02/2023

#02

The Quad: Carved in Code

Shaping (Inter)national Security through Reshaping Economic Incentives

Ravi Nayyar

DIGITAL DIPLOMACY AND STATECRAFT

POLICY BRIEF

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

DIGITAL DIPLOMACY AND STATECRAFT POLICY BRIEF

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 – Shaping (Inter)national Security through Reshaping Economic Incentives

Abstract

This policy brief explores the cooperation of the Quad governments (Japan, Australia, the United States, and India) on tackling cyber-borne threats to (inter)national security, focusing on their pledge to pursue certain minimum security standards for software procurement. After detailing the suboptimal state of software security, this policy brief will explain why governments need to provide a robust policy response and how the Quad does so. In this vein, the aforementioned pledge by the four governments is presented as a suitable policy option. The policy brief will argue this with reference to: the benefits of the pledge leveraging economic incentives to shape vendor behaviour, rather than enacting coercive statutory regimes for all software marketed in the Quad countries; the pledge functioning as a tool with which the Quad can counter structural issues in the software ecosystem; and the pledge enabling the Quad's internal credibility and thus making the four governments coalesce around implementing it and uplifting software security. It will conclude by pointing to how the benefits of the Pledge are easily transferable outside the Quad, helping position it as a positive force for encouraging the cyber resilience of societies and economies.

Policy Implications

- Countries have tended to focus on 'cleaning cobwebs, not killing the spider' in their cyber diplomacy: they have not devoted sufficient attention to working together to remedy systemic software insecurity.
- Governments must intervene as regulators because societies are inherently dependent on secure software, market forces have failed to appropriately incentivise software vendors to invest in a secure software development lifecycle ('SDLC') and the threat environment for software supply chains is deteriorating. The Quad governments have chosen to act by leveraging economic incentives to shape vendor behaviour: they have pledged to jointly develop software security standards for their procurement regulations.
- Because vendors will be driven to invest in their SDLCs, including through better understanding their software supply chains and performing robust due diligence on third-party code, the pledge will tackle structural issues in the software ecosystem.
- The pledge is highly likely to succeed because it encourages the internal credibility of the Quad, feeding directly into the Quad's agenda of tackling cyber-borne threats to (inter)national security. It is the product of each government's political will to uplift software security at home. In providing common procurement standards for vendors to comply with, the pledge will enhance economic and digital linkages within the Quad. It will deepen mutual trust because the governments will be able to rely on each other's standards for cyber resilience.
- The benefits of the pledge are readily transferable to stakeholders outside the Quad. The stated software security standards can be adopted by any government. If software vendors invest in their SDLC per these standards, all users of their products will benefit from greater software security. Therefore, the pledge will enable capacity building by the Quad of countries with not as developed approaches to cyber resilience, helping position the Quad as a positive force for encouraging cyber resilience around the world.

Introduction

The Quadrilateral Security Dialogue — also known as ‘the Quad’, comprising India, the United States, Australia and Japan — seeks to tackle security threats 'in the Indo-Pacific and beyond… including in cyber space’ (Biden et al., 2021, paras. 1-3). Under the Quad Cybersecurity Partnership (‘the QCP’), the four governments have committed to mitigate the threat to (inter)national security posed by software insecurity (Commonwealth of Australia et al., 2021, para. 1; Quad Senior Cyber Group, 2023, p. 2). This policy brief focuses on one innovative facet of that work: the Quad governments’ pledge to pursue certain minimum security standards for software procurement to uplift software security in general (hereinafter referred to as ‘the Pledge’). After defining software insecurity, this policy brief will explain why that problem requires much greater attention than it currently receives and why efforts to solve it are necessary. It will then identify the Pledge as a suitable policy option for the Quad as part of these efforts, pointing to the benefits of the Pledge in: leveraging economic incentives to shape vendor behaviour, rather than enacting coercive statutory regimes for all software marketed in the Quad countries; countering structural issues in the software ecosystem; and enabling the Quad’s internal credibility and thus making the four governments coalesce around implementing it successfully and uplifting software security. The policy brief will then conclude by pointing to how the benefits of the Pledge are easily transferable outside the Quad, helping position it as a positive force for encouraging the cyber resilience of societies and economies.

