occurs through market forces.[143] When international standards development organisations fail to reach consensus on a new standard, they will '[allow] market forces to pick the winner' from the candidate standards, not governments.[144] Critics can point to how, though the Pledge has a software security objective, the very concept of security is political because 'security is always for someone and some purpose'.[145] Therefore, akin to the United States committing to 'instil our

---

and China', *The Hindu* (4 Mar. 2023), para. 10, https://www.thehindu.com/news/international/quad-foreign-ministers-take-aim-at-russia-and-china/article66577074.ece, accessed 1 Mar. 2023; SBS News, 'China Has Slammed the Quad Alliance as a "Tool to Contain" the Country: Chinese Foreign Spokesperson Zhao Lijian Accused Quad Countries of Adopting a "Cold War Mentality"', *SBS News* (22 Feb. 2022), para. 1, https://www.sbs.com.au/news/article/china-has-slammed-the-quad-alliance-as-a-tool-to-contain-the-country/du6mr96w5, accessed 2 Mar. 2023.

[139] Ministry of External Affairs (India), *Annual Report 2022*, 270; Department of Foreign Affairs and Trade (Commonwealth of Australia), *Australia's International Cyber and Critical Technology Engagement Strategy*, 11; *National Defense Authorization Act for Fiscal Year 2023* (USA), ss. 9501(a)(1), 9502(a); The Government of Japan, *Cybersecurity Strategy,* 5-6, 13.

[140] The White House, *National Cybersecurity Strategy*, 24.

[141] See, eg, Ibid; Fleming, J., 'Director GCHQ Speaks at CyberUK 2022', *GCHQ* (10 May 2022), para. 28, https://www.gchq.gov.uk/speech/cyberuk2022, accessed 1 Mar. 2023.

[142] Commonwealth of Australia et al., *Joint Principles*, paras. 3.

[143] D.A. Barnes, 'Deworming the Internet', *Texas Law Review*, 83/1 (2004), 291.

[144] M. Sheehan & J. Feldgoise, 'What Washington Gets Wrong about China and Technical Standards', *Carnegie Endowment for International Peace* (Washington, DC, 27 Feb. 2023), 2, https://carnegieendowment.org/2023/02/27/what-washington-gets-wrong-about-china-and-technical-standards-pub-89110, accessed 28 February 2023.

[145] B. Buzan, O. Waever & J. de Wilde, *Security: A New Framework for Analysis* (London: Lynne Rienner Publishers, 1998) cited in R. Deibert, 'Divide and Rule: Republican Security Theory as Civil Society Cyber Strategy', *Georgetown Journal of International Affairs*, 14/3 (2013), 40.

values' in cyberspace, the four governments can be accused of seeking to impose their approach to software security on the world at large through the standards they will develop together and incorporate into their national procurement regulations.[146]

3.B.2. Weaponising Software Dependencies

Given the above, the Pledge can be framed as the Quad's weaponisation of other countries — especially poorer countries' — software dependencies on vendors and other key members of global software supply chains that are based in the Quad countries or (want to) count any of the Quad governments as customers. After all, the United States sits atop the global software market while India was predicted in 2022 to have the world's largest developer labour force by 2024.[147] This is arguably similar to how more powerful countries weaponise interdependence of weaker countries by exploiting their sitting atop 'hierarchical economic networks'.[148] Their favourable position stems from their having political authority and institutional capacity to control chokepoints in global value chains that they already occupy, such as by regulating the flow of goods and services through those chokepoints.[149] Critics can argue that the Quad's capacity for such weaponisation is implied by the sheer proportion of the world's data and activity online which is controlled by American technology firms, as well as the absence of meaningful alternatives to those firms.[150] In this vein, the Quad countries, particularly through the United States, can be argued to seek to reshape software markets by using their buying power, through their procurement regulations, to reshape incentives for global software vendors that happen to be headquartered in Quad countries or (want to) sell their wares to any of the Quad governments.

3.B.3. Securitisation of Technology Supply Chains

In a similar vein, critics can also position the Pledge purely as a tool for deepening the bifurcation of 'Big Tech' and 'Red Tech', that is, of American- and Chinese-led technology blocs, respectively.[151] Given a goal of the Pledge being to safeguard technology supply chains serving

---

[146] The White House, *National Cybersecurity Strategy*, 24.

[147] U.S. Department of Commerce & U.S. Department of Homeland Security, *Assessment*, 35.

[148] A. Narlikar, 'Must the Weak Suffer What They Must?', in D.W. Dresser, H. Farrell & A.L. Newman, *The Uses and Abuses of Weaponized Interdependence* (Washington, DC: Brookings Institution Press, 2021), 290.

[149] Ibid.

[150] Ibid, 291; J. Bateman, 'The Antitrust Threat to National Security', *Carnegie Endowment for International Peace* (22 Oct. 2019), paras. 6-7, https://carnegieendowment.org/2019/10/22/antitrust-threat-to-national-security-pub-80404, accessed 5 Mar. 2023.

[151] S. Saran & S. Mattoo, 'Big Tech vs. Red Tech: The Diminishing of Democracy in the Digital Age', *Observer Research Foundation* (15 Feb. 2022), para. 2, https://www.orfonline.org/research/big-tech-vs-red-tech/, accessed 8 Mar. 2023.

Quad countries' critical infrastructure assets, critics can allege the Pledge to be an example of the Western bloc's apparent securitisation of technology supply chains; drawing parallels with how the Quad countries' (indirectly) excluded equipment marketed by Huawei and ZTE from their telecommunications networks and/or government procurement.[152] Such action can be argued to reflect the Quad's being more concerned with the security of its own members, rather than seeking to help the international community — especially the Global South — navigate a worsening cyber threat landscape (as outlined in section 2.B.).

Points of rebuttal to the above anti-Pledge narrative will now be explained.

3.C. Rebuttal to the Anti-Pledge Narrative

The anti-Pledge narrative can be rebutted by highlighting how the Pledge: yields positive externalities; drives the delivery of public goods in every country; upholds multi-stakeholderism in technology governance; and upholds multilateralism in technology governance. These points of rebuttal also reinforce the nature of the Pledge as fundamental to the delivery of the Quad's agenda, namely its security facet (detailed above).

3.C.1. Yielding Positive Externalities

Any legal measure, such as procurement standards, which drives software vendors to invest in secure SDLCs will ultimately benefit all of their users. In seeking to win government contracts, if vendors make that investment, they will increase the security of all software produced through those hardened SDLCs. Given that 'software powers almost every component of modern society' (as detailed in section 3.A.1.), this will have positive externalities for the world at large.[153] This is all the more likely because of the dominance of American vendors in the global software market and the purchasing power particularly of the American government, which has proposed to spend

[152] 15 USC s. 1602; 47 USC s. 1603; 47 CFR ss. 1.5000, 2.903(a), 2.906(d), 2.907(c), 54.9(a), (d); Public Safety and Homeland Security Bureau (United States), 'List of Equipment and Services Covered By Section 2 of The Secure Networks Act', *Federal Communications Commission* (20 Sep. 2022) https://www.fcc.gov/supplychain/coveredlist, accessed 1 Mar. 2023; Department of Telecommunications (India), 'Amendment to the Unified Access Services License Agreement (UASL) for Procurement of Telecommunication Equipment' (New Delhi, 11 Jul. 2022), https://dot.gov.in/accessservices/amendment-unified-access-services-license-agreement-uasl-procurement, accessed 1 Mar. 2023; T. Uren & D. Cave, 'Why Australia Banned Huawei from Its 5G Telecoms Network', *Australian Strategic Policy Institute* (30 Aug. 2018), para. 9, https://www.aspi.org.au/opinion/why-australia-banned-huawei-its-5g-telecoms-network, accessed 1 Mar. 2023; Reuters, 'Japan to Ban Huawei, ZTE from Govt Contracts -Yomiuri', *Reuters* (7 Dec. 2018), https://www.reuters.com/article/japan-china-huawei-idUSL4N1YB6JJ, accessed 2 Mar. 2023.

[153] Google, *Perspectives on Security*, 5.

US$74 billion on information technology at federal civilian agencies and around US$12.7 billion for federal 'civilian cybersecurity-related activities' in the Fiscal Year 2024.[154]

The positive externalities of the Pledge particularly include the greater cyber resilience of critical infrastructure assets, systems vital to national security.[155] Given the dependence of these assets on secure software to function (as flagged above), they would be harder targets for malicious cyber actors. If the continuity of essential services that these assets provide can be assured, citizens have confidence in the continuance of 'economic and community stability', and thus national security.[156] This reflects the significant benefits of the Pledge as a tool to incentivise vendors to resolve security issues in their code at the earliest possible point in their SDLCs, driving 'stronger security and resiliency'.[157] The benefits of securer software supply chains servicing critical infrastructure assets were also recognised by the G7 Leaders in May 2023 when they warned of risks from 'geopolitical and geo-economic upheavals' to supply chains servicing G7 countries' critical infrastructure.[158] So significant are these externalities that the G7 Leaders committed to counter malicious cyber activity to 'protect global value and supply chains from illegitimate influence, espionage, illicit knowledge leakage, and sabotage'.[159]

The Pledge will also enable and safeguard economic development around the world, given the criticality of secure digital technologies to the achievement of the United Nations ('UN') Sustainable Development Goals ('SDGs').[160] Secure software is vital to the achievement of SDG 9,

---

[154] U.S. Department of Commerce & U.S. Department of Homeland Security, *Assessment*, 35; Office of Management and Budget (United States), 'Analytical Perspectives: Budget of the U.S. Government: Fiscal Year 2024', *U.S. Government Publishing Office* (Washington, DC, 13 Mar. 2023), 153-7, https://www.govinfo.gov/content/pkg/BUDGET-2024-PER/pdf/BUDGET-2024-PER.pdf, accessed 2 Mar. 2023.

[155] See, eg, The White House, *National Security Strategy*, 34.

[156] Parliamentary Joint Committee on Intelligence and Security (Commonwealth of Australia), 'Advisory Report on the Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022', *Parliament of Australia* (Canberra, Mar. 2022), 6, 62, https://parlinfo.aph.gov.au/parlInfo/download/committees/reportjnt/024898/toc_pdf/AdvisoryreportontheSecurityLegislationAmendment(CriticalInfrastructureProtection)Bill2022.pdf;fileType=application/pdf, accessed 3 Mar. 2023.

[157] Souppaya, Scarfone & Dodson, *SSDF*, 1, 4.

[158] J. R. Biden et al., *G7 Leaders' Statement on Economic Resilience and Economic Security* [media release] (20 May 2023), para. 6, https://www.whitehouse.gov/briefing-room/statements-releases/2023/05/20/g7-leaders-statement-on-economic-resilience-and-economic-security/, accessed 20 May 2023.

[159] Ibid.

[160] Secretary-General of the United Nations, 'Roadmap for Digital Cooperation', *United Nations* (New York, 11 Jun. 2020), 22, https://www.un.org/en/content/digital-cooperation-

given that it underpins the functioning of every digital economy, as above. The UN Secretary-General similarly called for countries to 'prioritize broader issues of trust and security to reap the benefits of the digital domain' in working towards the SDGs.[161] The Pledge has a role to play here, contrary to an argument that the QCP is focused solely on advancing the interests of the Quad countries and weaponising the Global South's dependence on Western-led software supply chains. Indeed, one should also recognise that the Pledge does not concern the strengthening of the Quad countries' offensive cyber capabilities; quite the opposite because uplifting software security makes computer networks harder targets for threat actors including the Quad countries' intelligence agencies.

The aforementioned positive externalities also feed into the next point of rebuttal to the anti-Pledge narrative: that the Pledge drives the delivery of public goods.

