# CyberCX Submission - Inquiry into Australia's response to the priorities of Pacific Island countries and the Pacific region

**Author: Alex Sallabank, Director, Strategy & Consulting, CyberCX**

DATE: July 2024

# Introduction

This submission from CyberCX addresses the critical issues and opportunities for the Australian Government in the Pacific region as they relate to the cyber security of Pacific communities. The submission emphasises the challenges faced by these countries in achieving widespread and reliable access to high-speed internet due to limited infrastructure. It also highlights the transformative impact that potential investments in digital infrastructure can have, such as improved connectivity, digital literacy, and economic growth through enhanced telecommunications. CyberCX emphasises the need for a strategic approach to digital investments made by the region's multiple development partners, as well as the opportunity that enhancing cyber security represents to support the wider economic development and resilience of the Pacific region.

CyberCX's key recommendations include:

- Australia and partner states should adopt a greater strategic approach to directing digital infrastructure investment in the Pacific. This is required because the multitude of bilateral and multilateral investment initiatives makes it challenging for governments and businesses to navigate.
- The Australian Government could support Pacific governments and businesses by creating simple information resources such as an up-to-date, comprehensive, and publicly accessible repository of relevant investment programs by the Australian and other governments.
- Future Australian-funded cyber training programs should seek to expand to upskilling key, strategically important segments of Pacific Island countries' (PIC) workforces that will improve the overall digital literacy of Pacific societies. This could include creating incentives for businesses operating in the region to invest in their workforce cyber education.
- Future support by Australia and its regional partners to PICs could focus on establishing consistent, better coordinated preparedness planning that incorporates cyber security considerations as a standard feature of good planning. Such plans could also be informed by input from private and other non-government organisations that are likely to be involved in aiding the cyber components of national and multi-national Humanitarian & Disaster Response (HADR) operations.
- The Australian government should prioritise efforts to better understand the deployable cyber support resources available across partner governments and the private sector. This improved understanding could allow for swifter mobilisation of HADR cyber units in a manner that is simultaneously better for response readiness and less impactful on Australia's own operational continuity.
- Australian government planning and programs need to regard improving cyber security as a key vector for accelerating economic equality in PICs.
- Australian and other states' infrastructure investment programs need to remove barriers to investing in cyber infrastructure, such as data centres, which will deepen PIC's digital resilience and improve their capacity for data sovereignty.

## The Technology & Communications Industry in the Pacific: Barriers & Opportunities

Pacific Island Countries (PICs) do not yet enjoy the widespread, reliable, and affordable access to high-speed internet connectivity that advanced economies like Australia enjoys. This is primarily due to the absence of enabling infrastructure operating at-scale across this large maritime region. The effect is that digital literacy is highly varied in PICs, with those living outside capital cities having far less knowledge of, and access to, digital services than their urban peers.

However, the investments that are being made in new Pacific digital infrastructure are achieving rapid and impressive transformations. Coming off a low base of connectivity means the lives of those in remote Pacific islands are being rapidly improved when new services and infrastructure are being established. For example, CyberCX has supported clients in the region to adopt remote access and virtual desktop infrastructure (VDI). In some instances, this has eliminated the need for staff to spend several days travelling between remote islands to provide services.

Improved connectivity across historically prohibitive geographic barriers holds the prospect of overcoming asymmetries in information and commercial services (like secure banking) that have long limited economic growth and diversification for many communities. Agriculture, fisheries and minerals extraction are likely to be the primary drivers of economic growth for much of the region for the foreseeable future. Improved connectivity has the capacity to mitigate workforce and other limitations affecting these industries as automation in these sectors becomes more viable.

Improving Internet connectivity and the growth of digital economies across the Pacific region is nevertheless dependent on largescale investment in several categories of telecommunications infrastructure, including: cellular base stations, data storage facilities, and undersea Internet cables. Australia has made important investments in this regard, including through recently underwriting Telstra's purchase of Digicel Pacific, the region's main mobile services provider. Others such as China, Japan, the United States, the European Union, France and India are also making significant contributions to the uplift of the region's infrastructure, both bilaterally and through multilateral groupings such as the Quad, the World Bank, the International Telecommunications Union, and the Asian Development Bank.

