www.diplomacy.edu

Cybersecurity in the Republic of Fiji

Salanieta Tamanikaiwaimaro

Abstract

Cybersecurity is a critical area that affects virtually everyone from governments, countries, organisations, multinationals, supermarkets, grocers, factories, schools, and individuals whose livelihood may depend on critical infrastructure or who use the Internet. Internet use ranges from pretty basic use, such as e-mails, to commercial transactions, such as Internet banking, shopping, or trading, to broadcasting content on social utility sites such as Twitter or commercial sports channels, etc. The cyber-environment is not limited to computers but covers all aspects of information and communications technology (ICT), including networks and infrastructure. The vulnerability of systems due to lack of a cybersecurity framework, poorly framed laws, and lack of appropriate policies are issues which need to be addressed. Whilst ICT is an enabler for economic growth, the illicit use of ICTs can also stunt growth. This paper discusses the challenges of cybersecurity in Fiji and offers recommendations. This is preliminary research, and it is envisaged that there will be other research papers to follow.

Keywords: cybersecurity; Fiji, cyber-environment; ICT challenges

Introduction

Cybersecurity affects everyone from national governments, the public sector, the private sector, and ordinary citizens in a country. It is important that small island developing states seek to understand it.

Fiji, as a small island developing state[1] is also categorised by the International Monetary Fund (IMF) as an emerging and developing economy (IMF, 2010). Fiji faces numerous development challenges (UN, 2010). Some of these challenges include managing resource constraints and the manner in which resources are prioritised. Perhaps because cybersecurity is a relatively new phenomenon, it has yet to be addressed by having national strategies and policies put in place.

For emerging economies that are dealing with issues hot on the agenda, such as energy and climate change, ICT often tends to take the backburner. This paper is intended to create awareness for policy writers and stakeholders.

Effective strategy is needed to efficiently manage cybersecurity in Fiji, a country which is essentially playing catch-up; other regions are more advanced in their cyber-infrastructure. For example, in 2009, the European Commission (EC) launched a draft strategy designed to protect Europe's critical information infrastructure from large-scale cyber-attacks (Barker, 2009).

Cybersecurity: a growing concern

The increased availability and use of computers in Fiji has led to a corresponding growth in international data transmission requirements (Fintel, 2011).

Pacific Island countries are vulnerable to common cyber-attacks seen around the globe, which include phishing, secure shell (SSH) brute force attacks, malicious software (malware), and telephone number hijacking. As an example, telephone number hijacking has been known to cause disruption in the Cook Islands Public Switch Telephony Network (PSTN), where they estimated losses of over USD$100 000 in just four hours (Tabureguci, 2007). The Republic of

[1] As described by the Permanent Mission of Fiji to the United States, 2010.

This document has been produced by DiploFoundation with the financial assistance of the European Union. The contents of this document are the sole responsibility of the author and can under no circumstances be regarded as reflecting the position of the European Union or DiploFoundation.

Marshall Islands also suffered a severe denial of service attack, which lasted for two days (Tabureguci, 2007).

The International Telecommunications Union (ITU), through its Telecommunications Standardisation Section (ITU-T), developed a definition of cybersecurity within its *ITU-T Recommendation X.1205* (Overview of Cyber Security). Clause 3.2.5 of *ITU-T Recommendation X.1205* defines cybersecurity as 'the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organisation and users' assets' (ITU, 2008).

Objectives of cybersecurity

The principal objective of cybersecurity is to ensure the 'attainment and maintenance of security properties of the organisation and user's assets against relevant security risks in the cyber environment' (ITU, 2008).