3.C.2. Driving the Delivery of Public Goods

Public goods are non-excludable (it is not feasible to exclude a person from using the good) and non-rivalrous (one person's use of the good does not affect another person's use of it).[162]

Software security is a public good for every country. Firstly, since software can be infinitely copied, it is non-rivalrous. By extension, the benefits of the 'hygiene' of that software are non-rivalrous, both in relation to the users of the software and society as a whole, which relies on systems running that software. Secondly, software security is non-excludable. It is because software vendors cannot exclude persons who free-ride on the broader societal benefits of higher software security that they do not appropriately invest in secure SDLCs.[163] When implementing the Pledge, neither will the Quad governments have the capability nor the intent to exclude those in other countries from benefiting from higher software security, as highlighted in sections 3.A.1. and 3.C.1. Thirdly, since vendors are not held responsible for the negative externalities of malicious cyber actors exploiting vulnerabilities in their software (such as lower national cyber resilience and national security), they fail to internalise these externalities, are not driven to invest in a

roadmap/assets/pdf/Roadmap_for_Digital_Cooperation_EN.pdf, accessed 28 February 2023; *International Telecommunications Union,* 'Digital Technologies to Achieve the UN SDGs', *International Telecommunications Union* (12 Dec. 2021), paras. 1-2, https://www.itu.int/en/mediacentre/backgrounders/Pages/icts-to-achieve-the-united-nations-sustainable-development-goals.aspx, accessed 2 Mar. 2023.

[161] Secretary-General of the United Nations, *Roadmap*, 20.

[162] T.Y. Ebrahim, 'National Cybersecurity Innovation', *West Virginia Law Review* 123/2 (2020), 522.

[163] N.A. Sales, 'Regulating Cyber-Security', *Northwestern University Law Review*, 107/4 (2013), 1528; C.J. Coyne & P.T. Leeson, 'Who's to Protect Cyberspace', *Journal of Law, Economics and Policy*, 1/2 (2005), 480.

secure SDLC and thus ‘under-produce' software security.[164] These three factors create a market failure,[165] namely inadequate software security (detailed in section 3.A.3.), and highlight the nature of software security as a public good. As a means by which the Quad governments intervene in software markets to incentivise vendors to invest in a secure SDLC, the Pledge becomes even more necessary; particularly since software security is vital for all societies, as detailed above. Indeed, the Quad countries themselves point to how high the stakes are when it comes to national security risks from software supply chain risks.[166]

One should also note that national security and national cyber resilience are public goods in every country. Neither can a government exclude anyone in their jurisdiction from enjoying national security nor can a person’s so benefitting undermine another person’s benefiting from that national security.[167] The same analysis applies to national cyber resilience, a driver of national security,[168] which makes national cyber resilience a public good. These public goods stand in contrast to a club good where, even though enjoyment of the good is non-rivalrous, but a degree of exclusion of persons from that enjoyment is possible.[169] As above, software security feeds directly into national cyber resilience and national security, making the Pledge a vital tool with which to incentivise software vendors to contribute to the provision of these public goods in each country where their products are used by investing in secure SDLCs. Indeed, this specifically rebuts the argument against the Pledge from section 3.B.2., namely that it weaponises the software dependencies of countries outside the Quad on vendors and other key members of global software supply chains that are based in the Quad countries or (want to) count any of the Quad governments as customers.

These points are reinforced by the broader intent of the Quad governments when it comes to delivering on their agenda for the Indo-Pacific:

---

[164] Ibid; European Commission, *Impact Assessment*, 9-10.

[165] National Research Council, *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy* (Washington, DC: The National Academies Press, 2010) 3, 4, 7; European Commission, *Impact Assessment*, 17.

[166] Quad Senior Cyber Group, *Joint Principles for Secure Software*, 2.

[167] L. Solum, ‘Legal Theory Lexicon: Public and Private Goods’, *Legal Theory Blog* [blog post] (19 Jun. 2016), https://lsolum.typepad.com/legaltheory/2016/06/legal-theory-lexicon-public-and-private-goods.html, accessed 2 Mar. 2023 cited in Chung, *Market Failure*, 454-5.

[168] C. Martin, 'Cyber "Deterrence": A Brexit Analogy', *Lawfare* (15 Jan. 2021), paras. 10, 20, https://www.lawfareblog.com/cyber-deterrence-brexit-analogy, accessed 1 Mar. 2023.

[169] R.D. Adams & K. McCormick, ‘Private Goods, Club Goods, and Public Goods as a Continuum’, *Review of Social Economy*, 45/2 (1987), 194.

> … we are determined to make a positive and lasting contribution to the resilience and prosperity of the Indo-Pacific…
>
> We will work transparently and in open dialogue to implement a practical agenda that delivers sustained economic and social value, is responsive to regional partners, and contributes to global priorities by advancing the United Nations' 2030 Agenda for Sustainable Development and its Sustainable Development Goals, noting the transformational power of technology to help meet these goals.[170]

These extracts from the May 2023 vision statement of the Quad Leaders reinforce the intent of the Quad as being a vehicle to deliver public goods in the region. Rather than weaponise their capabilities, the Quad countries are seeking to assure the region's actual resilience and economic development through driving the implementation of best practice in secure software development as recommended by NIST, as above. This is the background of the Pledge, rather than some design by the governments to securitise technology supply chains or 'play politics', directly rebutting the potential contentions of critics of the Pledge in sections 3.B.2. and 3.B.3.

3.C.3. Upholding Multi-Stakeholderism in Technology Governance

The allegation that the Pledge runs contrary to the Quad countries' preference for multi-stakeholderism in technology governance ignores the nature of the Pledge. Far from championing a state-centric approach, the Quad governments value engagement with domestic industry stakeholders as 'an essential element of' the Pledge.[171] They have committed to 'engage with the software industry to promote these practices', rebutting the narrative about the Pledge apparently bypassing industry stakeholders.[172] This is accentuated by the Pledge operating alongside the Quad Senior Cyber Group which coordinates public-private engagement on cyber resilience standards and secure software development.[173] One should also note the Quad's wanting to '[s]upport industry led, consensus-based multi-stakeholder approaches to the development of technology standards'.[174]

---

[170] A. Albanese et al., *Quad Leaders' Vision Statement – Enduring Partners for the Indo-Pacific* [media release] (20 May 2023), paras. 3, 9, https://www.whitehouse.gov/briefing-room/statements-releases/2023/05/20/quad-leaders-vision-statement-enduring-partners-for-the-indo-pacific/, accessed 20 May 2023.

[171] Commonwealth of Australia et al., *Joint Cybersecurity Principles*, para. 7.

[172] Quad Senior Cyber Group, *Joint Principles for Secure Software*, 2.

[173] The White House, *Fact Sheet: Quad Leaders' Summit*, para. 22.

[174] Quad Critical and Emerging Technology (CET) Working Group, *CET Standards*, 1.

The Pledge also reflects the four countries' stated commitment to multi-stakeholderism in their cyber diplomacy.[175] This is evident both in their strategies and the capacity building work they perform.

The United States' 'International Cyberspace Policy' commits it to promote multi-stakeholderism in Internet governance.[176] Australia's *International Cyber and Critical Technology Engagement Strategy* commits it to oppose a state-centric approach to Internet governance and enable all stakeholders to participate in multi-stakeholder Internet governance fora.[177] India's cyber diplomacy is defined by 'commitment to a multi-stakeholder model of cyber governance'.[178] Japan's *Cybersecurity Strategy* tasks the Japanese government to coordinate and collaborate with all stakeholders in its cyber diplomacy.[179]

Similarly, the championing of the multi-stakeholder approach by the Quad countries is evident in their involving the private sector in their capacity building efforts. For instance, major cyber resilience vendors participate in Australia's Cyber and Critical Tech Cooperation Program which invests (as at January 2023) over $100 million in delivering over 100 capacity building projects in the Indo-Pacific.[180] In the Ukraine war, the American government has closely worked with American technology companies to assure the protection of Ukrainian digital infrastructure.[181] It

[175] Ministry of External Affairs (India), *Annual Report 2022*, 270; Department of Foreign Affairs and Trade (Commonwealth of Australia), *Australia's International Cyber and Critical Technology Engagement Strategy*, 11; *National Defense Authorization Act for Fiscal Year 2023* (USA), ss. 9501(a)(1), 9502(a); The Government of Japan, *Cybersecurity Strategy,* 5-6, 13.

[176] *National Defense Authorization Act for Fiscal Year 2023* (USA), s. 9501(a).

[177] Department of Foreign Affairs and Trade (Commonwealth of Australia), *Australia's International Cyber and Critical Technology Engagement Strategy*, 64, 82.

[178] Ministry of External Affairs (India), *Annual Report 2022*, 270.

[179] *The Basic Act on Cybersecurity 2014* (Japan)*,* arts. 3(1)-(2) cited in The Government of Japan, *Cybersecurity Strategy,* 5.

[180] Department of Foreign Affairs and Trade (Commonwealth of Australia), 'Meet our CCTCP Partners', *Australia's International Cyber and Critical Tech Engagement* (5 Nov. 2022), para. 1, https://www.internationalcybertech.gov.au/our-work/capacity building/meet-our-CCTCP-partners, accessed 1 Mar. 2023; T. Feakin, 'After six incredible years of being Australia's first Ambassador for Cyber Affairs and Critical Technology…' [LinkedIn post] (Jan. 2023), https://www.linkedin.com/posts/tobias-feakin-1102255_aftersix-incredible-years-of-being-australias-activity-7025926440000884737-pvPW/, accessed 28 February 2023.

[181] See, eg, N. Beecroft, 'Evaluating the International Support to Ukrainian Cyber Defense', *Carnegie Endowment for International Peace* (3 Nov. 2022), 3-6, https://carnegieendowment.org/2022/11/03/evaluating-international-support-to-ukrainian-cyber-defense-pub-88322. Accessed 2 Mar. 2023.

has funded American firms' provision of digital services to Ukraine.[182] Indeed, the value of this embrace of multi-stakeholderism is in how private firms run global technology supply chains and/or critical infrastructure assets, and have tremendous first-hand visibility of the threat landscape, vital to uplifting national cyber resilience.[183]

3.C.4. Upholding Multilateralism in Technology Governance

The Pledge seeks to improve the security and resilience of technology supply chains, given the criticality of software to all technology, as flagged above. Therefore, the Pledge implements one of the norms for responsible state conduct in cyberspace that the UN General Assembly ('UNGA') approved by consensus in 2015 ('UNGA norms'): 'States should take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products'.[184] To operationalise this, countries were recommended to: develop 'policies and programmes to objectively promote the adoption of good practices by suppliers and vendors of ICT equipment and systems…'; and require 'ICT vendors to incorporate safety and security in the design, development and throughout the lifecycle of ICT products'.[185] The Pledge, including the suggested standards from the *Joint Principles,*[186] echoes the stated UNGA norm and these recommendations. Translating norms and recommendations endorsed by a multilateral body into national laws and policy frameworks is accepted state practice. The Quad, through the Pledge, is thus championing multilateralism. This rebuts the aforementioned narrative against the Pledge as an example of the Quad's disregarding multilateralism in technology governance.

---

[182] Ibid; Office of Press Relations (United States), *USAID Announces up to $60 Million to Bolster Ukraine's Cybersecurity* [media release] (10 Feb. 2023), https://www.usaid.gov/news-information/press-releases/feb-10-2023-usaid-announces-60-million-bolster-ukraines-cybersecurity, accessed 1 Mar. 2023; United States Agency for International Development, 'Cybersecurity', *United States Agency for International Development* (May 2022), https://www.usaid.gov/sites/default/files/2023-01/Cybersecurity_eng.pdf, accessed 2 Mar. 2023.