This policy brief 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’ (Ross, 2021, p. 60).

What Is the Problem?

Cyber-borne threats to (inter)national security are not merely theoretical. For example, there have been several breaches of cyber resilience at critical infrastructure assets around the world in recent years, spread across sectors including healthcare, financial services, telecommunications and managed services. The Quad countries have engaged in cyber diplomacy, bilaterally and multilaterally, to help mitigate the risk of cyber-borne threats to (inter)national security eventuating, including work on making technology supply chains and global digital infrastructure cyber resilient, as well as capacity building initiatives. Unfortunately, this diplomacy has not devoted sufficient attention to a large source of the problem: software insecurity (See, eg, European Commission, 2022a, p. 6).

This failure to pay due heed to software insecurity has resulted in, as the Director of the Cybersecurity & Infrastructure Security Agency put it, technology vendors reducing their end-users to ‘crash test dummies’ (Easterly, 2023, paras. 12, 15, 22). The issue stems in no small part from the inadequacy of market forces to uplift software security. Vendors remain more concerned with the speed by which they can get software to market than reasonably investing in a secure software development life cycle (‘SDLC’) (European Commission, 2022a, p. 11). Governments need to do more to reform such flawed incentive structures, particularly because malicious cyber actors view software supply chains as ‘priority target[s]’ and increasingly have the capability to compromise them, posing ‘a systemic risk’ for societies (Agence Nationale de la Sécurité des Systèmes d’Information, 2023, p. 30; Australian Cyber Security Centre, 2022, p. 65; European Union Agency for Cybersecurity, 2022, pp. 27, 30-31). The threat environment for software generally is so chaotic such that it ‘is virtually impossible to anticipate’, raising the stakes for governments to act (President’s National Security Telecommunications Advisory Committee (United States), 2021, p. 20). 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 recognising ‘the security risks posed by lack of adequate controls to prevent tampering with the software supply chain by adversarial and non-adversarial threats’ (Quad Senior Cyber Group, 2023, p. 2). It is little wonder that the Pledge seeks ‘to significantly reduce the number and potential impact of software vulnerabilities’, capturing how the policy stakes for governments to act have only grown in recent years (Quad Senior Cyber Group, 2023, p. 2).

Why Does It Matter?

Governments must intervene in the development and distribution of software because of the inherent dependence of societies on digital technologies, and thus (the security of the) software enabling the latter, to thrive. Software’s ubiquity weaves it into the very fabric of a modern economy. Therefore, governments must create legal requirements that incentivise software vendors to invest in bolstering their SDLCs; with the Quad governments defining their commitment under the Pledge as ‘integrating secure software practices throughout the software lifecycle’ and seeking to 'promote and strengthen a culture where software security is by design and default’ (Quad Senior Cyber Group, 2023, p. 2).

Using legal requirements to incentivise vendors’ investment in securing their SDLCs is also necessary because software security is a public good. 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: Ebrahim, 2020, p. 522). 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 is, persons who do not pay the vendors for those benefits – that they do not appropriately invest in secure SDLCs (Sales, 2013, p. 1528; Coyne & Leeson, 2005, p. 480). Thirdly, since vendors are not held responsible for the negative externalities of malicious cyber actors exploiting vulnerabilities in their software, they fail to internalise these externalities and are thus not driven to invest in a secure SDLC. These three factors create a market failure, namely inadequate software security, highlight the nature of software security as a public good, and thus demonstrate the Pledge to be even more necessary; particularly since software security is vital for all societies not just the Quad countries (European Commission, 2022a, pp. 9-10, 17).

