

Submission to the Enquiry into Australia's overseas aid and development assistance program

Key Recommendations

1. The online digital environment needs to be recognised as a cross-cutting aid issue which can provide positive outcomes across multiple aid sectors.
2. Assisting South East Asian and Pacific Island economies to take advantage of the global internet society and economy will multiply the benefits of existing sectoral based aid programs.
3. Providing development assistance focused on e-governance, e-commerce and e-education will reduce poverty and promote prosperity and stability within our region.
4. It is in Australia's national security interest to assist our regional aid recipients to use cyber security and cyber safety best-practise tools and techniques.

Background

The *Centre for Internet Safety* applauds the government's desire to reduce poverty and promote prosperity and stability within our region, particularly through the achievement of the Millennium Development Goals. However the Centre also believes these pursuits could be more easily accomplished if the government's aid program directed some resources to assisting the safe and secure uptake of the digital environment by aid recipient governments, businesses and civil society. Such opportunities, already enjoyed by developed nations, can assist many South East Asian and Pacific Islands economies to achieve better social outcomes.

The world is becoming increasingly interconnected: governments are seeking efficiencies in service delivery; markets are expanding; people are more mobile; the transfer of resources, finance and ideas is increasing; business is becoming more international; and developing countries are adopting more market-friendly policies which give the private sector greater scope.ⁱ Many of these initiatives are harnessed through the internet and mobile telephony (including the use of the internet via mobile phones and smart devices). Developing nations in South East Asia and the Pacific Islands are now online and while there are many benefits achievable from this, if not done correctly, there are also many pitfalls.

As Australia plays a central role in the South Pacific, we will need to continue to be a source of economic, diplomatic and, if necessary, military support.ⁱⁱ

The internet is widely regarded as a critical piece of a nation's infrastructure. The development and maintenance of this essential piece of public infrastructure is an important ingredient for sustained economic growth and poverty reduction.

About the Authors

Alastair MacGibbon is an internationally-respected authority on cybercrime, including Internet fraud, consumer victimisation and a range of Internet security and safety issues. For almost 5 years Alastair headed Trust & Safety at eBay Australia and later eBay Asia Pacific. He was a Federal Agent with the Australian Federal Police for 15 years, his final assignment as the founding Director of the Australian High Tech Crime Centre.

Nigel Phair is an influential analyst on the intersection of technology, crime and society. He has published two acclaimed books on the international impact of cybercrime, is a regular media commentator and provides executive advice on cyber security issues. In a 21 year career with the Australian Federal Police he achieved the rank of Detective Superintendent and headed up investigations at the Australian High Tech Crime Centre for four years.

About the Centre for Internet Safety

The Centre for Internet Safety at the University of Canberra was created to foster a safer, more trusted Internet by providing thought leadership and policy advice on the social, legal, political and economic impacts of cybercrime and threats to cyber security.

The Centre for Internet Safety is hosted within the Faculty of Law at the University of Canberra. The University of Canberra is Australia's capital university and focuses on preparing students for a successful and rewarding career.

www.canberra.edu.au/cis

No country has significantly reduced poverty without competent governance and sustained economic growth. The ability for Governments in South East Asia and the Pacific Islands to deliver internal and external services via the online environment can produce improved benefits for the population, provide greater transparency in decision making, improve governance arrangements and improve the economic growth of the region.

However, without proper security, regulation, policy and privacy arrangements in place, the gains from building an online economy, through the provision of new businesses, services and the physical infrastructure, will provide little benefit to their citizens, communities and economies. Rather, the online information and service economy will simply provide a vector for (predominantly overseas based) cyber criminals to prosper at their expense with relative impunity. Indeed, the harm to their citizens, communities and economies, could be more far-reaching and serious than many realise.

Discussion

The internet represents one of the most successful examples of the benefits of sustained investment and commitment to research and development of information infrastructure. Governmental use of IT systems can improve the activities of public sector organisations through e-government initiatives. Principally, e-government can improve government processes, connect citizens and improve relationships with institutions. Successful governance can mean better delivery of health, education and other services, stronger and more equitable economic growth, stability and security, and a population that has an open and responsive government.

Internet access in Melanesia, Micronesia and Polynesia is on the rise. That's a good thing, but there are gaps in governance. It would be in Australia's interests, and those of our friends and neighbours to help.ⁱⁱⁱ

Governance is about the network of institutions. Securing the IT infrastructure of Pacific governments and developing a range of e-government projects which will enhance governmental investment in IT systems and processes will improve governance in developing countries to deliver services, improve security, and enhance justice and human rights for marginalised people.

It is cross-cutting in nature and addresses the development themes including infrastructure and urban development, private sector development, education, health, gender equality, law and justice, governance, civil society and humanitarian and emergency assistance.^{iv}

The Asian Development Bank has concluded introducing IT systems cannot substitute good public management and internal controls. However, implemented in concert, the Bank argues IT systems can improve the efficiency and effectiveness of government. Further, the introduction of ICT can reduce corruption by better enforcing rules, reducing discretion of officials, and increasing transparency. It can support self-organising networks, which are increasingly important in governing industrial democracies.^v ICT applications support participatory and democratic processes in the Pacific through applications that empower civil society organisations; allowing citizens to express opinions over the Internet; reducing transaction costs; and increasing transparency.