The ITU has defined the general security objectives to include:

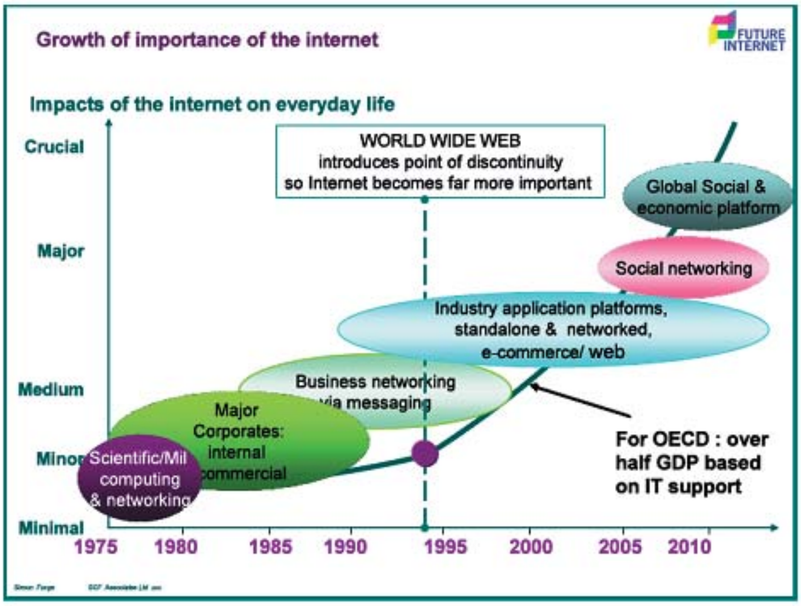
- *Availability*
- *Integrity*[2] *which may include authenticity and non-repudiation*
- *Confidentiality* (ITU, 2008, clause. 3.2.5)

These security objectives are critical as trade and commerce depends on them. For example, bank customers rely on and trust that banks have security mechanisms in place to protect their savings. These customers rely on the availability of systems and infrastructure within the cyber-environment to allow them to transact freely. Customers also rely on banks to have systems in place that will preserve data integrity, whether in the form of identity authentication or having the requisite means to verify a person's identification. Customers also rely on the confidentiality of the systems to keep their transactions confidential.

Increasing dependence on the Internet

It is clear from Figure 1 that there has been an increasing dependency on the Internet over the years. Social networking sites (SNS) and plat-

Figure 1. Increasing dependence on the Internet



Source: Towards a Future Internet (2010)

Figure 1. Illustration showing increasing dependence on the Internet (Sommer and Brown, 2011).

[2] Data Integrity is defined to be data that is not altered in an unauthorised manner in research on legislation in data privacy, security, and prevention of cybercrime.

forms like Facebook (Barratt, 2010) are realising that their personal information, furnished for what subscribers believe to be for 'limited purpose', has been abused, hijacked, misused, repackaged, sold and laid bare to the world (Garrie *et al.*, 2009). One cannot discuss cybersecurity without knowing what aspect of the cyber-environment needs to be secure.

The cyber-environment includes users, networks, devices, all software, processes, information in storage or transit, applications, services, and systems that can be connected directly or indirectly to networks (ITU, 2008, clause 3.2.4). The cyber-environment is related to the Internet access architecture: it does not exist in isolation.

Internet access architecture in Fiji

The Internet access architecture refers to the means within which Internet is accessed in Fiji. Fiji International Telecommunications Limited (FINTEL) and Telecom Fiji Limited (TFL) provide Internet access through connections to Southern Cross Cable. FINTEL provides connection to other Internet transit providers (ISPs).

The principal facilities-based competitors offering broadband Internet access are (Fong, 2010):

- Connect (TFL's ISP) – provides broadband services through ADSL and a combination of 2.5G, 3G wireless and a VSAT as last resort.
- Kidanet (a fully owned subsidiary of FINTEL) – provides wireless broadband services through WIMAX.
- Unwired – provides wireless broadband services through WIMAX.
- Vodafone – provides wireless broadband services through GPRS and HSDPA.
- Digicel – provides wireless broadband services using EDGE; however, they have been allocated WIMAX spectrum and are considering WIMAX deployment.

There are at least seven principal ISPs in Fiji. Customers include individual users, businesses, banks, schools, universities, etc.

The Internet architecture does not exist in isolation; it exists within an ecosystem.