The multitude of bilateral and multilateral investment initiatives creates challenges for Pacific governments and businesses in the region to identify the opportunities available and how they might inter-relate. A greater strategic approach to directing digital infrastructure investment into the Pacific is required. Such an approach will become especially important as the technology mix in the region becomes more complex, for example with the roll-out of next generation broadband Internet, supported by terrestrial and satellite infrastructure. The Australian Government could support Pacific governments and businesses by creating simple information resources such as an up-to-date, comprehensive, and publicly accessible repository of relevant investment programs by the Australian and other governments. Such resources will also help PIC government entities and businesses operating in the region navigate the persistent geopolitical competition between the PRC and the West that is manifesting as a race to establish the dominant technology norms and systems that will determine the region's future.

In addition to infrastructure, the availability of foundational digital skills and qualifications will remain a persistent challenge. This has been recognised by the Australian Government which has

for several years now supported cyber skilling programs delivered by both university and business partners. However, these programs have primarily focused on addressing urgent skills gaps within PIC government agencies and departments. Future programs should seek to expand to upskilling key, strategically important segments of the PIC workforce that will overtime improve the overall digital literacy of Pacific societies. This could include creating incentives for businesses operating in the region to invest in their workforce cyber education.

## The Threat Environment

PICs each have their own unique digital ecosystem, which means cyber security vulnerabilities and threats vary greatly depending on context. Cyber security incidents can have enduring impacts on developing countries' journey to self-reliance, and can exacerbate political, social, and economic instability. For example, high-profile cyber attacks can undermine the legitimacy of governments by highlighting their inability to protect their citizens from harm. Critical infrastructure networks in particular are attractive targets for malicious state and non-state actors.

Exacerbated by the borderless nature of the cyber domain, developing states face an increasingly complex environment in which malicious actors are regularly outpacing the ability of many states to respond. State actors are aggressively using advanced cyber capabilities to pursue objectives that do not align with agreed upon international laws and norms. State actors are continuing to target government entities, critical infrastructure, and businesses. This includes infiltrating connected systems and supply chains for cyber espionage and information gathering purposes. State actors have also been identified using cyber capabilities to disrupt systems and critical infrastructure and preposition on networks for future malicious activities.

Conflicts in Europe and the Middle East are generating sustained cyber instability as actors seek to gain an advantage outside of the kinetic environment. The governments of China, Russia, Iran, and North Korea are increasingly undertaking malicious actions in cyberspace creating destabilising environment globally. In May 2023 the United States along with its international partners released a joint advisory on a cyber espionage tool used by Russia's Federal Security Service (FSB) for long-term intelligence collection on sensitive and high-priority targets around the globe. In the same month, a joint cyber security advisory from international partners was released outlining malicious cyber activity associated with a People's Republic of China (PRC) state-sponsored cyber actor. Regional dynamics in the Indo-Pacific are increasing the risk of cyber operations being used by both state and non-state actors to challenge the sovereignty of others. Grey zone activities, including cyber espionage, information operations, subversion, cyber theft, and cyber attacks will continue to be pursued by state actors of varying sophistication.

Cyber criminals pose a threat to national security and the economic prosperity of states across the globe, but especially developing states such as those in the Pacific who's baseline level of institutional resilience is lower. The proliferation of cybercrime-as-a-service has enabled comparatively unskilled actors to leverage sophisticated tools for malicious intent. This has resulted in the proliferation of tools such as ransomware, phishing, Business Email Compromise (BEC), Identity theft, Denial of Service (DoS) and Distributed Denial of Service (DoS). Global conflicts such as the war in Ukraine and the Gaza conflict has seen the emergence of highly disruptive hacktivist criminal groups that are motivated by ideology rather than financial gain. These actors

are typically less capable and poorly resourced however can cause significant harm, reputational damage, and operational disruptions to impacted entities.

Many countries have already been significantly impacted by cyber security attacks. Papua New Guinea's Department of Finance's Payment System suffered a Ransomware attack in 2021. Similarly, in March 2022 the Republic of Marshall Islands' National Telecommunications Authority experienced a major distributed denial of service (DDoS) cyber attack that disrupted internet services for about 10 days. The entire Government of Vanuatu was essentially offline brought offline in 2022 due to a cyber attack. This non exhaustive snapshot of cyber security incidents depicts realised threats that developing countries face.