[183] See, eg, United States Government Accountability Office, 'Agencies Are Taking Steps to Expand Diplomatic Engagement and Coordinate with International Partners', *United States Government Accountability Office* (Washington, DC, 2 Feb. 2023), 18, https://www.gao.gov/assets/gao-23-105534.pdf, accessed 2 Mar. 2023; Beecroft, *Ukrainian Cyber Defense*, 3-6; E. Schroeder & S. Dack, 'A Parallel Terrain: Public-Private Defense of the Ukrainian Information Environment', *Atlantic Council* (Washington, DC, 27 Feb. 2023), 13-15, https://www.atlanticcouncil.org/wp-content/uploads/2023/02/A-Parallel-Terrain.pdf, accessed 2 Mar. 2023; J. Slowik, 'What Have We Learned?', *Stranded on Pylos* (16 Feb. 2023), paras. 16-19, https://pylos.co/2023/02/16/what-have-we-learned/, accessed 2 Mar. 2023; Ebrahim, *National Cybersecurity Innovation*, 492-3.

[184] UNGA, *Report of the Group of Governmental Experts*, 8, 14.

[185] Ibid, 14-15.

[186] Commonwealth of Australia et al., *Joint Principles*, para. 6.

Furthermore, the text of the *Joint Principles for Secure Software* makes the Quad's upholding of multilateralism in technology governance quite clear. The Pledge is made conditional on each Quad country's policies being 'consistent with international obligations'.[187] The four governments expressly 'encourage other nations to adopt these principles in pursuit of this shared vision for secure software'.[188] This is within the context of the Quad committing to: 'acknowledge and respect the centrality, agency, and leadership of regional institutions [in the Indo-Pacific]'; and 'work in and alongside them to complement their efforts and advance our shared interests'.[189] Therefore, it is unclear how critics can point to the Pledge as threatening the multilateral rules-based order or extant regional architectures. The Quad itself is calling for other countries to join its work by implementing the *Joint Principles for Secure Software*, providing a template for them to follow in their development, procurement and use of software — hardly the mark of a grouping which opposes multilateralism.

The above four points of rebuttal to a potential narrative against the Pledge reinforce its criticality as a means to uplift software security more generally and thus implement the Quad's agenda, namely the 'address[ing of] shared [security] challenges, including in cyber space'.[190]

4. Driving the Quad's Internal Credibility

Building on the critical analysis from Section 3 of the policy merits of the Pledge, this paper will now explain how it is core to the fulfilment of the Quad's agenda with reference to how it drives the Quad's internal credibility.

From the outset, it should be highlighted that the close working relationship required for regulatory coordination under the Pledge will be aided by the work of the Quad Senior Cyber Group ('QSCG'), the author of the *Joint Principles for Secure Software*. The QSCG is a forum for 'Leader-level experts' to coordinate efforts across the public and private sectors on matters including cyber resilience standards, secure software development, and 'secure and trustworthy digital infrastructure'.[191] As at the writing of this paper, the QSCG Principals have met twice: once

[187] Quad Senior Cyber Group, *Joint Principles for Secure Software*, 2.

[188] Ibid.

[189] Albanese et al., *Quad Leaders' Vision Statement*, para. 8.

[190] Biden et al., *The Spirit of the Quad*, para. 3.

[191] The White House, *Fact Sheet: Quad Leaders' Summit*, para. 22.

in Sydney in 2022 and once in New Delhi in 2023.[192] In providing a mechanism by which the most senior cyber resilience officials from each country work together and with industry stakeholders, the QSCG enables the reliable implementation of the agenda of the QCP generally, including the Pledge (because industry itself will have to comply with any new procurement regulations).[193] This is reinforced by how, in the *Joint Principles for Secure Software*, the QSCG itself 'reaffirms our [its] commitment to collectively improve software security' through measures including the Pledge.[194] These factors will make the four governments even more invested in the Pledge and thus working together to uplift software security.

In addition to the QSCG providing a bureaucratic structure to help guide these efforts, there are three reasons why the Pledge encourages the internal credibility of the Quad: the criticality of secure software to all economies; existing work by the Quad governments to uplift software security and cyber resilience generally; and regulatory coordination on the Pledge more broadly strengthening trust within the Quad.

4.A. The Criticality of Secure Software

The criticality of secure software to any economy (as detailed in sections 3.A.1. and 3.C.1.) assures the investment of each Quad member in implementing the Pledge. The countries already have stated their intent to make technology supply chains servicing their critical infrastructure assets securer.[195] The clear link between the cyber resilience of critical infrastructure assets and national security (as detailed in section 3.C.1.) reinforces that intent. Indeed, the clear national security relevance of secure software, and thus the Pledge itself, mitigates risks of disagreements on separate issues creating internal conflict in the Quad; issues such as the regulation of cross-border data flows, privacy, taxation and online safety.[196] These factors mean that the Quad will most likely coalesce around the Pledge.

---

[192] Commonwealth of Australia et al., *Quad Senior Cyber Group – Joint Statement* [media release] (28 Mar. 2022), https://www.homeaffairs.gov.au/news-media/archive/article?itemId=869, accessed 1 Mar. 2023; Department of Home Affairs, *Quad Senior Cyber Group Meets in New Delhi* [media release] (1 Feb. 2023), https://www.homeaffairs.gov.au/news-media/archive/article?itemId=1015, accessed 2 Mar. 2023.

[193] Commonwealth of Australia et al., *Joint Cybersecurity Principles*, para. 7; Quad Senior Cyber Group, *Joint Principles for Secure Software*, 2.

[194] Quad Senior Cyber Group, *Joint Principles for Secure Software*, 2.

[195] Biden et al., *The Spirit of the Quad*, para. 3.

[196] T. Scholz, 'Quad Vadis? A Risk Assessment of the Quad's Emerging Cybersecurity Partnership', *Observer Research Foundation* (New Delhi, 30 Nov. 2022), 11, https://www.orfonline.org/wp-content/uploads/2022/11/ORF_IssueBrief_592_Quad-Cybersecurity.pdf, accessed 2 Mar. 2023.

4.B. Existing Work by the Governments

The Pledge also drives the Quad's internal credibility because the four governments have passed laws and/or created policies that seek to uplift software security and cyber resilience generally. The Pledge thus leverages their individual political wills.

In the United States, the President's executive order on cybersecurity devoted a section to seeking to 'rapidly improve the security and integrity of the software supply chain, with a priority on addressing critical software', including through procurement regulations.[197] The National Institute of Standards and Technology ('NIST') defined, and recommended security measures to be used when deploying, critical software — measures that can be applied in relation to software generally.[198] NIST also released guidance on secure software development and software supply chain risk management, with all federal government agencies required to comply with that guidance.[199] More generally, the United States seeks to 'shift liability for insecure software products and services' to negligent software vendors.[200] It also is moving to work with allies and partners to secure international technology supply chains under its national strategy for cybersecurity.[201]

In Australia, 'protective cyber security technologies', which would include systems designed to improve software supply chain security, are classified as 'critical technologies in the national

[197] Exec. Order No. 14,028, 86 Fed. Reg. 26,633, 26,637-41 (17 May 2021).

[198] National Institute of Standards and Technology, 'Definition of Critical Software under Executive Order (EO) 14028', *National Institute of Standards and Technology* (United States, 13 Oct. 2021), https://www.nist.gov/system/files/documents/2021/10/13/EO Critical FINAL.pdf, accessed 1 Mar. 2023; National Institute for Science and Technology, 'Security Measures for "EO-Critical Software" Use under Executive Order (EO) 14028', *National Institute for Science and Technology* (United States, 9 Jul. 2021), https://www.nist.gov/system/files/documents/2021/07/09/Critical Software Use Security Measures Guidance.pdf, accessed 2 Mar. 2023.

[199] Souppaya, Scarfone & Dodson, *SSDF*, 1; National Institute of Standards and Technology, 'Software Supply Chain Security Guidance under Executive Order (EO) 14028 Section 4e', *National Institute of Standards and Technology* (United States, 4 Feb. 2022), https://www.nist.gov/system/files/documents/2022/02/04/software-supply-chain-security-guidance-under-EO-14028-section-4e.pdf, accessed 2 Mar. 2023; Director of the Office of Management and Budget (United States), 'Enhancing the Security of the Software Supply Chain through Secure Software Development Practices', *The White House* (Washington, DC, 14 September 2022), 1, https://www.whitehouse.gov/wp-content/uploads/2022/09/M-22-18.pdf, accessed 2 Mar. 2023.

[200] The White House, *National Cybersecurity Strategy*, 20-1.

[201] Ibid, 32.

interest'.[202] In early 2023, Australia enacted supply chain risk management obligations for critical infrastructure asset operators.[203]

Japan's *Cybersecurity Strategy* commits its government to 'promote efforts to develop and implement concrete security measures' for technology supply chain risk management by industry.[204] The government will also work towards (software) supply chain reliability and the development of a software verification system.[205] Japan's 2022 national security strategy similarly plans to improve the cyber resilience of government computer networks 'throughout the[ir] lifecycle', which would include software supply chain risk management.[206]

India's *2013 Policy* calls for mandating secure software development practices.[207] Linked with this, it requires the Indian government to: create facilities to test the cyber resilience of digital products; build 'trusted relationships' with vendors; and raise awareness of supply chain risks.[208]

Therefore, the Pledge drives the Quad's internal credibility because it leverages each government's political will and work at home to uplift software security. When combined with their commitment to bolster and coordinate these domestic efforts under the *Joint Principles for Secure Software*,[209] the incentives for the four governments to engage on other (cyber policy) issues through the Quad are indeed substantial.

What particularly augments the Pledge is how the QCP builds on the four governments' work at home for cyber resilience more generally. Cooperating in the QCP would be a natural extension of these initiatives — those described above for software security implement the software security pillar of the QCP. This is also evident with respect to the other three pillars of the QCP.

---

[202] Department of Industry, Science and Resources, 'Advanced Information and Communication Technologies', Department of Industry, Science and Resources (19 May 2023), paras. 1, 6, 12, https://www.industry.gov.au/publications/list-critical-technologies-national-interest/advanced-information-and-communication-technologies, accessed 19 May 2023.

[203] *Security of Critical Infrastructure (Critical Infrastructure Risk Management Program) Rules (LIN 23/006) 2023* (Australia) rr. 4, 8, 10.

[204] The Government of Japan, *Cybersecurity Strategy*, 23.

[205] Ibid, 23, 43.

[206] Ministry of Defense (Japan), *National Security Strategy*, 23.

[207] Ministry of Electronics and Information Technology (India), *2013 Policy*, 7.

[208] Ibid, 8.

[209] Quad Senior Cyber Group, *Joint Principles for Secure Software*, 2.

In terms of the critical infrastructure protection pillar, Australia and the United States reformed their national legislative frameworks for critical infrastructure protection in 2021 and 2022.[210] Japan's *Basic Act* commits the government to bolster critical infrastructure cyber resilience, including through capacity building and information sharing.[211] Japan's *National Security Strategy* from 2022 called for 'response capabilities' that are at least equal to Western capabilities to protect critical infrastructure assets.[212] India's 2013 policy on cyber security devotes a section to critical infrastructure protection, including measures similar to those enacted or proposed by its Quad partners.[213]

Cooperation on the supply chain resilience and security pillar is also grounded in common policy approaches, as seen in how the four governments have handled security risks from Huawei and ZTE. The Quad countries banned, whether specifically or implicitly, those vendors from their (5G) telecommunications networks and/or government procurement contracts.[214] Each government was motivated by, essentially, the same risk factors, such as these vendors': close association with the Chinese state; legal obligations to cooperate with Chinese intelligence agencies; and flawed equipment designs.[215] The governments' policy alignment on this point is crucial to the Quad's internal credibility, given the value of consensus on tackling serious cyber supply chain hazards to their critical infrastructure assets. Their shared approach is reinforced by the objective reality of

[210] See, eg, *Security Legislation Amendment (Critical Infrastructure) Act 2021* (Australia); *Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022* (Australia); *Cyber Incident Reporting for Critical Infrastructure Act of 2022*, 6 USC ss. 681-681g (2022).

[211] *The Basic Act on Cybersecurity 2014* (Japan)*,* art. 14.

[212] Ministry of Defense (Japan), *National Security Strategy*, 23; The Government of Japan, *Cybersecurity Strategy,* 30-1.