Given that software security enables the cyber resilience of today's societies, such legal requirements will enable the delivery of the public goods of national security and national cyber resilience in all countries. National security is a public good: neither can a government exclude persons subject to its jurisdiction from benefitting from its efforts to promote national security nor can a person's so benefitting undermine another person's benefitting from that national security. The same analysis also applies to national cyber resilience, a driver of national security, which makes national cyber resilience a public good. These factors particularly make it vital for the enactment of legal requirements that incentivise vendors to invest in secure SDLCs. The Quad countries themselves point to how high the stakes are when it comes to national security risks from software supply chain risks (Quad Senior Cyber Group, 2023, p. 2).

It should be noted that such a policy response – seeking to deliver public goods in software security, national security and national cyber resilience around the world – is welcome because it is different to the blatant weaponisation by governments of their countries' technology companies as instruments of influence and/or interference in the affairs of countries that buy those companies' products. These governments – such as the Chinese government with its Belt and Road Initiative and Digital Silk Road programmes – essentially seek to securitise their being the regulators of these companies that are chokepoints in global (technology) value chains; and thus aim to weaponise the interdependence of other countries with these value chains (Narlikar, 2021, p. 290; Lewis, 2023, p. 7).

What Should Be Done about It?

Governments have a few options for law reform.

For example, they can enact regulatory regimes that: mandate the development and distribution of software marketed to any person in their jurisdictions to comply with baseline security standards; and make software vendors liable for failures to comply with those regimes, for instance, through a 'duty of care' to their end-users (European Commission, 2022b, pp. 7-8; OECD Council, 2022, art. IV; The White House, 2023a, pp. 19, 20-21). Indeed, the *Joint Principles for Secure Software* convey the Quad governments' intent to 'where necessary… build policy frameworks' that 'encourage' software developers and vendors to invest in their SDLCs (Quad Senior Cyber Group, 2023, p. 2). This vague wording potentially foreshadows the creation of specific regulatory regimes for the security of software as flagged above.

Governments can also amend, however, their procurement regulations, that is, exploit their purchasing power in software markets in order to incentivise software vendors to invest in their SDLCs, rather than using purely coercive legal obligations under the aforementioned regulatory regimes.

The Pledge is the latter option, 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. 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 resilience across their economies and the software ecosystem more broadly (Commonwealth of Australia et al., 2022b, paras. 5-7; Quad Senior Cyber Group, 2023, p. 2). They also commit to 'establishing minimum cybersecurity guidelines for governments to guide their… procurement… of software' (Quad Senior Cyber Group, 2023, p. 2).

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 recommended for software developers and suppliers by the National Institute of Standards and Technology ('NIST'): 'Prepare the Organization'; 'Protect the Software'; 'Produce Well-Secured Software'; and 'Respond to Vulnerabilities' (Quad Senior Cyber Group, 2023, p. 2; Souppaya, Scarfone & Dodson, 2022, p. 4). The four governments have also committed to incorporate the following '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 (Quad Senior Cyber Group, 2023, p. 2).

There are three reasons for why the Pledge is a suitable policy option for the Quad, namely that it: leverages economic incentives, not solely vendors' fear of liability under a regulatory regime; counters structural issues in the software ecosystem; and drives the Quad's internal credibility, such that the four governments will be particularly invested in implementing it. These reasons will now be explained.

Leveraging Economic Incentives

The Pledge seeks to leverage economic incentives — the opportunity to sell software to the four governments — in order to drive vendors to invest in a secure SDLC, rather than the threat of legal liability for marketing insecure software to the public. The governments plan to control that opportunity by simply amending their procurement regulations, rather than enacting legislation which, it should be acknowledged, may take a long time to draft, consult on with political, civil society and industry stakeholders, and (depending on domestic political circumstances) pass through national parliaments. Therefore, the Pledge provides the Quad with a simpler means of driving change in vendors' practices more quickly than the avenue of legislation, as well as a more appealing motivation for vendors to improve their practices (the prospect of large sales).

One should also note that the Pledge operates in the context of: American dominance, certainly through that of American vendors, in the global software market; and the sizeable purchasing power of the American government which has proposed to spend 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 (U.S. Department of Commerce & U.S. Department of Homeland Security, 2022, p. 35; Office of Management and Budget (United States), 2023, pp. 153-157). These factors make the Pledge appropriately targeted because of the sheer scale of the positive externalities for society at large that will result from: major American vendors especially being incentivised to invest in making their products securer by default and design; as well as vendors generally investing in a secure SDLC because they stand to make sizeable revenues from selling software to the American government.

