Griffith UNIVERSITY
Queensland, Australia
Griffith Asia Institute

Digital challenges and political resilience in the Indo-Pacific

Ian Hall

Australia–India–Japan Trilateral 2023

POLICY BRIEF

CONTENTS

ACKNOWLEDGEMENTS

This policy brief is the product of a the Griffith Asia Institute Australia-India-Japan Trilateral Dialogue held in Brisbane on 10 February 2023, supported by the Ministry of Foreign Affairs, Japan.

Cover image: Shutterstock | metamorworks

Introduction

States and societies across the Indo-Pacific face an evolving set of challenges arising from our reliance on digital systems to communicate, transfer payments, operate infrastructure, conduct elections, and maintain social stability. Some of those challenges are technical, concerning the robustness of the hardware and software we use, but some are also political, concerning the effects of misinformation or disinformation rapidly spreading through online social networks. All these challenges demand cooperation between governments and within states, as well as between governments, public institutions, businesses, the media, and civil society organisations, to ensure that the digital world remains rule governed and secure.

The Griffith Asia Institute recently hosted analysts from Australia, India, and Japan to discuss these challenges and identify potential responses that might be implemented by the Australian, Indian, and Japanese governments—and indeed others—individually and collaboratively, in minilateral and multilateral contexts.

The Trilateral conference explored:

- Persistent and emerging online threats to regional political resilience
- Best practice in responding to those threats in ways that uphold free and open societies and secure political institutions
- Areas where Japan, India, and Australia could work together to build the necessary capacity to manage these challenges.

This policy paper summarises the findings of the conference, focusing on the participants' assessment of the digital challenges faced in the Indo-Pacific and their recommendations for action.

Persistent and emerging challenges

The participants at the Trilateral observed that the Indo-Pacific faces multiple digital challenges.

- Widespread, persistent, and evolving cyber-attacks, some likely initiated by state actors and some by criminal gangs, for espionage, ransom, fraud, and other purposes
- Patchy and incomplete information about the scale, frequency, and nature of cyber-attacks, compounded by official, corporate, and individual reluctance to publicly admit incidents
- Inadequate legislation concerning cyber-security and data protection
- Variable levels of regional state capacity, with some states lacking functional computer emergency and cyber incident response teams
- Highly inconsistent levels of cyber-security in both the public and private sectors across the region, with varying levels of understanding of best practice in mitigating and managing threats and incidents
- Vulnerabilities in the systems tasked with controlling critical infrastructure, exposed by multiple attempts at intrusion and manipulation
- Emerging technologies that may have transformative potential, from Artificial Intelligence to Quantum Computing
- Disagreements between regional states over the standards that should be used to govern all aspects of the digital domain
- Divergences in the approaches taken across the region in managing disinformation in cyber-space, potentially reflecting a lack of information-sharing about best practice, as well as significant differences about the optimal political response
- Skills shortages and the "brain drain" of skilled workers from developing to developed states.

Griffith
DIGITAL CHALLENGES AND POLITICAL RESILIENCE IN THE INDO-PACIFIC
Australia-India-Japan Trilateral Dialogue

CASE STUDY 1

Vanuatu ransomware attack

On 4 November 2022, the government of Vanuatu's servers were taken offline by an alleged ransomware attack. Every gov.vu domain was rendered inaccessible, forcing government departments, schools, courts, and hospitals, to use other means of delivering essential services. Some turned to Facebook or Gmail accounts, others use non-digital means, including writing cheques to cover the wages of public servants, over the following weeks, before the servers were finally brough back online.

The attack likely began with phishing activity, which led to malware being uploaded into government computers.[1] It was alleged that the government of Vanuatu was contacted with a ransom demand soon after the servers were taken down.[2] But others have speculated that there may have been a political motive behind the attack. Vanuatu has been at the forefront of diplomatic activism concerning Indonesia's governance of the province of Irian Jaya, which local Melanesian separatists call West Papua.[3] And Vanuatu has recently been the subject of both Chinese and Western efforts to exercise influence in the Pacific.[4] So far, however, no authoritative statement identifying a likely perpetrator has been released.

The Vanuatu attack illustrates several of the key challenges faced in the region, including the vulnerability of many states and societies to relatively simple cyber-attacks and the difficulties inherent in locating the origin of attacks.

Vanuatu parliament house, Port Vila. (Wikimedia Commons | Phillip Capper)

CASE STUDY 2

Disinformation and the Philippines

The May 2022 election in the Philippines was accompanied by widespread allegations that politicians and other actors were using social media platforms to spread false and misleading stories about themselves and their opponents.[5] In a country in which the overwhelming majority of voters are online, disinformation can spread quickly. Moreover, it can do so on multiple social media and messenger platforms with very different approaches to content moderation.