[213] Ministry of Electronics and Information Technology (India), *2013 Policy*, 7.

[214] 15 USC s. 1602; 47 USC s. 1603; 47 CFR ss. 1.5000, 2.903(a), 2.906(d), 2.907(c), 54.9(a), (d); Public Safety and Homeland Security Bureau, *List of Equipment*; Department of Telecommunications, *Amendment to the UASL*; Uren and Cave, *Australia Banned Huawei*, para. 9; Reuters, *Japan to Ban Huawei, ZTE*.

[215] See, eg, Federal Communications Commission (United States), 'Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs; Huawei Designation; ZTE Designation', *Federal Register* (Washington, DC, 3 Jan. 2020), 231, 234, https://www.govinfo.gov/content/pkg/FR-2020-01-03/pdf/2019-27610.pdf, accessed 2 Mar. 2023; Huawei Cyber Security Evaluation Centre Oversight Board (United Kingdom), 'Annual Report 2021: A Report to the National Security Adviser of the United Kingdom', *GOV.UK* (London, 20 Jul. 2021), para. 1.9, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1004291/2021_HCSEC_OB_REPORT_FINAL__1_.pdf, accessed 2 Mar. 2023; Huawei Cyber Security Evaluation Centre Oversight Board (United Kingdom), 'Annual Report 2019: A Report to the National Security Adviser of the United Kingdom', *GOV.UK* (London, 28 Mar. 2019), paras. 5.ii.-5.vii., https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/790270/HCSEC_OversightBoardReport-2019.pdf, accessed 2 Mar. 2023.

said risk factors in relation to Huawei and ZTE,[216] rather than an ideologically-driven securitisation of technology supply chains — rebutting the argument of critics of the Pledge flagged in section 3.B.3. This was backed implicitly by the G7 Leaders in May 2023 when they committed their governments to '[cooperate] on enhancing security and resiliency in critical infrastructure particularly in the digital domain', and 'reaffirm[ed] the need to assess political, economic, and other risks of a non-technical nature posed by vendors and suppliers'.[217] After all, these risks echo the risk factors identified above as motivating the Quad governments' decisions to ban Huawei and ZTE.

To return to the Pledge itself, the Quad governments' approach neither seems even remotely ideological nor seeking to weaponise or securitise anything. The specific software development practices and qualities of software that the governments will target in their procurement decisions mimic the best practice recommendations of NIST that were developed with the input of a range of key software sector stakeholders.[218] Furthermore, the *Joint Principles for Secure Software* are vendor-agnostic, positioning the security of vendors' SDLCs as a screening mechanism for government procurement, not their nationality.

Cooperation under the QCP on workforce development and talent is enabled by a shared appreciation of the criticality of people who are trained in the operational and policy dimensions of cyber resilience to thriving digital economies.[219] This can be seen in commonalities between the Quad countries' national strategies for cyber resilience, with each devoting sections and/or objectives towards upskilling in cyber resilience, funding training programs and more generally helping match demand for expertise in cyber resilience with supply.[220]

In this vein, the Pledge's contribution to the internal credibility for the Quad will be accentuated by the four countries' operationalisation of the QCP. Based on their existing initiatives at home, the Quad members share an intent and, broadly speaking, approaches to uplift cyber resilience generally, just like they do with software security under the Pledge. The Pledge and QCP thus represent a convergence of interests (such as security interests), as well as intent and modes to

[216] Ibid.

[217] Biden et al., *Economic Resilience and Economic Security*, para. 3.

[218] Souppaya, Scarfone & Dodson, *SSDF*, iii.

[219] See, eg, Australian Government, *Cyber Security Strategy 2020*, 32.

[220] Ibid, 32-3; The White House, *National Cybersecurity Strategy*, 26; Government of Japan, *Cybersecurity Strategy*, 46-8; Ministry of Electronics and Information Technology (India), *2013 Policy*, 4, 8.

advance those interests. This feeds into the third reason for the Pledge as a driver of the Quad's internal credibility.

4.C. Regulatory Coordination as a Driver of Trust

Regulatory coordination can strengthen mutual trust because it reflects the aforementioned convergences. This has an even stronger effect through the Pledge and the QCP: regulatory harmonisation is diplomacy by another means, especially when the regulatory frameworks directly concern cyber resilience, a matter critical to national security, as flagged in section 3.C.2.

Working together to make software security standards under procurement regulations more robust can particularly boost engagement and trust in the Quad. Given that these regimes govern the choice and management of the very systems that keep the four governments' departments and agencies operational, the Pledge will assure the governments' operational resilience and the availability of the critical services they provide to their citizens. This will deepen the level of trust the governments have in each other and their advice on how to assure their own cyber resilience. After all, in implementing the Pledge, the four governments will be using the same standards for software security to improve their collective cyber resilience. Since the governments are designing these standards together, the Pledge is both a symbol and an enabler of mutual trust within the Quad.

Harmonising procurement regulations will also make it easier for software vendors to compete for the Quad governments' business, helping grow economic and digital linkages within the Quad. In fact, since vendors wanting to sell to any of the four governments would have to demonstrate compliance with the same set of robust software security standards, this makes it easier for the four governments to trust each other's software procurement decisions and thus work even more closely together. That trust would particularly be strengthened if the four governments patronised vendors headquartered in each other's jurisdictions and vetted by each other's agencies, given the governments' shared approach to software security as well as technology development, design, governance and use; building on principles that they endorsed in September 2021.[221] For instance, if the Australian, Indian and Japanese governments deepened their procurement

[221] Commonwealth of Australia et al., *Quad Principles on Technology Design, Development, Governance, and Use* [media release] (24 Sep. 2021), https://www.whitehouse.gov/briefing-room/statements-releases/2021/09/24/quad-principles-on-technology-design-development-governance-and-use/, accessed 2 Mar. 2023.

relationships with the American software sector — already key to the United States' technological dominance — this would strengthen their relationships with the United States.[222]

5. Conclusion

This working paper explored a particular aspect of the Quad's agenda: a pledge by the four governments under the QCP to align their development of software security standards as part of their procurement regulations. It situated the Pledge within the context of the cyber diplomacy by the individual members of the Quad, defining the bureaucracy carrying out that diplomacy, the strategies guiding it and the initiatives that the Quad countries undertake as part of it. The paper then juxtaposed those initiatives with the escalation of the threat landscape. Though it is difficult to attribute the growth in cyber attacks to the apparent ineffectiveness of cyber diplomacy, it was highlighted that the latter has not paid sufficient attention to a large source of the problem: insecure software. The need for governments to work together to uplift software security was thus defined.

In this vein, the Pledge, being targeted at uplifting software security, was presented as the way forward for cyber diplomacy by the Quad countries. Its nature as core to the Quad's agenda, especially its mission to deal with cyber-enabled threats to (inter)national security, was critically analysed. The importance of the Pledge was pointed to with reference to the inherent dependence of societies and economies on secure software in order to function, the worsening threat landscape for software supply chains and the suboptimal state of software security. A potential narrative against the Pledge was analysed, namely the arguments that the Pledge: runs contrary to multilateralism and multi-stakeholderism in technology governance; weaponises software dependencies of non-Quad countries on technology vendors headquartered in the Quad countries and/or wanting to sell their products to the four governments; and is focused on securitising technology supply chains for the benefit of the Quad countries. This narrative was rebutted by arguing that the Pledge: yields positive externalities for all software users (not just the Quad governments); drives the delivery of public goods, namely software security, national cyber resilience and national security around the world (directly contradicting the arguments of critics that the Pledge weaponises software dependencies of non-Quad countries and securitises technology supply chains to benefit the Quad countries); upholds multi-stakeholderism in technology governance because of the Pledge being implemented in collaboration with the private sector; and

[222] U.S. Department of Commerce & U.S. Department of Homeland Security, *Assessment*, 35; Schroeder & Dack, *A Parallel* Terrain, 13-15; Beecroft, *International Support to Ukrainian Cyber Defense*, 3-6.

upholds multilateralism in technology governance by implementing the UNGA norm and associated recommendations for bolstering the integrity of technology supply chains.

Having demonstrated the criticality of the Pledge as a tool to uplift software security and fulfil the Quad's commitment to 'address shared [security] challenges, including in cyber space',[223] this working paper built on that analysis by showing how the Pledge will drive the Quad's internal credibility and thus why it is key to the fulfilment of the Quad's agenda. It did so with reference to three factors: the criticality of software security to the national security of the four Quad members; the Pledge building on existing work by the Quad governments to uplift software security and cyber resilience generally; and the nature of regulatory coordination under the Pledge as a driver of trust among the Quad countries.

In terms of the way forward, one should note that the benefits of the Pledge are easily transferable outside the Quad as part of the four governments' cyber diplomacy in the Indo-Pacific and indeed the world at large. This is for two reasons.

The first is, as flagged in section 3.C.1., the sheer collective purchasing power of the Quad governments — especially through the American government — and the dominance of American vendors in global software markets. If those vendors bolster the security of their SDLCs in order to be able to sell to the Quad governments, all of their users (a substantial number worldwide) will benefit from the greater security of their products, not just the Quad governments.

Secondly, the underlying software security standards that the Quad countries will develop and insert into their procurement regulations — that would be made public — can be adopted by any government or indeed any vendor looking for guidance on how to invest in a secure SDLC. This will enable effective capacity building by the Quad of countries with not as developed approaches to cyber resilience; not least since such efforts would be targeted at a major source of their attack surface, namely insecure software. The Quad's approach to directly bolstering software security can thus spread across the world with said standards as a template for others to follow. Indeed, the Quad has defined the *Joint Principles for Secure Software* as one, calling on other countries to 'adopt these principles in pursuit of this shared vision for secure software'.[224] In this fashion, the Pledge will help position the Quad as a positive force for encouraging the cyber resilience of societies and economies.

[223] Biden et al., *The Spirit of the Quad*, para. 3.

[224] Quad Senior Cyber Group, *Joint Principles for Secure Software*, 2.

After all, the Pledge is carved out of the criticality of software security to the very existence of societies and economies.

And so, the Pledge carves the Quad in code.

6. References

15 USC s. 1602.

47 CFR ss. 1.5000, 2.903(a), 2.906(d), 2.907(c), 54.9(a), (d).

47 USC s. 1603.

Adams, R.D. & McCormick, K., 'Private Goods, Club Goods, and Public Goods as a Continuum', *Review of Social Economy*, 45/2 (1987), 192-199.

Agence Nationale de la Sécurité des Systèmes d'Information, 'Cyber Threat Overview 2022', *Agence Nationale de la Sécurité des Systèmes d'Information* (Paris, 15 Jan. 2023), https://www.cert.ssi.gouv.fr/uploads/CERTFR-2023-CTI-002.pdf, accessed 1 Mar. 2023.

Albanese, A. et al., *Quad Joint Leaders' Statement* [media release] (24 May 2022), https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/24/quad-joint-leaders-statement/, accessed 9 Mar. 2023.

Albanese, A. et al., *Quad Leaders' Vision Statement – Enduring Partners for the Indo-Pacific* [media release] (20 May 2023), https://www.whitehouse.gov/briefing-room/statements-releases/2023/05/20/quad-leaders-vision-statement-enduring-partners-for-the-indo-pacific/, accessed 20 May 2023.

Alderfer, R. et al. (United States), 'Report on Recommended Best Practices to Improve Communications Supply Chain Security', *Federal Communications Commission* (Washington, DC, Sep. 2022), https://www.fcc.gov/file/23839/download, accessed 1 Mar. 2023.

ANI, 'India Becomes 5th Largest Economy in World: A Perspective', *ANI* (17 Sep. 2022), https://www.aninews.in/news/world/asia/india-becomes-5th-largest-economy-in-world-a-perspective20220917025023/, accessed 1 Mar. 2023.