Internet ecosystem

The Internet ecosystem consists of licensed operators who provide backhaul capacity and Internet services, regulators, and other organisations who have a direct and indirect impact on the development of the Internet. The Internet ecosystem is made up of the organisations and communities that guide the operation and development of the

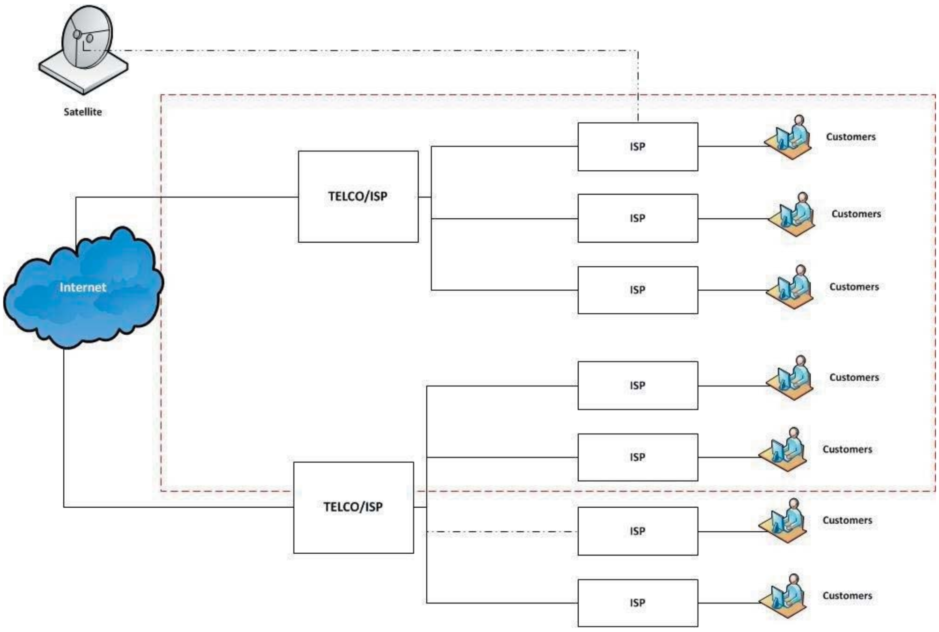


Figure 2. A basic physical diagram of how the Internet in Fiji is accessed by users.[3]

[3] ©Salanieta Tamanikaiwaimaro (2011)

technologies and infrastructure that comprise the global Internet (Internet Society, 2010).

The cyber environment in Fiji includes licensed operators, telecoms, as well as the ISPs, TAF, Commerce Commission, and other organisations and is linked to an Internet ecosystem. One of the challenges in Fiji is that there is not sufficient awareness amongst stakeholders within the cyber-environment of the stakeholders within the Internet ecosystem and how each relates to each other.

An organisation's and a user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunication systems, and the totality of transmitted and/or stored information in the cyber-environment (ITU, 2008). Cyber-attacks target different aspects of the cyber-environment. Sceptics may say that the Pacific Islands do not face cyber-attacks and threats and therefore do not need protection.

Protection from whom/what?

Cyber-attacks and threats vary and can be politically driven or criminally motivated as the following examples illustrate.

- *Arab – Israeli cyberwar*

Geopolitical wars between the Arab and Israeli governments have transcended into cyberspace. The Israeli defense community has been aware of cybersecurity threats for the past two decades (Day Press News, 2010).

- *Syria – Israel*

Unofficial reports by foreign experts allege that Israel attacked Syria through cyberwar operations. In September 2007, an attack was launched on a Syrian structure housing a nuclear weapons development programme. Air defenses were hacked and controlled by the Israelis during the attack. Part of the attack involved simulating that Syrian skies appeared empty and safe to air-defense radars whilst Israeli jets infiltrated the airspace.

- *Palestine – Israel*

The Israeli Defense Force (IDF) was involved in heavy fighting in Gaza around 2009 when there was an attack on Israel's Amos 3 spy satellite. It was subsequently discovered that the attacker transmitted modulated digital video broadcasting to Amos 3 and inserted a TV programme called 'Oassam'. The frequency used by the attacker was identified as the feed – channel of Arab-Sat, which normally transmits the Al-Aksa TV channel of Hamas.