Countering Structural Issues in the Software Ecosystem

The necessity of the Pledge as a means to incentivise vendors to invest in secure SDLCs arises from, in addition to the aforementioned suboptimal state of software security and deteriorating threat environment, two 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 (de Salins, 2021a, p. 10). For example, from January to July 2022, Mandiant observed organisations, on average, to have '244 unique technology vendors and business relationships' each (Mandiant, 2022, p. 12). 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 do so. As this complexity increases, so does the difficulty for stakeholders, including vendors, to map vulnerabilities across their supply chains and remedy them, giving rise to an even larger attack surface for software end-users (Google, 2022, p. 6). Exacerbating matters is the absence of a 'standard method for software development' (President's National Security Telecommunications Advisory Committee (United States), 2021, p. 15). In this regard, the 'conflicting incentives' and regulatory inconsistencies that define software supply chains provide threat actors with several vulnerabilities to exploit (President's National Security Telecommunications Advisory Committee (United States), 2021, p. 16). In laying down standards for vendors, seeking lucrative government contracts, in terms of establishing and maintaining a secure SDLC, the Pledge will help promote uniformly robust software development and maintenance practices in the broader 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).

Secondly, there is a misallocation of responsibility for assuring software security (de Salins, 2021a, p. 12). 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 (Smith et al., 2021, p. 19; Kikas et al., 2017, p.103.). Stakeholders may also be unable to compel third-party authors to disclose their security practices or promptly resolve vulnerabilities. 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' (Alderfer et al., 2022, p. 33). 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, such as the Quad governments, will also 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), helping end-users more swiftly identify and manage their own software supply chain risks (Commonwealth of Australia et al., 2022b, para. 6; National Telecommunications and Information Administration (United States), 2021, p. 1). One should also note that the Quad governments have 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' (Quad Senior Cyber Group, 2023, p. 2). 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.

Driving the Quad's Internal Credibility

The Pledge is an appropriate policy option because it drives the Quad's internal credibility as a grouping and thus encourages the four governments to coalesce around implementing the Pledge, uplifting the chances of its success and thus the level of software security.

From the outset, one should note that the close working relationship required for regulatory coordination under the Pledge is enabled 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' (The White House, 2021, para. 22). As at the writing of this paper, the QSCG Principals have met twice: once in Sydney in 2022 and once in New Delhi in 2023 (Commonwealth of Australia et al., 2022a; Department of Home Affairs, 2023). 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). 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 (Quad Senior Cyber Group, 2023, p. 2).

In addition to the QSCG providing a bureaucratic structure to guide these efforts, there are three reasons why the Pledge encourages the internal credibility of the Quad.

Firstly, the Pledge feeds directly into the Quad's agenda, namely the Quad's commitment to tackle security threats 'in the Indo-Pacific and beyond… including in cyber space' (Biden et al., 2021, paras. 2-3). Combatting what has been termed a serious driver of 'systemic risk across the digital ecosystem' is inherent to the guiding vision of the Quad itself and of the QCP (The White House, 2023a, p. 20). 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 committing to uplift the security of technology supply chains serving those assets (Commonwealth of Australia et al., 2022b, paras. 2-3). The vitality of software security to societies' very functioning, as highlighted above, grounds the policy merits of the Pledge and its linkage with the Quad's agenda. 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 (Scholz, 2022, p. 11). These factors mean that the Quad will most likely coalesce around the Pledge.

Secondly, the Pledge is an appropriate policy option for the Quad governments because they have passed laws and/or created policies that seek to uplift software security. The Pledge thus leverages their political will at home to tackle the latter issue, driving the Quad's internal credibility, which itself increases the chances of the Pledge's success. Examples of this political will now be provided.