AP News, 'Guadeloupe Government "Large-Scale" Cyberattack', *AP News* (23 Nov. 2022), https://apnews.com/article/caribbean-puerto-rico-guadeloupe-government-and-politics-0e299e596db2ba25971c947a8f831a61, accessed 5 Mar. 2023.

Attrey, A. et al., 'Digital Enablers of the Global Economy: Background Paper for the CDEP Ministerial Meeting', *OECD* (Paris, 15 Nov. 2022), https://read.oecd.org/10.1787/f0a7baaf-en?format=pdf, accessed 13 Mar. 2023.

Australian Cyber Security Centre, 'ACSC Annual Cyber Threat Report 2021-22', *Australian Cyber Security Centre* (Canberra, 4 Nov. 2022), https://www.cyber.gov.au/sites/default/files/2022-11/ACSC-Annual-Cyber-Threat-Report-2022.pdf, accessed 5 Mar. 2023.

Australian Securities and Investments Commission, 'Report 429: Cyber Resilience: Health Check', *Australian Securities and Investments Commission* (Canberra, 19 Mar. 2015), https://download.asic.gov.au/media/3062900/rep429-published-19-march-2015-1.pdf, accessed 28 Feb. 2023.

Bajak, F., 'How the Kremlin Provides a Safe Harbor for Ransomware', *Associated Press News* (17 Apr. 2021), https://apnews.com/article/business-technology-general-news-government-and-politics-c9dab7eb3841be45dff2d93ed3102999, accessed 2 Mar. 2023.

Barnes, D.A., 'Deworming the Internet', *Texas Law Review*, 83/1 (2004), 279-330.

Bateman, J., 'The Antitrust Threat to National Security', *Carnegie Endowment for International Peace* (22 Oct. 2019), https://carnegieendowment.org/2019/10/22/antitrust-threat-to-national-security-pub-80404, accessed 5 Mar. 2023.

Beaumont, K., 'Kaseya Supply Chain Attack Delivers Mass Ransomware Event to US Companies', *DoublePulsar* [blog post] (3 Jul. 2021), https://doublepulsar.com/kaseya-supply-chain-attack-delivers-mass-ransomware-event-to-us-companies-76e4ec6ec64b, accessed 11 Mar. 2023.

Beecroft, N., 'Evaluating the International Support to Ukrainian Cyber Defense', *Carnegie Endowment for International Peace* (3 Nov. 2022), https://carnegieendowment.org/2022/11/03/evaluating-international-support-to-ukrainian-cyber-defense-pub-88322. Accessed 2 Mar. 2023.

Bernat, L., 'Enhancing the Digital Security of Critical Activities', *OECD* (Paris, 31 Aug. 2021), https://goingdigital.oecd.org/data/notes/No17_ToolkitNote_DigitalSecurity.pdf, accessed 13 Mar. 2023.

Better Cybercrime Metrics Act 2022 (USA).

Biden, J.R. et al., *Quad Leaders' Joint Statement: "The Spirit of the Quad"* [media release] (12 Mar. 2021), https://www.whitehouse.gov/briefing-room/statements-releases/2021/03/12/quad-leaders-joint-statement-the-spirit-of-the-quad/, accessed 10 Mar. 2023.

Biden, J. R. et al., *G7 Hiroshima Leaders' Communiqué* [media release] (20 May 2023), https://www.whitehouse.gov/briefing-room/statements-releases/2023/05/20/g7-hiroshima-leaders-communique/, accessed 20 May 2023.

Biden, J. R. et al., *G7 Leaders' Statement on Economic Resilience and Economic Security* [media release] (20 May 2023), https://www.whitehouse.gov/briefing-room/statements-releases/2023/05/20/g7-leaders-statement-on-economic-resilience-and-economic-security/, accessed 20 May 2023.

Buzan, B., Waever, O. & de Wilde, J., *Security: A New Framework for Analysis* (London: Lynne Rienner Publishers, 1998).

Chirgwin, R., 'Australia's First Cyber Ambassador Moves on', *iTnews* (31 Jan. 2023), https://www.itnews.com.au/news/australias-first-cyber-ambassador-moves-on-590318, accessed 1 Mar. 2023.

Chong, J., 'Bad Code: The Whole Series', *Lawfare* (4 Nov. 2013), https://www.lawfareblog.com/bad-code-whole-series, accessed 3 Mar. 2023.

Chung, J.J., 'Critical Infrastructure, Cybersecurity, and Market Failure', *Oregon Law Review*, 96(2) (2018), 442-476.

Cimpanu, C., 'Cyberattack Brings down Vodafone Portugal Mobile, Voice, and TV Services', *The Record* (8 Feb. 2022), https://therecord.media/cyberattack-brings-down-vodafone-portugal-mobile-voice-and-tv-services/, accessed 4 Mar. 2023.

Clancy, C. et al., 'Deliver Uncompromised: Securing Critical Software Supply Chains', *MITRE* (United States, 29 Jan. 2021), https://www.mitre.org/sites/default/files/2021-11/prs-21-0278-deliver-uncompromised-securing-critical-software-supply-chain.pdf, accessed 2 Mar. 2023.

Commonwealth of Australia et al., *Quad Principles on Technology Design, Development, Governance, and Use* [media release] (24 Sep. 2021), https://www.whitehouse.gov/briefing-room/statements-releases/2021/09/24/quad-principles-on-technology-design-development-governance-and-use/, accessed 2 Mar. 2023.

Commonwealth of Australia et al., *Quad Senior Cyber Group – Joint Statement* [media release] (28 Mar. 2022), https://www.homeaffairs.gov.au/news-media/archive/article?itemId=869, accessed 1 Mar. 2023.

Commonwealth of Australia et al., 'Quad Cybersecurity Partnership: Joint Principles', *Department of Home Affairs* (Canberra, 24 May 2022), https://www.homeaffairs.gov.au/cyber-security-subsite/files/qscg-joint-principles.pdf, accessed 2 Mar. 2023.

Coyne, C.J. & Leeson, P.T., 'Who's to Protect Cyberspace', *Journal of Law, Economics and Policy*, 1/2 (2005), 473-496.

Critical Technologies Policy Coordination Office (Commonwealth of Australia), 'The Action Plan for Critical Technologies', *Department of Industry, Science and Resources* (Canberra, 17 Nov. 2021), https://www.industry.gov.au/sites/default/files/2022-08/ctpco-action-plan-critical-technology.pdf, accessed 2 Mar. 2023.

Cyber Incident Reporting for Critical Infrastructure Act of 2022, 6 USC ss. 681-681g (2022).

Cyber Safety Review Board (United States), 'Review of the December 2021 Log4j Event', *Cybersecurity and Infrastructure Security Agency* (Washington, DC, 11 Jul. 2022), https://www.cisa.gov/sites/default/files/publications/CSRB-Report-on-Log4-July-11-2022_508.pdf, accessed 12 Mar. 2023.

Cybersecurity and Infrastructure Security Agency Information and Communications Technology Supply Chain Risk Management Task Force, 'Information and Communications Technology Supply Chain Risk Management Task Force Year 2 Report: Status Update on Activities and Objectives of the Task Force', (Washington, DC, 17 Dec. 2020), https://www.cisa.gov/sites/default/files/publications/ict-scrm-task-force_year-two-report_508.pdf, accessed 3 Mar. 2023.

Cybersecurity and Infrastructure Security Agency, 'Defending against Software Supply Chain Attacks', *Cybersecurity and Infrastructure Security Agency* (26 Apr. 2021), https://www.cisa.gov/sites/default/files/publications/defending_against_software_supply_chain_attacks_508_1.pdf, accessed 1 Mar. 2023.

Cybersecurity and Infrastructure Security Agency et al., 'Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure', *U.S. Department of Defense* (Washington, DC, 20 Apr. 2022), https://media.defense.gov/2022/Apr/20/2002980529/-1/-1/1/JOINT_CSA_RUSSIAN_STATE-SPONSORED_AND_CRIMINAL_CYBER_THREATS_TO_CRITICAL_INFRASTRUCTURE_20220420.PDF, accessed 2 Mar. 2023.

Cybersecurity and Infrastructure Security Agency, *CISA Urges Increased Vigilance One Year After Russia's Invasion of Ukraine* [media release] (23 Feb. 2023), https://www.cisa.gov/news-

events/alerts/2023/02/23/cisa-urges-increased-vigilance-one-year-after-russias-invasion-ukraine, accessed 1 Mar. 2023.

de Salins, G., 'Enhancing the Digital Security of Products: A Policy Discussion', *OECD* (9 Feb. 2021), https://www.oecd-ilibrary.org/docserver/cd9f9ebc-en.pdf?expires=1679558080&id=id&accname=guest&checksum=5BE96FFD158E0E2A7D46C8CCE6CC9DAE, accessed 2 Mar. 2023.

de Salins, G., 'Understanding the Digital Security of Products: An In-Depth Analysis', *OECD* (Paris, 9 Feb. 2021), https://www.oecd-ilibrary.org/docserver/abea0b69-en.pdf?expires=1679552648&id=id&accname=guest&checksum=D03505E9BD4AB041A6D6A76FA7EC15C6, accessed 1 Mar. 2023.

Deibert, R., 'Divide and Rule: Republican Security Theory as Civil Society Cyber Strategy', *Georgetown Journal of International Affairs*, 14/3 (2013), 39-50.

Department of Foreign Affairs and Trade (Commonwealth of Australia), 'Australia's International Cyber and Critical Tech Engagement', *Australia's International Cyber and Critical Tech Engagement* (7 Mar. 2023), https://www.internationalcybertech.gov.au/, accessed 1 Mar. 2023.

Department of Foreign Affairs and Trade (Commonwealth of Australia), 'Australia's International Cyber and Critical Technology Engagement Strategy', *Australia's International Cyber and Critical Tech Engagement* (Canberra, 21 Apr. 2021), https://www.internationalcybertech.gov.au/strategy, accessed 1 Mar. 2023.

Department of Foreign Affairs and Trade (Commonwealth of Australia), 'Partnerships and Agreements', *Australia's International Cyber and Critical Tech Engagement* (2022), https://www.internationalcybertech.gov.au/our-work/partnerships-and-agreements, accessed 12 Mar. 2023.

Department of Foreign Affairs and Trade (Commonwealth of Australia), 'Multilateral Engagement', *Australia's International Cyber and Critical Tech Engagement* (2022), https://www.internationalcybertech.gov.au/our-work/multilateral-engagement, accessed 12 Mar. 2023.

Department of Foreign Affairs and Trade (Commonwealth of Australia), 'Capacity Building', *Australia's International Cyber and Critical Tech Engagement* (2022), https://www.internationalcybertech.gov.au/our-work/capacity building, accessed 4 Mar. 2023.

Department of Foreign Affairs and Trade (Commonwealth of Australia), 'Meet our CCTCP Partners', *Australia's International Cyber and Critical Tech Engagement* (5 Nov. 2022), https://www.internationalcybertech.gov.au/our-work/capacity building/meet-our-CCTCP-partners, accessed 1 Mar. 2023.

Department of Foreign Affairs and Trade (Commonwealth of Australia), 'Organisation Structure', *Department of Foreign Affairs and Trade* (Canberra, 6 Feb. 2023), https://www.dfat.gov.au/sites/default/files/dfat-org-chart-executive.pdf, accessed 1 Mar. 2023.

Department of Home Affairs, *Quad Senior Cyber Group Meets in New Delhi* [media release] (1 Feb. 2023), https://www.homeaffairs.gov.au/news-media/archive/article?itemId=1015, accessed 2 Mar. 2023.

Department of Homeland Security (United States), *DHS Expands Abraham Accords to Cybersecurity* [media release] (2 Feb. 2023), https://www.dhs.gov/news/2023/02/02/dhs-expands-abraham-accords-cybersecurity, accessed 1 Mar. 2023.

Department of Homeland Security (United States), *Readout of Secretary Mayorkas's Meeting with Japanese Minister Nishimura* [media release] (6 Jan. 2023), https://www.dhs.gov/news/2023/01/06/readout-secretary-mayorkass-meeting-japanese-minister-nishimura, accessed 15 Mar. 2023.