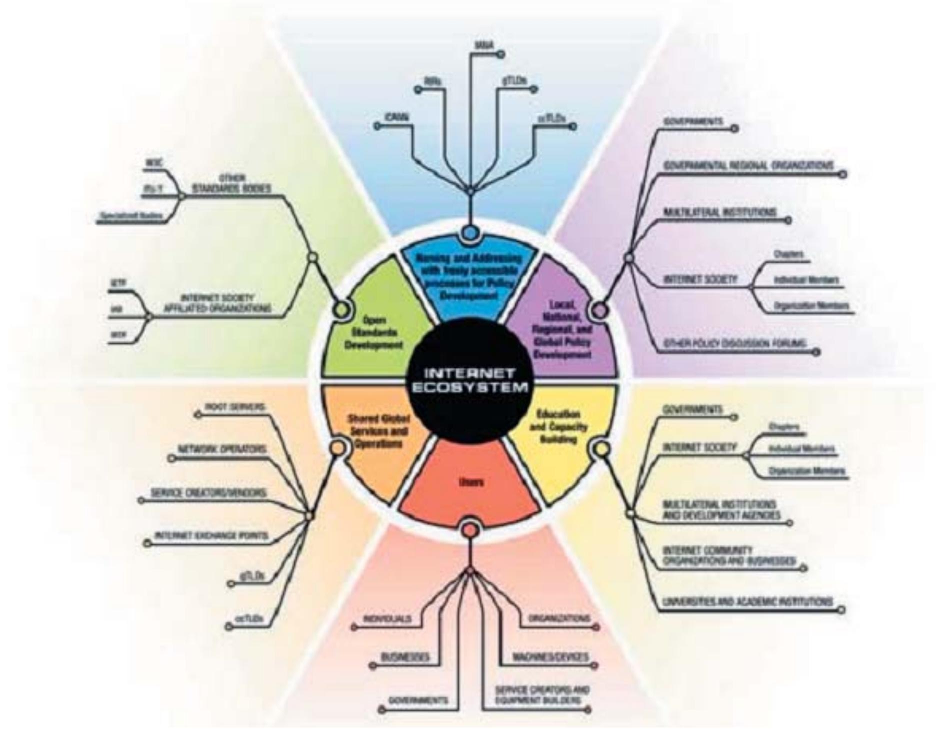

INTERNET ECOSYSTEM
Naming and Addressing with freely accessible processes for Policy Development
IANA
RIRs
gTLDs
ccTLDs
CANN
Local, National, Regional, and Global Policy Development
GOVERNMENTS
GOVERNMENTAL REGIONAL ORGANIZATIONS
MULTILATERAL INSTITUTIONS
INTERNET SOCIETY
Chapters
Individual Members
Organization Members
OTHER POLICY DISCUSSION FORUMS
Education and Capacity Building
GOVERNMENTS
INTERNET SOCIETY
Chapters
Individual Members
Organization Members
MULTILATERAL INSTITUTIONS AND DEVELOPMENT AGENCIES
INTERNET COMMUNITY ORGANIZATIONS AND BUSINESSES
UNIVERSITIES AND ACADEMIC INSTITUTIONS
Users
INDIVIDUALS
BUSINESSES
GOVERNMENTS
ORGANIZATIONS
MACHINES/DEVICES
SERVICE CREATORS AND EQUIPMENT BUILDERS
Shared Global Services and Operations
ROOT SERVERS
NETWORK OPERATORS
SERVICE CREATORS/VENDORS
INTERNET EXCHANGE POINTS
gTLDs
ccTLDs
Open Standards Development
OTHER STANDARDS BODIES
W3C
ITU-T
Specialized Bodies
INTERNET SOCIETY AFFILIATED ORGANIZATIONS
IETF
IAB
IRTF

Figure 3. The Internet Ecosystem (Internet Society, 2010).

- *Hezbollah – Israel*

Hezbollah guerillas hacked Israeli communication, during the 2006 second Lebanon war through monitoring and deciphering frequencies. This enabled the Hezbollah to intercept intelligence and thwart tank assaults. The Hezbollah was assisted by Iran's revolutionary guards. The successful decryption allowed the Hezbollah to have constant access to IRD's troop movements, casualty reports, and supply routes. Whilst there was no official comment by the IDF, it is reported that a former senior officer revealed that the Hezbollah's ability to hack into Israeli's military transmissions had disastrous consequences for Israeli's offensive (Day Press News, 2010).