Cybercriminals and state-backed actors are not limited by and do not respect borders. A significant cyber security incident in one country can have unexpected ripple effects across the region and the globe. The interconnected and global cyber security ecosystem is only as secure as its weakest links. By ensuring that systems and networks abroad are secure, countries increase their own protection.

## Digital Resilience and Humanitarian Assistance & Disaster Response (HADR)

When the right skills and tools are available, cyber security is a transformative enabler of a nation's wider economic prosperity and national security. Conversely, the absence of sufficient cyber security protections can undermine a society's digital resilience and exacerbate the harmful impacts of other crises.

For many Pacific Island countries (PICs), poor digital resilience to cyber threats risks hampering Humanitarian Assistance & Disaster Response (HADR) operations as well as long term recovery efforts. CyberCX assesses that profit-motivated threat actors will continue to exploit crises as opportunities to extort governments, businesses, and relief organisations, especially via ransomware attacks. In the context of the region's enduring geopolitical competition. CyberCX also expects that state and state-backed actors will continue to look to capitalise upon environmental disasters and humanitarian crises as opportunities to disrupt and shape the internal politics of Pacific states, including via cyber espionage or cyber-enabled information operations.

As the reliance of PICs on digital systems grow over time, the Australian Government may wish to evaluate whether a widespread cyberattack in and of itself could constitute a humanitarian disaster, especially if it threatens lives by depriving access to essential services.

The consequence of Pacific states having limited sovereign cyber capabilities during times of humanitarian or environmental crisis is that Australia's HADR operations will consistently require dedicated cyber security contingents that can enable front-line relief and stabilisation activities in the face of a hostile cyber environment. This will put pressure on other core cyber responsibilities of the Australian government and potentially risk generating challenging concurrency pressures should critical cyber incidents simultaneously arise at home.

CyberCX sees two elements to addressing this challenge. Firstly, there is the need for PICs to have access to improved digital preparedness planning and capabilities prior to humanitarian and environmental incidents occurring. Secondly, the Australian government alongside other partner

states needs to ensure cyber security support teams and technical resources are reliably available for deployment when incidents arise that exceed local capacities. These two elements should be incorporated into future programs by Australia and partner states to improve Pacific resilience to humanitarian and environmental disasters.

- **Improving Preparedness and Pacific Capabilities.** CyberCX's experience indicates that preparedness planning within PIC governments for HADR operations is limited and does not consistently incorporate cyber security considerations. Future support by Australia and its regional partners to PICs could focus on establishing consistent, better coordinated preparedness planning that incorporates cyber security considerations as a standard feature of good planning. Such plans could also be informed by input from private and other non-government organisations that are likely to be involved in aiding the cyber components of national and multi-national HADR operations.
- **Improving Reliability and Availability of Deployable Cyber Support.** HADR operations naturally focus in the first instance on mobilising and deploying medical and emergency services alongside peace and law enforcement personnel. However, deployable and remote cyber security teams will need to be more frequently mobilised as part of this initial HADR contingent. The Australian government could therefore prioritise efforts to understand the deployable units available across partner governments and the private sector. This improved understanding could allow for swifter mobilisation of HADR cyber units in manner that is simultaneously better for response readiness and less impactful on Australia's operational continuity. DFAT has committed $26.2 million to establishing Cyber Rapid Assistance for Pacific Incidents and Disasters (RAPID) teams comprising Australian private sector and government specialists led by DFAT. CyberCX believes Cyber RAPID has already made a significant impact and is a model to follow for the creation of a multinational approach to deployable cyber support.

## Cyber Security as an Enabler of Equitable Economic Development

Cyber security is critical for the economic development of all countries, but especially pivotal to those such as PICs that are seeking to reduce poverty and inequality while seeking to move up the value chain of the global economy. For developing nations, robust cyber security measures can stimulate economic growth by reassuring foreign investors and driving diversification. Improved cyber security can also foster a degree of economic equality that boosts productivity and societal resilience. By safeguarding digital infrastructure, common cyber security measures can create a more secure environment conducive to business operations, innovation, and equitable access to economic opportunities.