Department of Industry, Science and Resources, 'Advanced Information and Communication Technologies', Department of Industry, Science and Resources (19 May 2023), https://www.industry.gov.au/publications/list-critical-technologies-national-interest/advanced-information-and-communication-technologies, accessed 19 May 2023.

Department of Telecommunications (India), 'Amendment to the Unified Access Services License Agreement (UASL) for Procurement of Telecommunication Equipment' (New Delhi, 11 Jul. 2022), https://dot.gov.in/accessservices/amendment-unified-access-services-license-agreement-uasl-procurement, accessed 1 Mar. 2023.

Director of the Office of Management and Budget (United States), 'Enhancing the Security of the Software Supply Chain through Secure Software Development Practices', *The White House* (Washington, DC, 14 September 2022), https://www.whitehouse.gov/wp-content/uploads/2022/09/M-22-18.pdf, accessed 2 Mar. 2023.

Easterly, J. & Goldstein, E., 'Stop Passing the Buck on Cybersecurity: Why Companies Must Build Safety into Tech Products', *Foreign Affairs* (1 Feb. 2023), https://www.foreignaffairs.com/united-states/stop-passing-buck-cybersecurity, accessed 1 Mar. 2023.

Easterly, J., 'CISA Director Easterly Remarks at Carnegie Mellon University', *Cybersecurity & Infrastructure Security Agency* (Washington, DC, 27 Feb. 2023), https://www.cisa.gov/cisa-director-easterly-remarks-carnegie-mellon-university, accessed 2 Mar. 2023.

Ebrahim, T.Y., 'National Cybersecurity Innovation', *West Virginia Law Review* 123/2 (2020), 483-546.

European Commission, 'Commission Staff Working Document: Impact Assessment Report Accompanying the Document Proposal for a Regulation of the European Parliament and of the Council on Horizontal Cybersecurity Requirements for Products with Digital Elements and amending Regulation (EU) 2019/1020', *EUR-Lex* (Brussels, 15 Sep. 2022), https://eur-lex.europa.eu/resource.html?uri=cellar:af2401a4-34e9-11ed-9c68-01aa75ed71a1.0001.02/DOC_1&format=PDF, accessed 28 Feb. 2023.

European Commission, 'Proposal for a Regulation of the European Parliament and of the Council on Horizontal Cybersecurity Requirements for Products with Digital Elements and amending Regulation (EU) 2019/1020', *EUR-Lex* (Brussels, 15 Sep. 2022), https://eur-lex.europa.eu/resource.html?uri=cellar:864f472b-34e9-11ed-9c68-01aa75ed71a1.0001.02/DOC_1&format=PDF, accessed 1 Mar. 2023.

European Commission, *EU-India: New Trade and Technology Council to Lead on Digital Transformation, Green Technologies and Trade* [media release] (6 Feb. 2023), https://ec.europa.eu/commission/presscorner/detail/en/IP_23_596, accessed 1 Mar. 2023.

European Union Agency for Cybersecurity, 'ENISA Threat Landscape for Supply Chain Attacks', *European Union Agency for Cybersecurity* (Athens, 29 Jul. 2021),

https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks, accessed 5 Mar. 2023.

European Union Agency for Cybersecurity, 'ENISA Threat Landscape 2022: (July 2021 to July 2022)', *European Union Agency for Cybersecurity* (Athens, 3 Nov. 2022), https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022, accessed 1 Mar. 2023.

Exec. Order No. 14,028, 86 Fed. Reg. 26,633 (17 May 2021).

Feakin, T., 'After six incredible years of being Australia's first Ambassador for Cyber Affairs and Critical Technology… '[LinkedIn post] (Jan. 2023), https://www.linkedin.com/posts/tobias-feakin-1102255_aftersix-incredible-years-of-being-australias-activity-7025926440000884737-pvPW/, accessed 28 February 2023.

Federal Communications Commission (United States), 'Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs; Huawei Designation; ZTE Designation', *Federal Register* (Washington, DC, 3 Jan. 2020), https://www.govinfo.gov/content/pkg/FR-2020-01-03/pdf/2019-27610.pdf, accessed 2 Mar. 2023.

Ferris, J., *Behind the Enigma: The Authorised History of GCHQ, Britain's Secret Cyber Intelligence Agency* (Great Britain: Bloomsbury Publishing, 2020).

Fleming, J., 'Director GCHQ Speaks at CyberUK 2022', *GCHQ* (10 May 2022), https://www.gchq.gov.uk/speech/cyberuk2022, accessed 1 Mar. 2023.

France24, 'French Hospital Suspends Operations after Cyber Attacks', *France24* (5 Dec. 2022), https://www.france24.com/en/france/20221205-french-hospital-suspends-operations-after-cyber-attacks, accessed 1 Mar. 2023.

Google, 'Perspectives on Security: Volume One: Securing Software Supply Chains', *Google* (8 Dec. 2022), https://services.google.com/fh/files/blogs/perspectives_on_security_volume_one_digital.pdf, accessed 2 Mar. 2023.

Greenberg, A., *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers* (United States: Doubleday, 2019).

Haidar, S. & Krishnan, A., 'Quad Foreign Ministers Take Aim at Russia and China: The Joint Statement that Refers to Both the Ukraine Conflict and the Situation in the South and East China Seas, Draws Criticism from Russia and China', *The Hindu* (4 Mar. 2023), https://www.thehindu.com/news/international/quad-foreign-ministers-take-aim-at-russia-and-china/article66577074.ece, accessed 1 Mar. 2023.

Herr, T. et al., 'Breaking Trust: Shades of Crisis across an Insecure Software Supply Chain', *Atlantic Council* (Washington, DC, 26 Jul. 2020), https://www.atlanticcouncil.org/wp-content/uploads/2020/07/Breaking-trust-Shades-of-crisis-across-an-insecure-software-supply-chain.pdf, accessed 1 Mar. 2023.

Huawei Cyber Security Evaluation Centre Oversight Board (United Kingdom), 'Annual Report 2019: A Report to the National Security Adviser of the United Kingdom', *GOV.UK* (London, 28 Mar. 2019), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/790270/HCSEC_OversightBoardReport-2019.pdf, accessed 2 Mar. 2023.

Huawei Cyber Security Evaluation Centre Oversight Board (United Kingdom), 'Annual Report 2021: A Report to the National Security Adviser of the United Kingdom', *GOV.UK* (London, 20 Jul. 2021), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1004291/2021_HCSEC_OB_REPORT_FINAL__1_.pdf, accessed 2 Mar. 2023.

Indian Technical and Economic Cooperation Programme, 'Upcoming Courses', *Indian Technical and Economic Cooperation Programme* (5 Jan. 2023), https://www.itecgoi.in/upcoming_courses, accessed 1 Mar. 2023.

International Telecommunications Union, 'Digital Technologies to Achieve the UN SDGs', *International Telecommunications Union* (12 Dec. 2021), https://www.itu.int/en/mediacentre/backgrounders/Pages/icts-to-achieve-the-united-nations-sustainable-development-goals.aspx, accessed 2 Mar. 2023.

Jaishankar, S., 'EAM: Global Technology Summit 2022 '[video], YouTube (29 Nov. 2022), https://www.youtube.com/live/MR-ebRUHMCU, accessed 9 Mar. 2023.

Kikas, R. et al., 'Structure and Evolution of Package Dependency Networks', paper presented to the 2017 IEEE/ACM 14th International Conference on Mining Software Repositories (MSR), Buenos Aires (20 - 21 May 2017), 102-112, https://www.computer.org/csdl/proceedings-article/msr/2017/07962360/12OmNyRPgq5, accessed 2 Mar. 2023.

Mandiant, 'Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims with SUNBURST Backdoor', *Mandiant* (10 May 2022), https://www.mandiant.com/resources/blog/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor, accessed 1 Mar. 2023.

Mandiant, 'The Defender's Advantage: Cyber Snapshot Issue 2', *Mandiant* (17 Oct. 2022), https://mandiant.widen.net/s/j2qvgwwhmm/defenders-advantage-cyber-snapshot-report-issue-2, accessed 1 Mar. 2023.

Martin, A., 'Multiple Government Departments in New Zealand Affected by Ransomware Attack on IT Provider', *The Record* (6 Dec. 2022), https://therecord.media/multiple-government-departments-in-new-zealand-affected-by-ransomware-attack-on-it-provider/, accessed 5 Mar. 2023.

Martin, C., 'Cyber "Deterrence": A Brexit Analogy', *Lawfare* (15 Jan. 2021), https://www.lawfareblog.com/cyber-deterrence-brexit-analogy, accessed 1 Mar. 2023.

Martin, C., 'Cyber Realism in a Time of War', *Lawfare* [blog post] (2 Mar. 2022), https://www.lawfareblog.com/cyber-realism-time-war, accessed 1 Mar. 2023.

Ministry of Defense (Japan), 'National Security Strategy', *Ministry of Defense* (Tokyo, Dec. 2022), https://www.mod.go.jp/j/policy/agenda/guideline/pdf/security_strategy_en.pdf, accessed 6 Mar. 2023.

Ministry of Electronics and Information Technology (India), 'National Cyber Security Policy - 2013', *Ministry of Electronics and Information Technology* (New Delhi, 2 Jul. 2013), https://www.meity.gov.in/sites/upload_files/dit/files/National Cyber Security Policy (1).pdf, accessed 1 Mar. 2023.

Ministry of External Affairs (India), 'Annual Report 2021 | 2022', *Ministry of External Affairs* (New Delhi, 24 Feb. 2022), https://mea.gov.in/Uploads/PublicationDocs/34894_MEA_Annual_Report_English.pdf, accessed 1 Mar. 2023

Ministry of External Affairs (India), 'Annual Report 2022', *Ministry of External Affairs* (New Delhi, 23 Feb. 2023), https://mea.gov.in/Uploads/PublicationDocs/36286_MEA_Annual_Report_2022_English_web.pdf, accessed 1 Mar. 2023.

Ministry of External Affairs (India), 'Organogram of the Ministry of External Affairs', *Ministry of External Affairs* (New Delhi, 22 Mar. 2023), https://www.mea.gov.in/Images/amb1/MeA_organograms_NW_23_22NN.pdf, accessed 22 Mar. 2023.

Ministry of Foreign Affairs of Japan, *ARF-ISM on ICTs Security 7th OESG* [media release] (28 Apr. 2021), https://www.mofa.go.jp/press/release/press22e_000052.html, accessed 8 Mar. 2023.

Ministry of Foreign Affairs of Japan, 'Cybersecurity', *Ministry of Foreign Affairs of Japan* (7 Feb. 2023), https://www.mofa.go.jp/policy/page18e_000015.html, accessed 5 Mar. 2023.

Ministry of Foreign Affairs of Japan, *The 7th Japan – UK Bilateral Consultations on Cyber Issues* [media release] (7 Feb. 2023), https://www.mofa.go.jp/press/release/press3e_000542.html, accessed 5 Mar. 2023.

Narlikar, A., 'Must the Weak Suffer What They Must?', in D.W. Dresser, H. Farrell & A.L. Newman, *The Uses and Abuses of Weaponized Interdependence* (Washington, DC: Brookings Institution Press, 2021), 289-304.

National Center of Incident Readiness and Strategy for Cybersecurity, 'Commitment to a Free, Fair and Secure Cyberspace', *National Center of Incident Readiness and Strategy for Cybersecurity* (2023), https://www.nisc.go.jp/eng/index.html, accessed 1 Mar. 2023.

National Center of Incident Readiness and Strategy for Cybersecurity, 'National Center of Incident Readiness and Strategy for Cybersecurity', *National Center of Incident Readiness and Strategy for Cybersecurity* (2023), https://www.nisc.go.jp/eng/index.html, accessed 1 Mar. 2023.