- *Japan – South Korea*

The Japanese BBS 2 channel (BBS 2ch) is Japan's biggest Internet forum and a Japanese Internet phenomenon (Katayama, 2007). BBS 2ch was also reported to have celebrated the lynching of a Korean international student in Russia by Russian skinheads in February 2010 and a post was said to have recorded 'damn Korean who deserved to die' (inewp, 2010). There was a subsequent post on BBS 2ch that stated that Korean figure skater Kim Yu Na bribed the judges following the winter Olympics. This sparked a massive cyber-attack, which was launched on 1 March 2010 by Korean web users against the Japanese site. The date on which the attack occurred was the 91st anniversary of the independence movement. It is reported that 10 000 Korean users coordinated their attacks through South Korean web communities (Min Sun-Young, 2010).

- *Malaysia – Indonesia*

A fierce cyberwar between Malaysian and Indonesian hackers was sparked by the alleged mistreatment of an Indonesian model by a Malaysian royal. The attacks infiltrated Yahoo! messenger (YM) and attacked several Malaysian websites in 2009 (WorldFuture, 2009).

- *North Korea and South Korea and the USA*

In 2009, a malicious cyber-attack thought to be launched from North Korea targeted South Korean and US government computers over a two-day period, shutting down websites of the White House, the Pentagon, and the New York Stock Exchange.

- *The USA and China*

Another example includes the USA's spy plane incident in April 2001, where the escalating political tension between the USA and China led to attacks by USA and pro-Chinese hackers on important websites and mail servers of the opposing side during a period of several weeks (Dang, 2011).

- *Estonia and Russia: denial of service attacks*

Estonia faced a series of denial of service (DOS) attacks allegedly from Russia that began in April 2007. Since the Estonian government heavily relied on the Internet, this in turn crippled Estonia's banking systems and government, including telephone access to emergency services, as reported by Hillar Aarelaid, CSO for Estonia's Computer Emergency Response Team (Kirk, 2007). The North Atlantic Treaty Organisation (NATO) assisted them in tracking the source and origins of the attacks and said that analysts have found postings on web sites indicating that Russian hackers may have been involved in the attacks. According to Aarelaid, analysis of the malicious traffic showed that computers from the United States, Canada, Brazil, Vietnam, and others were used in the attacks.

- *Iran: stuxnet virus*

More recently, the United Nations General Assembly (GA) First Committee: Disarmament and International Security (DISEC) were informed at the ODUMUNC 2011 by Dang (2011) that the most recent cyber-attack was the detection of the Stuxnet[4] virus seen early in 2011, targeting Iran's nuclear facilities. Experts believe that the Stuxnet malware was very well funded and was designed by a country.

Organised criminals/cyber mafias

There are numerous reasons why profiling criminal organisations that operate over the

[4] Carefully designed malware that can infect computers and automatically look for a particular model of programmable logic controller made by Siemens to reprogram and even provide dangerous commands.

Internet can be difficult. Capturing data can be extremely difficult given that the Internet has no boundaries.

- *Wonderland Club*

The dissemination of child pornography online has been an unfortunate abuse of the Internet and ICT. An example was the Wonderland Club, an international network with members in at least 14 nations ranging from Europe, North America, and Australia. Access to the group was password protected, and contents were encrypted. Police investigation of the activity, codenamed Operation Cathedral resulted in approximately 100 arrests around the world and the seizure of over 100 000 images in September 1998.

- *Italian cybermafia*

Organised crime in Italy is fully utilizing the Internet for malicious activities from propaganda to money laundering (Cybernaut, 2010).

- *Russian and Brazillian cybermafia*

Portugal is known as a playground for international cybermafia who are operating and laundering their profits in Portugal. Russian and Brazilian crime rings that are experts at phishing to obtain private personal information have netted more than €2 million in 2010. Online banks and money transfer sites are the most targeted, particularly those used by immigrants from Eastern Europeans (PressEurop, 2010).

- *Japan disaster: target for cybermafias*

The recent Japanese earthquake and tsunami, where the death toll has surpassed the 10 000 mark, has made Japan vulnerable to cybermafia who seek to exploit the disaster through phishing, spam attacks, and search engine poisoning (rediff NEWS, 2011).