The United States 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 the use of federal procurement regulations (Exec. Order No. 14,028, 86 Fed. Reg. 26,633, 26,637-41 (17 May 2021)). The National Institute of Standards and Technology ('NIST') defined and recommended security measures for the use of critical software, measures that can be applied to software generally (National Institute of Standards and Technology, 2021a; National Institute of Standards and Technology, 2021b). NIST also released guidance on secure software development and software supply chain risk management, with all federal government agencies mandated to comply with that guidance (Souppaya, Scarfone & Dodson, 2022, p. 1; National Institute of Standards and Technology, 2022; Director of the Office of Management and Budget (United States), 2022, p. 1). More generally, the United States seeks to 'shift liability for insecure software products and services' to negligent software vendors, and will penalise government contractors for knowingly failing to comply with contractual standards for the cyber resilience of their products and/or misrepresenting their own controls through the Civil Cyber Fraud Initiative (The White House, 2023a, pp. 20-22).

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 interest' (Department of Industry, Science and Resources, 2023, paras 1, 6, 12). In early 2023, Australia enacted supply chain risk management obligations for critical infrastructure asset operators (*Security of Critical Infrastructure (Critical Infrastructure Risk Management Program) Rules (LIN 23/006) 2023* (Australia) rr. 8, 10).

Japan's *Cybersecurity Strategy* commits it to 'promote efforts to develop and implement concrete security measures' for technology supply chain risk management by industry (The Government of Japan, 2021, p. 23). The government will also work towards (software) supply chain reliability and the development of a software verification system (The Government of Japan, 2021, pp. 23, 43). 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 (Ministry of Defense (Japan), 2022, p. 23).

India's *National Cyber Security Policy-2013* calls for mandating secure software development practices. 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 (Ministry of Electronics and Information Technology (India), 2013, pp. 7-8).

In this fashion, the four governments are already tackling or have pledged to tackle software security as part of their domestic laws and/or policies. Therefore, the Pledge is an extension of the governments' intent to improve software security at home, seen in how they have committed to bolster and coordinate these domestic efforts under the *Joint Principles for Secure Software*. Crucially, this makes the incentives for the four governments to engage on other (cyber policy) issues through the Quad substantial.

Thirdly, the Quad countries will coalesce around the Pledge and be invested in implementing it in order to uplift software security because the resultant regulatory coordination will strengthen their mutual trust. In general, such coordination reflects convergences, both of interests and approaches to advance them, after all.

Working together to make software security standards under their procurement regulations more robust can particularly boost engagement in the Quad. Given that these regimes govern the choice and management of the very systems that keep the four governments' agencies operational, the Pledge will assure the governments' operational resilience and the availability of the critical services they provide to their citizens. 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 as part of the Quad. That trust would especially be strengthened if the four governments patronised vendors headquartered in each other's jurisdictions and vetted by each other's agencies, given their shared approach to software security as well as technology development, design, governance and use more generally; building on the principles that the Quad endorsed for the latter in September 2021 (Commonwealth of Australia et al., 2021). For instance, if the Australian, Indian and Japanese governments deepened their procurement relationships with the American software sector, key to the United States' technological dominance, this would strengthen their relationships with the United States (U.S. Department of Commerce & U.S. Department of Homeland Security, 2022, p. 35; Beecroft, 2022, pp. 3-6).

These factors will make the four governments particularly invested in the Pledge, working together to uplift software security and thus implement the guiding vision of the Quad. Given that this would ultimately benefit their own cyber resilience and enhance their digital and economic linkages between, the Pledge is a driver of the internal credibility of the Quad.

Conclusion

This paper situated the Pledge within the context of societies' inherent dependence on secure software, complicated by a worsening threat environment for software supply chains and governments' generally overlooking the software security problem in their cyber diplomacy. Market forces have failed to appropriately incentivise software vendors to invest in secure SDLCs, necessitating intervention by the state as a regulator. This policy brief argued that the Pledge is a suitable option for how the Quad should intervene in software markets, that is, by leveraging the four governments' buying power in software markets to shape vendor behaviour. The Pledge is also a suitable option because, by applying to vendors that sell to the four governments, it will help the latter counter structural issues in the software ecosystem. Additionally, the Pledge is a suitable policy option because it will drive the internal credibility of the Quad, making the four governments rally around implementing it.

