Author's Brief

General notes

Page size: A4

Margins: 2.5 cm

Headers (font, size): Calibri (Headings) 12 for Question; Calibri (Headings) 16 for response title

Font and Font size: Calibri (Body) 10 for text, Calibri (Body) 9 for reference text, Calibri (Body) 9 for reference script

Reference style: Chicago Endnotes

Reference script type, script style: superscript, numeric

Bold to be used when: In response title

Acronyms: To be spelt in full upon their first use (bracketed acronym)

Numbers: one – eight, and then 9-100 numeric

Mathematical: per cent in place of % symbol for a fraction of 100

How should Australia better contribute to international standards-setting processes in relation to cyber security, and shape laws, norms and standards that uphold responsible state behaviour in cyber space?

A HUMAN RIGHTS-BASED APPROACH TO CYBER SECURITY

The digital sphere is a civic space that provides the potential for increased opportunities around the enjoyment of human rights. Simultaneously, unequal internet access, insecure use and the lack of ownership over online information magnifies the power disparities and divisions that threaten these rights. This experience online amplifies the experiences of individual and collective injustice and inequality that undermine social cohesion, resilience and national security. Yet the lack of global digital governance means there are few internationally agreed rules, norms and agreements around how human rights are expressed in cyberspace, and limited mechanisms for their implementation.

Australia has an opportunity to position itself as a cyber security leader through a human rights-based approach that accelerates a safe and inclusive digital sphere. This approach would place people at its heart and treat equal access, secure use and ownership of cyberspace as foundational to state stability. It would broaden the traditional cyber security scope and involve a bottom-up approach that removes the trade-off between security and human rights. Through this approach we can reinforce the principle that the full, equal and meaningful enjoyment of human rights set the necessary conditions for state security. We can demonstrate that opportunities are present in online spaces for remedial human rights-based approaches to cyber security and create a blueprint for other states to follow for resilient and cohesive, digitally-engaged communities.

Digital human rights are about more than the most extreme violations that we address through our cybercrime laws, such as child exploitation. Unequal access to the internet, for example, can infringe on the right to protection, health and education services during a political or environmental crisis. Surveillance technologies can violate the right to security and freedom of movement by enabling the tracking of dissidents and the use of metadata for targeting news feeds can spread extreme views and violate the freedom from cruelty. These examples highlight the large degree of overlap between human rights, social cohesion and resilience that are core to our national security.

To truly set standards around exercising digital human rights we must lead by example and harmonise our own security laws with our human rights obligations. A good place to start would be to re-frame and re-align anti-discrimination legislation to better deal with the online discrimination that affects large portions of the population. At the same time, we could use this human rights framework to re-evaluate and re-purpose legislation around privacy, freedom of expression and surveillance. This would also require a re-examination of where the legislative line is drawn between our private and public lives. While these reviews should not dismiss national security threats, nor should they disregard the responsibility of government to uphold the human rights of its citizens. The involvement of national security issues does not justify policies that favour coercion over human rights.

The ability to regulate both domestic and international companies when needed to secure human rights would be an important step in setting these standards. We can't expect that enemies and criminals would adhere to these regulations and standards. But in the same way that security is provided through the regulation of arms, we can provide digital security in a way that moves us closer to the enjoyment of rights. Australia has already demonstrated its ability to regulate international companies in the digital space with the News Media Bargaining Code. This world-first law to make tech companies pay for news content is viewed by other states as a blueprint for how to subsidise local news platforms. Similarly, we could impose stricter regulations in areas

such as data collection, retention and use, and the sale, purchase and use of surveillance technologies, and hold companies liable for non-compliance.

Pacific Island states are at a high risk of cyber-attack and their security is intertwined with our own. Tuvalu is already exploring ways to use digital innovation to protect the nation's political, economic and cultural rights, by digitally recreating itself. Our cyber security strategy should also reinforce that it is Australia they should be looking to to secure their digital rights. This would require more than awareness training, voluntary ethical frameworks and the strengthening of policies and skills that form part of our existing offerings. By enabling diasporas to maintain language, culture and traditions securely and meaningfully, we would loudly signal our commitment to digital human rights in the Pacific. If Pacific states follow Tuvalu in replicating themselves into cyberspace, our leadership on this issue will become even more important.

Setting standards around internet use and ownership is one part of a solution to securing digital human rights. The second part is setting standards for equal internet access. This is particularly important for women, who are at a higher risk of domestic abuse as a result of political or collective violence. By comprehensively addressing digital rights we can reduce vulnerabilities to enable individuals and communities to more quickly bounce back from a crisis**.** The Albanese government has already committed to bridging the 'digital divide'. But our national cyber security strategy should take this further. Australians replace their mobile phones every 35 months on average, but only 22 per cent of these are recycled.[1] One option for bridging this divide would be a National Device Bank like the one developed by the United Kingdom's Good Things Foundation.[2] This would involve a mobile device recycling campaign to collect and refurbish devices before re-distributing them to struggling communities along with low or no cost sims and services.

Australia could leverage its telecommunications partnerships to roll out a similar initiative for Pacific Island nations. Despite 86 per cent of mobile coverage, high electricity rates, the affordability of devices and services and other socio-economic issues place the usage of mobiles at 27 per cent.[3] This has meant that populations are falling further behind in areas such as education and health, which disproportionately affects the rights of women. This initiative, along with support for local start-ups and investment in network stability could form part of an industry incentive package to meet their digital human rights obligations.

Cyber security is the concern of multiple governmental agencies and non-governmental institutions, however there is currently a lack of clear coordination and consistency. Achieving this human rights-based approach to cyber security would require that we address the technological, legal, social and national security components together. We would need a multi-stakeholder approach that brings together government, technologists, industry and legal, human rights and national security experts. Together, these stakeholders could map the issues, institutions and processes that comprise the cyber security sphere. This would allow us to build human rights into cyber security governance processes that can be consistently applied across the nation. We could validate this approach through the European Convention of Cybercrime (the Budapest Convention) and leverage this validation to call on states to safeguard these rights in the global commons.

Cybersecurity too often focuses on geopolitical issues and state power relations. We can set ourselves apart by developing a cyber security strategy focused on digital human rights. This approach recognises that power disparities and divisions undermine social cohesion and resilience. It aims to strengthen our national security by remediating unequal access, insecure internet use and ownership of cyberspace at the individual level. By connecting individual experiences of human rights breaches with state measures to promote resilience and cohesion, we can prosecute national security legislation, regulation and normative reforms while avoiding the pitfalls associated with the securitisation of human rights. Through this approach we can set standards around digital human rights, position Australia as a cyber security asset and create a model for states to adopt and adapt. This will allow us to influence and build the necessary trust to shape global norms around responsible state behaviour in cyberspace.

[1] Australian Mobile Telecommunications Association, Mobile Muster Annual Report 2022 (North Sydney: Australian Mobile Telecommunications Association, 2022), https://www.mobilemuster.com.au/annual-report-2022/.

[2] "National Device Bank," Good Things Foundation, accessed April 3, 2023, https://www.goodthingsfoundation.org/national-device-bank/.

[3] Tim Hatt, "The Mobile Economy Pacific Islands 2023 Executive Summary," Global Systems for Mobile Communications Intelligence, Global System for Mobile Communications Association, accessed April 3, 2023, https://data.gsmaintelligence.com/research/research/research-2023/the-mobile-economy-pacific-islands-2023-executive-summary.