- *Republic of Marshall Islands*

On 25 March 2011, news from what appeared to be an authentic CBS website (www.cbsbreakingnews.com) spread news that the Republic of Marshall Islands had legalised cocaine. This was later found to be libellous and the Office of the President issued an official notice stating that this was a hoax (Office of the President Republic of the Marshall Islands, 2011).

Impact of cybersecurity on infrastructure, national security and economic development

With the rapid evolution of ICT in Fiji, growing Internet penetration and growing reliance on the Internet for commercial operations, trade, and health makes cybersecurity a matter of concern for the Republic of Fiji. Resolution GPL/1 reaffirmed the awareness that ICTs have significantly modified the ways in which people access telecommunications and that its illicit use of ICTs should have a detrimental impact on a member state's infrastructure, national security, and economic development (ITU, 2010).

The illicit use of ICTs can adversely affect Fiji's infrastructure, national security, and economic development. It is vital that there are necessary mechanisms in place that will address cybersecurity issues. Currently there are no legislative mechanisms in place in relation to the criminalisation of the illicit use of ICTs. However, the telecommunications promulgation 2008 creates an obligation for the telecommunications authority to have mechanisms in place to preserve national security.

Critical infrastructure (CI)

Nowadays, computers are interconnected in network infrastructures that satisfy customer needs. In Fiji, with the increasing trends of convergence of services and devices, such as short message services (SMS) banking, checking FNPF eligibility and so forth are part of services that usually belong to public and private companies that provide facilities to citizens, like banks and Telcos. In Fiji, the housing authority recently signed agreements with two telecommunications companies, giving customers flexibility in making loan repayments through their mobile phones (Baselala, 2011).

The ITU defines critical infrastructure (CI) as the key systems, services, and functions whose disruption or destruction would have a debilitating impact on public health and safety, commerce, and national security, or any combination of those matters. CI consists of both physical elements (such as facilities and buildings) and virtual elements (such as systems and data).[5]

Model 1. ITU-D STUDY GROUP 1 4th STUDY PERIOD (2006–2010)

Different countries have different definitions of what they would classify as critical infrastructure, whether they are ICT, banking, energy, public health, and essential government services. There is little understanding of the critical infrastructure dependencies and how this affects the internet architecture or vice versa.

Most governments consider the publication of critical infrastructure to be classified in case of attacks by terrorist groups, etc. Interestingly, Fiji is classified by the USA as 'critical infrastructure and key resources located aboard' due to Southern Cross Company Limited's (SCCLs) undersea cable that is connected to FINTEL (Fiji Times Online, 2010).

To appreciate an example of critical infrastructure interdependencies, see Figure 4 which shows how the infrastructure and industries are interrelated and how they affect each other. This will serve to show how when one is affected it can have a domino effect and impact other sectors.

Like the Dutch model, Fiji's infrastructure is dependent on the Internet. Banks, airports, energy, telecommunication, public health, and e-government are increasingly reliant and dependent on each other. Increasingly, customers in Fiji are given the opportunity to pay bills and loans with their phones and lately they even exercise the option of receiving their salaries through phones. With new waves of cybersecurity threats like smishing, where sms are hijacked, can also be cause for concern.