In terms of the way forward, 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 reason is 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 users of their products will benefit from using securer software, not just the Quad governments.

Secondly, the underlying software security standards that the latter 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 countries 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 — insecure software. The Quad's approach to directly bolstering software security can thus spread across the Indo-Pacific and the world with said standards as a template for others to follow. Indeed, the Quad has positioned the *Joint Principles for Secure Software* as a template, calling on other countries to 'adopt these principles in pursuit of this shared vision for secure software' (Quad Senior Cyber Group, 2023, p. 2). In this fashion, the Pledge will help position the Quad as a positive force for encouraging the cyber resilience of societies and economies.

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.

References

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., '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.

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.

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 Government, 'Australia's Cyber Security Strategy 2020', Department of Home Affairs (Canberra, 6 Aug. 2020), https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf, accessed 1 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.

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 2023a), 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 2023b), https://www.whitehouse.gov/briefing-room/statements-releases/2023/05/20/g7-leaders-statement-on-economic-resilience-and-economic-security/, accessed 20 May 2023.

Chung, J.J., 'Critical Infrastructure, Cybersecurity, and Market Failure', Oregon Law Review, 96(2) (2018), 441-476.

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.

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. 2022a), 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 2022b), 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.

Cybersecurity & Infrastructure Security Agency, ‘Defending against Software Supply Chain Attacks’, Cybersecurity & 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.

de Salins, G., ‘Enhancing the Digital Security of Products: A Policy Discussion’, OECD (9 Feb. 2021a), 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. 2021b), https://www.oecd-ilibrary.org/docserver/abea0b69-en.pdf?expires=1679552648&id=id&accname=guest&checksum=D03505E9BD4AB041A6D6A76FA7EC15C6, accessed 1 Mar. 2023.

Department of Foreign Affairs and Trade, ‘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 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 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.

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., ‘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. 2022a), 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. 2022b), 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 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, 26,637-41 (17 May 2021).

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.

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.

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.

Lewis, J., ‘An Overview of Global Cloud Competition’, Centre for Strategic & International Studies (Washington, DC, 10 Apr. 2023), https://csis-website-prod.s3.amazonaws.com/s3fs-public/2023-04/230410_Lewis_Overview_Cloud_1.pdf?VersionId=6AadFmPzIuwPiLPNrlqX.sqwOZYnPOu0, accessed 2 Mar. 2023.

Lostri, E. & Pell, S., 'The Biden-Harris Administration Releases New National Cybersecurity Strategy’, Lawfare (3 Mar. 2023), paras. 28, 52-3, https://www.lawfareblog.com/biden-harris-administration-releases-new-national-cybersecurity-strategy, accessed 10 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.

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.

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)

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. 2021a), 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. 2021b), 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, Cybersecurity & 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.

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.

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 the Director of National Intelligence (United States), 'Annual Threat Assessment of the U.S. Intelligence Community', Office of the Director of National Intelligence (Washington, DC: 7 Feb. 2022), https://www.dni.gov/files/ODNI/documents/assessments/ATA-2022-Unclassified-Report.pdf, accessed 3 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) 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 2 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.

President's National Security Telecommunications Advisory Committee (United States), 'Software Assurance in the Information and Communications Technology and Services Supply Chain', Cybersecurity & 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.

'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.

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.

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.

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

Scholz, T., ‘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.

Schroeder, E. & S. Dack, ‘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.

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

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 18 May 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 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, 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, ‘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, ‘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, 'National Cybersecurity Strategy', The White House (Washington, DC, 2 Mar. 2023a), 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 2023b), 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 2023c), https://www.whitehouse.gov/briefing-room/statements-releases/2023/05/20/quad-leaders-summit-fact-sheet/, accessed 20 May 2023.

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 11 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
POLICY
BRIEF