National Counterintelligence and Security Center, 'Kaseya VSA Supply Chain Ransomware Attack', *Director of National Intelligence* (10 Apr. 2021), https://www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/Kaseya VSA Supply Chain Ransomware Attack.pdf, accessed 2 Mar. 2023.

National Defense Authorization Act for Fiscal Year 2023 (USA).

National Institute for Science and Technology, 'Security Measures for "EO-Critical Software" Use under Executive Order (EO) 14028', *National Institute for Science and Technology* (United States, 9 Jul. 2021), https://www.nist.gov/system/files/documents/2021/07/09/Critical Software Use Security Measures Guidance.pdf, accessed 2 Mar. 2023.

National Institute of Standards and Technology, 'Definition of Critical Software under Executive Order (EO) 14028', *National Institute of Standards and Technology* (United States, 13 Oct. 2021), https://www.nist.gov/system/files/documents/2021/10/13/EO Critical FINAL.pdf, accessed 1 Mar. 2023.

National Institute of Standards and Technology, 'Software Supply Chain Security Guidance under Executive Order (EO) 14028 Section 4e', *National Institute of Standards and Technology* (United States, 4 Feb. 2022), https://www.nist.gov/system/files/documents/2022/02/04/software-supply-chain-security-guidance-under-EO-14028-section-4e.pdf, accessed 2 Mar. 2023.

National Research Council, *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy* (Washington, DC: The National Academies Press, 2010).

National Security Agency, 'NSA Cybersecurity Year in Review 2022' (Baltimore, 15 Dec. 2022), https://media.defense.gov/2022/Dec/15/2003133594/-1/-1/0/0139_CSD_YIR22_FINAL_LOWSIDE_ACCESSIBLE_FINAL_V2.PDF, accessed 11 Mar. 2023.

National Security Agency, Cybersecurity and Infrastructure Security Agency & Office of the Director of National Intelligence, 'Securing the Software Supply Chain: Recommended Practices for Developers', *U.S. Department of Defense* (Washington, DC, 1 Sep. 2022), https://media.defense.gov/2022/Sep/01/2003068942/-1/-1/0/ESF_SECURING_THE_SOFTWARE_SUPPLY_CHAIN_DEVELOPERS.PDF, accessed 4 Mar. 2023.

National Telecommunications and Information Administration (United States), 'SBOM at a Glance', *National Telecommunications and Information Administration* (Washington, DC, 2021), https://ntia.gov/sites/default/files/publications/sbom_at_a_glance_apr2021_0.pdf, accessed 2 Mar. 2023.

NATO Cooperative Cyber Defence Centre of Excellence, *The NATO CCDCOE Welcomes New Members Iceland, Ireland, Japan, and Ukraine* [media release] (17 May 2023), https://ccdcoe.org/news/2023/the-nato-ccdcoe-welcomes-new-members-iceland-ireland-japan-and-ukraine/, accessed 8 May 2023.

Neuberger, A., 'The U.S. Government's Global Cyber Initiatives', *U.S. Department of State* (17 Nov. 2022), https://www.state.gov/briefings-foreign-press-centers/global-cyber-initiatives, accessed 2 Mar. 2023.

Nikkei Asia, 'Japan, U.S. to Agree on Security Standards for Government Software: Nishimura and Mayorkas to Sign Memorandum on Cooperation for Cybersecurity', *Nikkei Asia* (5 Jan. 2023), https://asia.nikkei.com/Politics/International-relations/Japan-U.S.-to-agree-on-security-standards-for-government-software, accessed 4 Mar. 2023.

OECD Council, 'Recommendation of the Council on Digital Security of Critical Activities', *OECD* (Paris, 11 Dec. 2019), https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0456, accessed 1 Mar. 2023.

OECD Council, 'Recommendation of the Council on the Digital Security of Products and Services', *OECD* (Paris, 26 Sep. 2022), https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0481, accessed 27 Feb. 2023.

OECD, 'OECD Policy Framework on Digital Security', *OECD* (Paris, 14 Dec. 2022), https://read.oecd.org/10.1787/a69df866-en?format=pdf, accessed 11 Mar. 2023.

Office of Management and Budget (United States), 'Analytical Perspectives: Budget of the U.S. Government: Fiscal Year 2024', *U.S. Government Publishing Office* (Washington, DC, 13 Mar. 2023), https://www.govinfo.gov/content/pkg/BUDGET-2024-PER/pdf/BUDGET-2024-PER.pdf, accessed 2 Mar. 2023.

Office of Press Relations (United States), *USAID Announces up to $60 Million to Bolster Ukraine's Cybersecurity* [media release] (10 Feb. 2023), https://www.usaid.gov/news-information/press-releases/feb-10-2023-usaid-announces-60-million-bolster-ukraines-cybersecurity, accessed 1 Mar. 2023.

Office of the National Cyber Director (United States), 'A Strategic Intent Statement for the Office of the National Cyber Director', *The White House* (Washington, DC, 28 Oct. 2021), https://www.whitehouse.gov/wp-content/uploads/2021/10/ONCD-Strategic-Intent.pdf, accessed 12 Mar. 2023.

Office of the Spokesperson (United States), *U.S. Support for Connectivity and Cybersecurity in Ukraine* [media release] (10 May 2022), https://www.state.gov/u-s-support-for-connectivity-and-cybersecurity-in-ukraine/, accessed 1 Mar. 2023.

Office of the Spokesperson (United States), *Department of State Cybersecurity Training Series Boosts Global Resilience Against Democratic People's Republic of Korea Malware* [media release] (7 Sep. 2022), https://www.state.gov/department-of-state-cybersecurity-training-series-boosts-global-resilience-against-democratic-peoples-republic-of-korea-malware/, accessed 10 Mar. 2023.

Office of the Spokesperson (United States), *Joint Statement on Australia-U.S. Ministerial Consultations (AUSMIN) 2022* [media release] (6 Dec. 2022), https://www.state.gov/joint-statement-on-australia-u-s-ministerial-consultations-ausmin-2022/, accessed 1 Mar. 2023.

Office of the Spokesperson (United States), *The 2022 U.S.-EU Cyber Dialogue* [media release] (21 Dec. 2022), https://www.state.gov/the-2022-u-s-eu-cyber-dialogue/, accessed 11 Mar. 2023.

Office of the Spokesperson (United States), *Co-Chairs' Statement on the Third ASEAN-U.S. Cyber Policy Dialogue* [media release] (3 Feb. 2023), https://www.state.gov/co-chairs-statement-on-the-third-asean-u-s-cyber-policy-dialogue/, accessed 5 Mar. 2023.

Office of the Spokesperson (United States), *Marking One Year Since the Release of the Administration's Indo-Pacific Strategy* [media release] (13 Feb. 2023), https://www.state.gov/marking-one-year-since-the-release-of-the-administrations-indo-pacific-strategy/, accessed 3 Mar. 2023.

Orzel, E., 'Software Supply Chain Attacks: 2021 in Review', *Aqua Blog* [blog post] (25 Jan. 2022), https://blog.aquasec.com/software-supply-chain-attacks-2021, accessed Mar. 2023.

Pant, H.V. & Mattoo, S., eds., 'The Rise and Rise of the 'Quad': Setting an Agenda for India', *Observer Research Foundation* (New Delhi, 23 Sep. 2021), https://www.orfonline.org/wp-content/uploads/2021/09/ORF_SpecialReport_161_Quad-India-Agenda.pdf, accessed 9 Mar. 2023.

Parliament and Council Directive 2022/2555 on Measures for a High Common Level of Cybersecurity across the Union, Amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and Repealing Directive (EU) 2016/1148 (NIS 2 Directive) [2022] OJ L 333/80.

Parliamentary Joint Committee on Intelligence and Security (Commonwealth of Australia), 'Advisory Report on the Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022', *Parliament of Australia* (Canberra, Mar. 2022), https://parlinfo.aph.gov.au/parlInfo/download/committees/reportjnt/024898/toc_pdf/AdvisoryreportontheSecurityLegislationAmendment(CriticalInfrastructureProtection)Bill2022.pdf;fileType=application/pdf, accessed 3 Mar. 2023.

Patil, S., 'India's Cyber Diplomacy', *India Perspectives* (New Delhi, 7 Oct. 2020), para. 5, https://www.indiaperspectives.gov.in/en_US/indias-cyber-diplomacy/, accessed 1 Mar. 2023.

Payão, F., 'Banco BRB Sofre Ataque de Ransomware e Acaba Chantageado', *tecmundo* (6 Oct. 2022), https://www.tecmundo.com.br/seguranca/250306-banco-brb-sofre-ataque-ransomware-acaba-chantageado.htm, accessed 2 Mar. 2023.

Perlroth, N., *This Is how They Tell Me the World Ends* (United States: Bloomsbury Publishing, 2021).

President's National Security Telecommunications Advisory Committee (United States), 'Software Assurance in the Information and Communications Technology and Services Supply Chain', *Cybersecurity and Infrastructure Security Agency* (Washington, DC, 2 Nov. 2021), https://www.cisa.gov/sites/default/files/publications/NSTAC Report to the President on Software Assurance.pdf, accessed 2 Mar. 2023.

Public Safety and Homeland Security Bureau (United States), 'List of Equipment and Services Covered By Section 2 of The Secure Networks Act', *Federal Communications Commission* (20 Sep. 2022) https://www.fcc.gov/supplychain/coveredlist, accessed 1 Mar. 2023.

Quad Critical and Emerging Technology (CET) Working Group, 'Quad Principles on Critical and Emerging Technology Standards', *Department of the Prime Minister and Cabinet*, (Canberra, 20 May 2023), https://www.pmc.gov.au/sites/default/files/resource/download/quad-principles-critical-emerging-technology-standards.pdf, accessed 20 May 2023.

Quad Senior Cyber Group, 'Quad Cybersecurity Partnership: Joint Principles for Secure Software', *Department of the Prime Minister and Cabinet*, (Canberra, 20 May 2023), https://www.pmc.gov.au/sites/default/files/resource/download/quad-joint-principles-secure-software.pdf, accessed 20 May 2023.

Quigley, K., Burns, C. & Stallard, K., "'Cyber Gurus": A Rhetorical Analysis of the Language of Cybersecurity Specialists and the Implications for Security Policy and Critical Infrastructure Protection', *Government Information Quarterly*, 32/2 (2015), 108-117, https://doi.org/10.1016/j.giq.2015.02.001.

Raimondo, G. et al., *U.S.-EU Joint Statement of the Trade and Technology Council* [media release] (16 May 2022), https://www.commerce.gov/news/press-releases/2022/05/us-eu-joint-statement-trade-and-technology-council, accessed 2 Mar. 2023.

Reiff, N., '10 Biggest Software Companies: MSFT, ORCL, and SAP Lead the 10 Biggest Software Companies List', *Investopedia* (28 Feb. 2023), https://www.investopedia.com/articles/personal-finance/121714/worlds-top-10-software-companies.asp, accessed 2 Mar. 2023.

Renn, O., 'White Paper on Risk Governance: Toward an Integrative Framework', in Renn, O. & Walker, K.D., eds., *Global Risk Governance: Concept and Practice using the IRGC Framework* (The Netherlands: Springer, 2008), 3-73.

Reuters, 'Japan to Ban Huawei, ZTE from Govt Contracts -Yomiuri', *Reuters* (7 Dec. 2018), https://www.reuters.com/article/japan-china-huawei-idUSL4N1YB6JJ, accessed 2 Mar. 2023.

RNZ, 'PNG Government System Hit by Ransomware Attack', *RNZ* (29 Oct. 2021), https://www.rnz.co.nz/international/pacific-news/454467/png-government-system-hit-by-ransomware-attack, accessed 5 Mar. 2023.

Ross, R. et al., 'Developing Cyber-Resilient Systems: A Systems Security Engineering Approach', *National Institute of Standards and Technology* (United States of America, Dec. 2021), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2r1.pdf, accessed 3 Mar. 2023.