Improved cyber security can enhance economic development for PICs by: protecting financial transactions, supporting the attraction of foreign investment, enabling digital transformation of key services, fostering entrepreneurialism, and reducing the cost of cyber incidents.

- **Protecting Financial Transactions.** In PICs, safeguarding financial transactions through cyber security is vital in order to build trust in digital systems and protect individuals and businesses from theft and extortion. The digital economy in these countries is growing, with online banking and mobile money services being steadily adopted. Measures, such as encryption and introducing secure payment gateways, can help protect these transactions from fraud and cyber-attacks. This protection should boost consumer confidence,

encouraging more people to engage in the digital economy, which in turn drives economic growth.

- **Reassuring Foreign Investors.** Robust cyber security frameworks can make PICs more attractive to foreign investors. Investors prefer regions with strong cyber security to avoid the risks associated with data breaches and financial losses. With strong potential in the mining, fisheries, and agricultural sectors, the Pacific has some fundamental characteristics to support new lucrative economic growth. However, readiness to invest in these economic opportunities has historically been stifled by concerns sovereign risk concerns relating to political and institutional instability as well as under-developed security protections, including cyber security. By implementing more advanced cyber security measures, PICs can improve their reputation as secure investment destinations. This could lead to increased foreign direct investment (FDI), which is critical for economic development as it brings capital, technology, and expertise.
- **Enabling Digital Transformation and Entrepreneurship.** The wider application of baseline cyber security measures will be essential for supporting the digital transformation of Pacific states. Digitalisation can improve efficiency and productivity in sectors such as healthcare, education, and within government. However, applying smarter digital tools to these sectors will inherently attract cyber threats. If partner states can assist PICs to secure enabling digital infrastructure, these states will be better placed to support the ongoing digitisation of critical services. Such digital transformation could result in significant economic benefits, including cost reduction to PICs and donor states as well as enhanced service delivery for individuals, households, and businesses. Over time, the emergence of a more secure digital economy in PICs will help protect small businesses and entrepreneurs who will be vital to economic diversification in PICs.

Improving basic cyber hygiene and access to standard cyber security protections has a real capacity to improve economic equality in developing Pacific states by removing barriers to digital services, protecting vulnerable groups, improving access to key skills, and creating new jobs.

- **Overcoming the Digital Divide.** Cyber security measures can help overcome barriers to participation in the digital economy in PICs by ensuring equitable and reliable access to digital services. In many Pacific Island communities, especially in rural areas, there is limited access to secure and reliable Internet connectivity and digital services. By focusing on supporting rural and regional areas to access secure Internet services, governments can provide equitable access to education, healthcare, and financial support. This access can improve the quality of life for marginalized populations, reducing endemic economic equality.
- **Protecting Vulnerable Populations.** Cyber security is crucial for protecting vulnerable populations from exploitation, and the impact of significant attacks against critical infrastructure. Disruptions to essential services are more likely to affect disabled people and 'hack and leak' attacks targeting the healthcare or justice system could result in discrimination against impacted individuals and groups. Women, children, and minority groups (such as ethnic and religious minorities) are also often directly targeted by cybercriminals who can be profit motivated, but also motivated to intimidate or coerce groups they see as politically or socially unaligned. Supporting critical infrastructure protection and introducing marginalised groups to methods for interacting safely online

can help safeguard vulnerable people from online harassment, exploitation, identity theft, fraud, and intimidation.

- **Enabling Digital Literacy and Skills Development.** Investment by Australia and other partner states in cyber security needs to continue to heavily focus on enhancing digital literacy and skills among the population. Digital literacy programs can teach citizens how to protect themselves online, recognize cyber threats such as phishing attacks, and use digital tools safely. By helping PICs provide equal opportunities for digital education, citizens can be empowered to take advantage of economic opportunities, reducing inequality.
- **Creating New Job Opportunities.** The cyber security sector itself should be able to create new employment opportunities in PICs as the region's digital economy expands. There will be government and private sector jobs associated with education, cyber security training programs, law enforcement and other cyber initiatives targeting the wider population. Overtime, higher cyber literacy could foster an affordable digital workforce that can help grow Pacific economies by attracting companies looking to outsource parts of their operations.