For these reasons, the Philippines has been termed "Patient Zero" for online disinformation—the first classic case of how it can be used, what impact it can have on political processes, and how it might be countered.[6]

UNITEAM
BONG BONG MARCOS PRESIDENT 2022
INDAY SARA DUTERTE VICE PRESIDENT 2022
UNITEAM
BONG BONG MARCOS PRESIDENT 2022
INDAY SARA DUTERTE VICE PRESIDENT 2022

Campaign posters of candidates Ferdinand Marcos Jr and Sarah Duterte, La Trinidad, Benguet, Philippines, February 15, 2022. (Shutterstock | CaveDweller99)

Enhancing Indo-Pacific cyber-security

The Trilateral explored several ways to enhance regional cyber-security, acknowledging the scale and the dynamic nature of the challenges involved.

Recommendations:

Several wide-ranging recommendations were made:

1. Governments and public and private institutions should invest in ongoing cyber-security contingency planning across a range of scenarios and build the capabilities to manage potential threats. This includes enhancing the cyber literacy of boards and senior executives.
2. Australia, India, and Japan should ensure that their cyber-security foreign engagement programs are well-funded and well-designed, and that digital divides between the well-prepared and the more vulnerable states in the region do not persist.
3. Australia, India, and Japan should also use their ongoing dialogues on cyber issues to review their experiences in mitigating risk and managing threats, given clear divergences in approach between the three to dealing with cyber security incidents. Priority should be given to discussing best practice for engaging the business community and the wider public.
4. Australia, India, and Japan should review and, if necessary, upgrade their intelligence sharing agreements and protocols concerning cyber threats and lessons learned from earlier incidents.
5. The three countries should consider developing trilateral cyber security threat and best practice response indices, for distribution across the Indo-Pacific.
6. Australia, India, and Japan should also consider developing trilateral table-top exercises to model the management of critical threats.
7. Australia, India, and Japan should collaborate in setting out preferred standards for a range of existing and emerging technologies, including 5G internet protocols, and collectively advance these proposals in regional and global multilateral negotiations.
8. Australia, India, and Japan should review and, if necessary, invest in research collaborations in cyber-security and critical and emerging technologies between universities and research organisations in all three countries. The participants expressed the concern that there were too few collaborations and that funding was patchy and scarce, and that these factors were undermining the capacity of all three states to manage the challenge they face.

Cyber Resilience

- Proactive contingency planning
- AI & data analytics
- Social engineering attack vectors
- Tri-lateral inter-agency cooperation
- Aust Cyber Security Centre: cyber.gov.au