S. A. M. S. P. T. H. Sen, *Chairman's Statement of the 25th ASEAN-Japan Summit* [media release] (12 Nov. 2022), https://www.mofa.go.jp/files/100425548.pdf, accessed 5 Mar. 2023.

Sales, N.A., 'Regulating Cyber-Security', *Northwestern University Law Review*, 107/4 (2013), 1503-1568.

Saran, S. & Mattoo, S., 'Big Tech vs. Red Tech: The Diminishing of Democracy in the Digital Age', *Observer Research Foundation* (15 Feb. 2022), https://www.orfonline.org/research/big-tech-vs-red-tech/, accessed 8 Mar. 2023.

SBS News, 'China Has Slammed the Quad Alliance as a "Tool to Contain" the Country: Chinese Foreign Spokesperson Zhao Lijian Accused Quad Countries of Adopting a "Cold War Mentality"', *SBS News* (22 Feb. 2022), https://www.sbs.com.au/news/article/china-has-slammed-the-quad-alliance-as-a-tool-to-contain-the-country/du6mr96w5, accessed 2 Mar. 2023.

Scholz, T., 'Quad Vadis? A Risk Assessment of the Quad's Emerging Cybersecurity Partnership', *Observer Research Foundation* (New Delhi, 30 Nov. 2022), https://www.orfonline.org/wp-content/uploads/2022/11/ORF_IssueBrief_592_Quad-Cybersecurity.pdf, accessed 2 Mar. 2023.

Schroeder, E. & Dack, S., 'A Parallel Terrain: Public-Private Defense of the Ukrainian Information Environment', *Atlantic Council* (Washington, DC, 27 Feb. 2023), https://www.atlanticcouncil.org/wp-content/uploads/2023/02/A-Parallel-Terrain.pdf, accessed 2 Mar. 2023.

Secretary-General of the United Nations, 'Roadmap for Digital Cooperation', *United Nations* (New York, 11 Jun. 2020), https://www.un.org/en/content/digital-cooperation-roadmap/assets/pdf/Roadmap_for_Digital_Cooperation_EN.pdf, accessed 28 February 2023.

Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022 (Australia).

Security Legislation Amendment (Critical Infrastructure) Act 2021 (Australia).

Security of Critical Infrastructure (Critical Infrastructure Risk Management Program) Rules (LIN 23/006) 2023 (Australia).

Security of Critical Infrastructure Act 2018 (Australia).

Sheehan, M. & Feldgoise, J., 'What Washington Gets Wrong about China and Technical Standards', *Carnegie Endowment for International Peace* (Washington, DC, 27 Feb. 2023), https://carnegieendowment.org/2023/02/27/what-washington-gets-wrong-about-china-and-technical-standards-pub-89110, accessed 28 February 2023.

Slowik, J., 'What Have We Learned?', *Stranded on Pylos* (16 Feb. 2023), https://pylos.co/2023/02/16/what-have-we-learned/, accessed 2 Mar. 2023.

Smart, W. (United Kingdom), 'Lessons Learned Review of the WannaCry Ransomware Attack', *NHS England* (London, 1 Feb. 2018), https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf, accessed 2 Mar. 2023.

Smith, A. et al., 'Mitigating ICT Supply Chain Risks with Qualified Bidder and Manufacturer Lists: Recommendations on the Use of Qualified Lists and Considerations for the Evaluation of Supply Chain Risks', Cybersecurity & Infrastructure Security Agency (Washington, DC, Apr.

2021), https://www.cisa.gov/sites/default/files/publications/ICTSCRMTF_Qualified-Bidders-Lists_508.pdf, accessed 10 Mar. 2023.

Solum, L., 'Legal Theory Lexicon: Public and Private Goods', *Legal Theory Blog* [blog post] (19 Jun. 2016), https://lsolum.typepad.com/legaltheory/2016/06/legal-theory-lexicon-public-and-private-goods.html, accessed 2 Mar. 2023.

Souppaya, M., Scarfone, K. & Dodson, D., 'Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities', *National Institute of Standards and Technology* (United States, Feb. 2022), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-218.pdf, accessed 1 Mar. 2023.

The Basic Act on Cybersecurity 2014 (Japan).

The Government of Japan, 'Cybersecurity Strategy', *National Center of Incident Readiness and Strategy for Cybersecurity* (Tokyo, 28 Sep. 2021), https://www.nisc.go.jp/eng/pdf/cs-senryaku2021-en.pdf, accessed 5 Mar. 2023.

The White House, 'International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World', *National Archives* (Washington, DC, May 2011), https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf, accessed 1 Mar. 2023.

The White House, *Fact Sheet: Imposing Costs for Harmful Foreign Activities by the Russian Government* [media release] (15 Apr. 2021), https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/, accessed 3 Mar. 2023.

The White House, *Fact Sheet: Quad Leaders' Summit* [media release] (24 Sep. 2021), https://www.whitehouse.gov/briefing-room/statements-releases/2021/09/24/fact-sheet-quad-leaders-summit/, accessed 10 Mar. 2023.

The White House, *Fact Sheet: The United States and India — Global Leadership in Action* [media release] (24 Sep. 2021), https://www.whitehouse.gov/briefing-room/statements-releases/2021/09/24/fact-sheet-the-united-states-and-india-global-leadership-in-action/, accessed 21 Feb. 2023.

The White House, 'Indo-Pacific Strategy of the United States', *The White House* (Washington, DC, 11 Feb. 2022), https://www.whitehouse.gov/wp-content/uploads/2022/02/U.S.-Indo-Pacific-Strategy.pdf, accessed 27 Feb. 2023.

The White House, 'USA National Security Strategy', *The White House* (Washington, DC, 12 Oct. 2022), https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf, accessed 1 Mar. 2023.

The White House, *Fact Sheet: The Second International Counter Ransomware Initiative Summit* [media release] (1 Nov. 2022), https://www.whitehouse.gov/briefing-room/statements-releases/2022/11/01/fact-sheet-the-second-international-counter-ransomware-initiative-summit/, accessed 28 Feb. 2023.

The White House, *International Counter Ransomware Initiative 2022 Joint Statement* [media release] (1 Nov. 2022), https://www.whitehouse.gov/briefing-room/statements-releases/2022/11/01/international-counter-ransomware-initiative-2022-joint-statement/, accessed 8 Mar. 2023.

The White House, 'National Cybersecurity Strategy', *The White House* (Washington, DC, 2 Mar. 2023), https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf, accessed 10 Mar. 2023.

The White House, *Fact Sheet: Partnership for Global Infrastructure and Investment at the G7 Summit* [media release] (20 May 2023), https://www.whitehouse.gov/briefing-room/statements-releases/2023/05/20/fact-sheet-partnership-for-global-infrastructure-and-investment-at-the-g7-summit/, accessed 20 May 2023.

The White House, *Quad Leaders' Summit Fact Sheet* [media release] (20 May 2023), https://www.whitehouse.gov/briefing-room/statements-releases/2023/05/20/quad-leaders-summit-fact-sheet/, accessed 20 May 2023.

Trautman, L. J. & Ormerod, P. C., 'WannaCry, Ransomware, and the Emerging Threat to Corporations', *Tennessee Law Review*, 86 (2019), 505-556.

U.S. Department of Commerce & U.S. Department of Homeland Security, 'Assessment of the Critical Supply Chains Supporting the U.S. Information and Communications Technology Industry', *U.S. Department of Homeland Security* (Washington, DC, 25 Feb. 2022), https://www.dhs.gov/sites/default/files/2022-02/ICT Supply Chain Report_2.pdf, accessed 4 Mar. 2023.

U.S. Department of State, 'Digital Connectivity and Cybersecurity Partnership', *U.S. Department of State* (2021), https://www.state.gov/digital-connectivity-and-cybersecurity-partnership/, accessed 12 Mar. 2023.

U.S. Department of State, 'Bureau of Cyberspace and Digital Policy', *U.S. Department of State* (3 Feb. 2023), https://www.state.gov/bureaus-offices/deputy-secretary-of-state/bureau-of-cyberspace-and-digital-policy/, accessed 2 Mar. 2023.

U.S. Department of State, 'Nathaniel C. Fick', *U.S. Department of State* (3 Feb. 2023), https://www.state.gov/biographies/nathaniel-c-fick/, accessed 2 Mar. 2023.

U.S. Department of State, *The 3rd U.S.-ROK Working Group Meeting on the DPRK Cyber Threat* [media release] (9 Mar. 2023), https://www.state.gov/the-3rd-u-s-rok-working-group-meeting-on-the-dprk-cyber-threat/, accessed 10 Mar. 2023.

U.S. Department of the Treasury, *Treasury Sanctions Russia with Sweeping New Sanctions Authority* [media release] (15 Apr. 2021), https://home.treasury.gov/news/press-releases/jy0127, accessed 12 Mar. 2023.

U.S. Government Publishing Office, 'Bolstering the Government's Cybersecurity: Lessons Learned from WannaCry', *U.S. Government Publishing Office* (Washington, DC, 15 Jun. 2017), https://www.govinfo.gov/content/pkg/CHRG-115hhrg26234/pdf/CHRG-115hhrg26234.pdf, accessed 9 Mar. 2023.

'UN OEWG 2021-2025 – International Law', *The Digital Watch Observatory* (2022), https://dig.watch/event/un-oewg-2021-2025-2nd-substantive-session/un-oewg-2021-2025-international-law, accessed 1 Mar. 2023.

UNGA 'Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security' UN GAOR 76th sess Preliminary List Item 96, UN Doc A/76/135 (2021).

UNGA Res 199 (LVIII) (30 January 2004).

United States Agency for International Development, 'Cybersecurity', *United States Agency for International Development* (May 2022), https://www.usaid.gov/sites/default/files/2023-01/Cybersecurity_eng.pdf, accessed 2 Mar. 2023.

United States Government Accountability Office, 'Agencies Need to Assess Adoption of Cybersecurity Guidance', *United States Government Accountability Office* (Washington, DC, 9 Feb. 2022), https://www.gao.gov/assets/gao-22-105103.pdf, accessed 2 Mar. 2023.

United States Government Accountability Office, 'Actions Needed to Better Secure Internet-Connected Devices', *United States Government Accountability Office* (Washington, DC, 1 Dec. 2022), https://www.gao.gov/assets/gao-23-105327.pdf, accessed 26 Feb. 2023.

United States Government Accountability Office, 'Agencies Are Taking Steps to Expand Diplomatic Engagement and Coordinate with International Partners', *United States Government Accountability Office* (Washington, DC, 2 Feb. 2023), https://www.gao.gov/assets/gao-23-105534.pdf, accessed 2 Mar. 2023.

United States Government Accountability Office, 'Federal Agency Efforts to Address International Partners' Capacity to Combat Crime', *United States Government Accountability Office* (Washington, DC, 1 Mar. 2023), https://www.gao.gov/assets/gao-23-104768.pdf, accessed 4 Mar. 2023.

Uren, T. & Cave, D., 'Why Australia Banned Huawei from Its 5G Telecoms Network', *Australian Strategic Policy Institute* (30 Aug. 2018), https://www.aspi.org.au/opinion/why-australia-banned-huawei-its-5g-telecoms-network, accessed 1 Mar. 2023.

Uren, T., 'Give Me E2EE or Give Me Death: PLUS: Beware the Tiny Stick of Regulation', *Seriously Risky Business* (2 Mar. 2023), https://srslyriskybiz.substack.com/p/give-me-e2ee-or-give-me-death, accessed 3 Mar. 2023.

Weigand, S., 'Government of Vanuatu Offline since Early November in Suspected Ransomware Attack', *SC Media* (12 Dec. 2022), https://www.scmagazine.com/news/ransomware/the-government-of-vanuatu-offline-since-early-november-in-suspected-ransomware-attack, accessed 5 Mar. 2023.

DIGITAL DIPLOMACY AND STATECRAFT WORKING PAPER