## Assessment of Relevant Government Initiatives

CyberCX has partnered with the Australian Government and Pacific governments on a range of initiatives to bolster the cyber security preparedness of the PICs. We have therefore developed some insight into the existing Australian and other programs seeking to support Pacific cyber security uplift. In selecting the initiatives we have participated in, CyberCX has used the principles of value-for-money, effectiveness, and need to triage which projects we direct our resources to. CyberCX suggests these are useful principles for others to follow when assessing which projects to support.

The Cyber and Critical Tech Cooperation Program (CCTCP) was established in 2016 and is the Department of Foreign Affairs and Trade's (DFAT) primary means of providing cyber security uplift and assistance to Pacific nations. Grants delivered under the program have supported a range of private enterprises, academic institutions, and multilateral bodies from Australia and the region to deliver cyber and tech related projects across the Indo-Pacific region. This program, however, means that Pacific projects have to compete for limited resources with projects targeting other sub-regions such as South East Asia.

The Cyber Rapid Assistance for Pacific Incidents and Disasters (RAPID) Teams allows DFAT to provide incident response and crisis support upon request from Pacific Nations. CyberCX believes that the RAPID program is an effective way to provide tangible and high value interventions into the Pacific. Integrating DFAT staff, government representatives, and specialist support from the private sector allows RAPID teams to provide comprehensive and direct support to Pacific Nations. CyberCX suggests that the RAPID be coordinated with other donor cyber security programs and DFAT's broader development program to ensure the incident response support is accompanied by targeted and mutually beneficial technical capability uplift activities. Doing so will reduce stakeholder fatigue while ensuring lasting long-term improvements to the cyber security maturity of nations in the Pacific.

DFAT has also provided $16.7m for the Modernisation and Secure by Design Solutions program in the Pacific. This program identifies issues and vulnerabilities in legacy software and hardware that

DFAT can pay to be upgraded. This program has helped to build long term resilience in the Pacific by working with partners to proactively identify vulnerabilities – such as end-of-life hardware and software – and trial secure by design solutions that reduce cyber incidents. The Australian Government is working with regional governments and technical community partners to pilot options to use technology to protect the region at scale. The Australian cyber security and telecommunications sector can help leverage industry solutions to protect more people, systems and data from cyber threats.

There are a wide range of infrastructure investment programs targeting the Pacific. Australia's main vehicle for this is the Australian Infrastructure Financing Facility for the Pacific (AIFFP). This $3 billion facility focuses on investment in energy, water, transport, and telecommunications infrastructure, with a significant overarching commitment to investments that also address climate change. Unfortunately, the facility has some mechanisms that limit its ability to support projects that bolster the region's cyber security. For example, it is not currently possible for the facility to direct investment into constructing data centres or migration to cloud-based solutions. This is despite data centres being an essential piece of infrastructure for support the adoption of artificial intelligence, for establishing digital resilience, and improving data sovereignty. The Australian Government and other investment partners to the region should ensure that the investment programs they have established adequately allow for the development of digital infrastructure that will enhance the resilience of digital infrastructure and ability to restore digital services when facing both cyber and environmental harms.

## Conclusion

This inquiry represents an opportunity to explore policy options that capitalise on the critical role digital infrastructure and cyber security can play in driving the Pacific's economic development, societal resilience, and equality. By investing in the region's digital infrastructure, improving cyber literacy, and providing secure online environments for vulnerable communities, Pacific Island countries can overcome significant barriers to economic growth and social inclusion. Calibrated appropriately, and in a coordinated way with partner states, Australia's strategic investments and partnerships in these areas can more effectively support the region's digital and socio-economic transformation. To sustain and amplify these efforts, a coordinated approach involving international collaboration, enhanced regulatory frameworks, and continued investment in cyber resilience will be essential. A holistic multilateral strategy will not only bolster the economic prospects of Pacific Island nations but also contribute to regional stability and prosperity in the face of current geopolitical competition playing out in the technology domain.