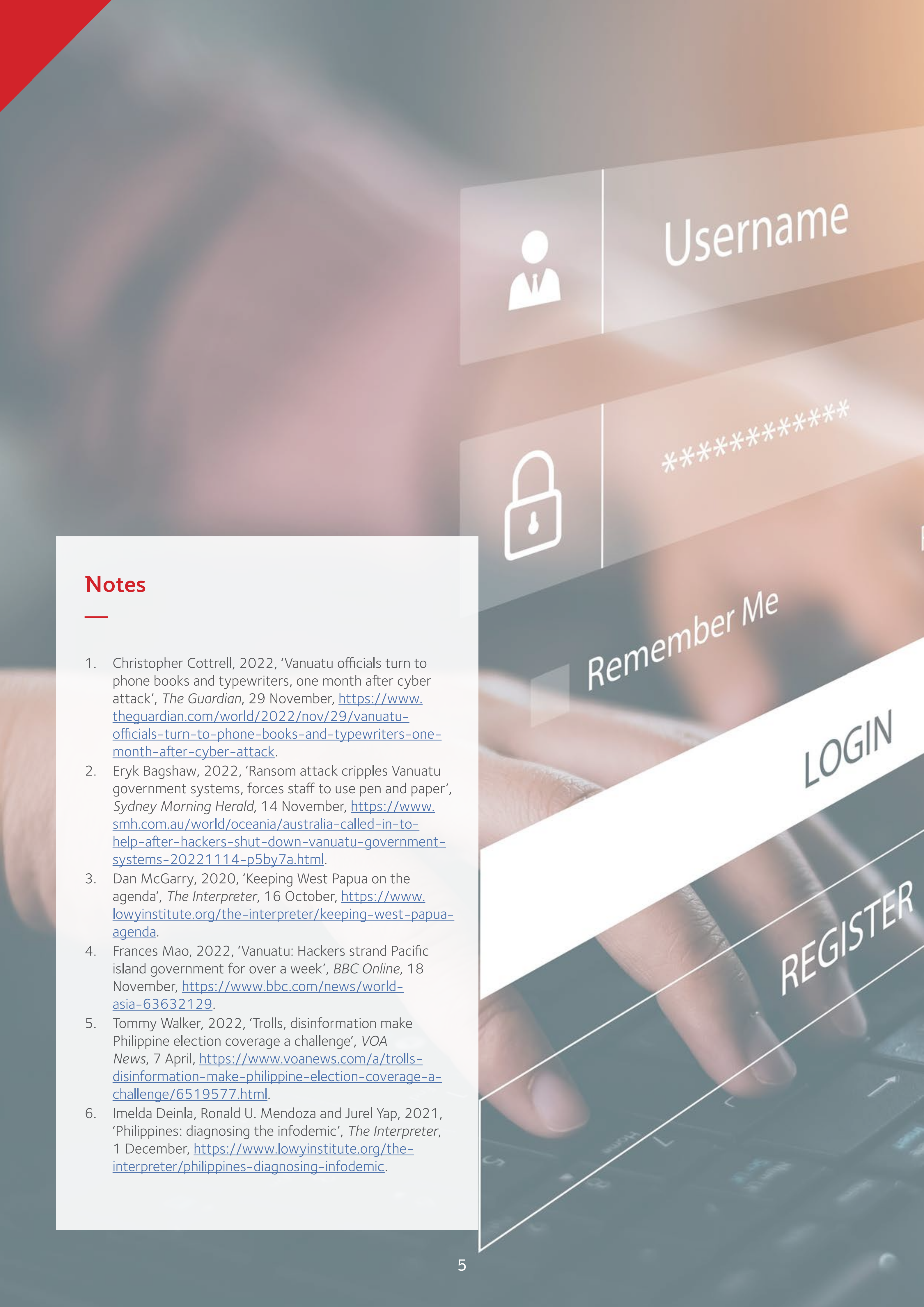
Countering disinformation

The Trilateral participants also discussed how best to counter disinformation, recognising that it can pose a significant threat to democratic processes and to social stability. They observed that Australia, India, and Japan have different approaches, reflecting the different scales and origins of disinformation circulating in their societies and different modes of regulating public speech and the traditional and non-traditional media.

Some recommendations were made, recognising that Australia, India, and Japan are already engaged in discussions about countering disinformation within the context of the Quad.

Recommendations:

1. Australia, India, and Japan should share more information about the extent and nature of the online disinformation challenges they face, especially from third parties.
2. Australia, India, and Japan should discuss their approaches to managing disinformation, ranging from fact-checking, regulatory controls on apps, and mandated content moderation by media platforms.
3. Australia, India, and Japan need to push forward discussions on achieving better public education to improve media literacy, including the ability to recognise disinformation, and best practices in public messaging to counter disinformation, while sharing information about their practices.
4. Australia, India, and Japan should share information about the management of foreign interference in the digital domain, based on the experience of the three states.



Notes

1. Christopher Cottrell, 2022, 'Vanuatu officials turn to phone books and typewriters, one month after cyber attack', *The Guardian*, 29 November, https://www.theguardian.com/world/2022/nov/29/vanuatu-officials-turn-to-phone-books-and-typewriters-one-month-after-cyber-attack.
2. Eryk Bagshaw, 2022, 'Ransom attack cripples Vanuatu government systems, forces staff to use pen and paper', *Sydney Morning Herald*, 14 November, https://www.smh.com.au/world/oceania/australia-called-in-to-help-after-hackers-shut-down-vanuatu-government-systems-20221114-p5by7a.html.
3. Dan McGarry, 2020, 'Keeping West Papua on the agenda', *The Interpreter*, 16 October, https://www.lowyinstitute.org/the-interpreter/keeping-west-papua-agenda.
4. Frances Mao, 2022, 'Vanuatu: Hackers strand Pacific island government for over a week', *BBC Online*, 18 November, https://www.bbc.com/news/world-asia-63632129.
5. Tommy Walker, 2022, 'Trolls, disinformation make Philippine election coverage a challenge', *VOA News*, 7 April, https://www.voanews.com/a/trolls-disinformation-make-philippine-election-coverage-a-challenge/6519577.html.
6. Imelda Deinla, Ronald U. Mendoza and Jurel Yap, 2021, 'Philippines: diagnosing the infodemic', *The Interpreter*, 1 December, https://www.lowyinstitute.org/the-interpreter/philippines-diagnosing-infodemic.

Trilateral participant list

The Griffith Asia Institute would like to express its gratitude to the following participants in the 2023 Australia-India-Japan Trilateral.

Ms Baani Grewal
Australian Strategic Policy Institute
Canberra

Mr Daisuke Kawai
Japan Institute of International Affairs
Tokyo

Ms Kyoko Kuwahara
Japan Institute of International Affairs
Tokyo

Dr Teesta Prakash
Australian Strategic Policy Institute
Canberra

Dr Rajeswari Pillai Rajagopalan
Observer Research Foundation
New Delhi

Ms Trisha Ray
Observer Research Foundation
New Delhi

Dr David Tuffley
Griffith University
Brisbane

ABOUT THE GRIFFITH ASIA INSTITUTE

The Griffith Asia Institute (GAI) is an internationally recognised research centre in the Griffith Business School. GAI reflects Griffith University's longstanding commitment and future aspirations for the study of and engagement with nations of Asia and the Pacific.

At GAI, our vision is to lead new ideas, knowledge and networks that contribute to an inclusive, sustainable and prosperous Asia-Pacific region.

We do this by: i) delivering research excellence on the politics, security, trade and business, governance and economic development of the region; ii) partnering for policy and impact outcomes in the region; and iii) shaping the next generation of Asia-Pacific leaders through learning experiences.

ABOUT THE AUTHOR

Ian Hall is a Professor of International Relations and the Acting Director of the Griffith Asia Institute.

GRIFFITH ASIA INSTITUTE

Griffith University Nathan campus
Nathan Queensland 4111, Australia

Email: gai@griffith.edu.au

griffith.edu.au/asia-institute