The development of ICT practises for Pacific Island governments, business and civil-society will allow them to engage nationally and internationally. Countries that have engaged with the global economy have grown more quickly than those that have not.^{vi} Additionally, States that have invested in the health and education of their people have been more successful than those that have not.^{vii}

Threats

When combined with increased deregulation and trade, new communications technologies have provided a huge boost to transnational crime, facilitating money laundering, the smuggling of drugs, people and weapons,^{viii} and intellectual property theft.

Just like Australia, South East Asian and Pacific Island nations are not immune from international organised crime groups and other actors seeking profit, corporate proprietary information or the revelation of government secrets. Indeed, Pacific governments could be seen as a soft target to gain information, not just about their own affairs, but also their communication with other sovereign governments.

Also like Australia, each South East Asian and Pacific Island nation has its own Top Level Domain name giving it influence yet requiring prudence in its management and that of lower-level domains subsequently administered. Indeed, as the Pacific Islands have been previously targeted as havens for money laundering and as transit points for large-scale narcotic importation, they are susceptible to electronic attacks from criminals or rogue states. The Top Level Domains of many nations are favoured by criminals, further damaging the level of trust in legitimate business and government activities in those countries.

The global online threat environment continues to grow. There are many and varied vectors and the borderless nature of the internet makes detecting, investigating and prosecuting individuals extremely difficult. Such criminal activity includes hacking, malicious software, website defacing, intellectual property theft, fraud and most importantly identity theft. Such attacks can occur from external users, but also from insiders.

These threats can have very real and personalised consequences. Smart phones connected to the internet has allowed the Pacific Islands to embrace mobile payment systems, an industry that has grown exponentially elsewhere in the developing world (Africa is the leading example and provides a useful guide as to how Pacific island use of mobile technologies will evolve).

The distance of the Pacific Islands from centres of economic density sees many Pacific Islanders migrating for long periods to work in large countries abroad, sending cash remittances on a regular basis that are the equivalent of much as 30% of GDP in some Islands, including 77% of Tongan families relying on these transfers. The high cost of remitting funds has repeatedly been identified as a major detriment to the people and countries in the Pacific that are dependent on such funds.^{ix} Cyber criminals target these payments and the people utilising them, through a combination of technical expertise and social engineering.

National Interest

It is in Australia's national interest for South East Asian and Pacific Island government computer systems to be robust and secure. A compromise of a governmental computer system will effect economic growth and trade, reduce governmental stabilisation, make them more prone to radicalisation, and become more susceptible to the influence of countries and ideas, possibly at odds with Australia's interests.

Cyber intrusions can take a number of forms and directly relate to national security. Such compromises include stealing information or damaging information or systems. Key threats which may impact on Australia's national interest include:

- Cyber 'hacktivists' (including politically-motivated groups);
- Cyber criminals, ranging from individuals to sophisticated organised crime groups, and
- The intelligence and security agencies of nation states that might carry out cyber espionage (targeting information held in Government and corporate networks) or cyber warfare (warlike conflict that primarily involves information technology means).

In the developing world, foreign direct investment as a whole may eventually be affected by the safety and integrity of data networks available to investors in host countries. In advanced industrial nations, basic public trust in modern economies and the electronic networks on which they depend is eroded when electronic data is stolen, becomes corrupted, or can no longer be authenticated.^x

To achieve an effective aid program, Australia needs to understand current trends and emerging challenges to prepare for the future.

Australia has an enduring interest in capacity building in South Pacific nations. Helping them to develop a robust internet backbone and the ability to deal with unlawful and malicious online behaviour is a natural extension of our other activities. It's not as obvious as other activities, but it's no less important.^{xi}

ⁱ Independent Review of Aid Effectiveness. (April 2011) p13

ⁱⁱ Defence White Paper. (2013), p15
http://www.defence.gov.au/WhitePaper2013/docs/WP_2013_web.pdf

ⁱⁱⁱ ASPI. Cyber in the Pacific Islands.
<http://www.aspistrategist.org.au/cyber-in-the-pacific-islands/>

^{iv} Above, n1, Independent Review of Aid Effectiveness, p19.

^v See
<http://www.adb.org/Documents/Papers/E-Government/egov-asiapac.pdf> for further detail.

^{vi} AusAID. An Effective Aid Program, p13.

^{vii} *ibid*, p 14.

^{viii} Lowy Institute. Study of the Future State of the World as it Relates to the Australian Program (2010)

^{ix} Horscroft, V. An Eye on East Asia and the Pacific. The World Bank (2010)

^x World Bank.
<http://siteresources.worldbank.org/EXTINFORMATIONANDCOMMUNICATIONANDTECHNOLOGIES/Resources/CyberSecurity.pdf>

^{xi} ASPI, above n3