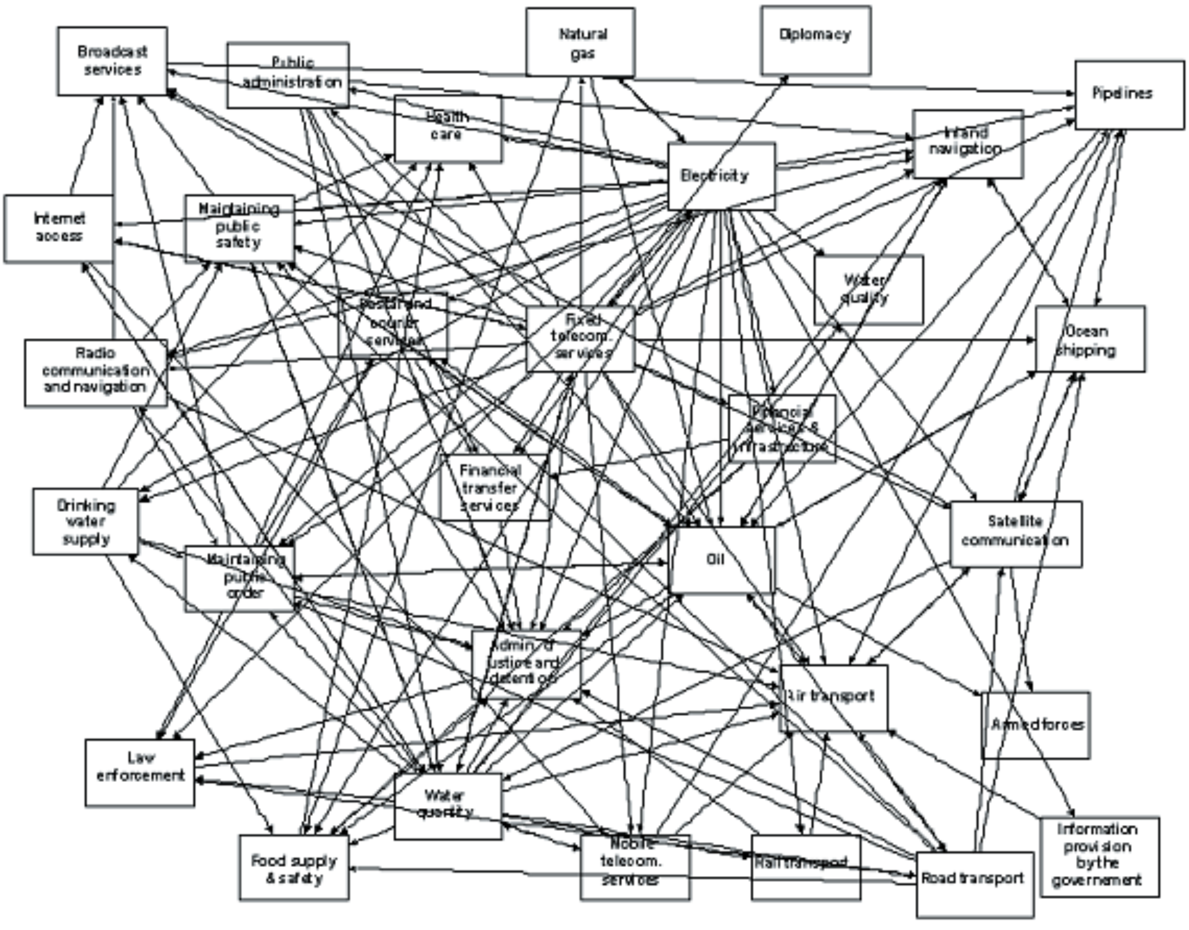


Figure 4. Critical infrastructure inter-dependencies (Luff, 2010).

[5] Question 22/1 Securing Information and Communication Networks: Best Practices for developing a culture of cyber security developed by ITU-D Study Group 1, 14th Study Period (2006-2010)

The Fiji Cyber Security Working Group is in the process of mapping these dependencies. Recently, a major international gateway provider within Fiji tempered with connectivity of another operator on 1 July 2011 and whilst this was a commercial dispute it impacted a wide range of industries. Whilst it was down for only three hours, flights were grounded, health services were disrupted, and banks and financial institutions were also affected.

The cyber-environment needs to have means in place that would protect the critical information infrastructure.

Critical information infrastructure protection (CIIP)

Europol defines critical information infrastructure as 'physical and IT facilities, networks, services and assets which if disrupted or destroyed, would have a serious impact on health, safety, security or economic we well-being of citizens or effective functioning of governments' (DGTREN, 2007).

Critical information infrastructure protection (CIIP) is critical when addressing cybersecurity issues. The EC is at the forefront of developing strategies to protect CCIP. The EC's Communication on CIIP COM (2009) 149 Action Plan has five key pillars (Vandrianavaly, 2009):

1. Preparedness and prevention
2. Detection and response
3. Mitigation and recovery
4. International cooperation
5. Criteria for European Critical Infrastructures in the ICT sector

CIIP is critical because the degree to which it is protected directly affects the livelihood of the many people who depend on efficient security.

Fiji does not have any CIIP mechanisms in place. The protection of critical information infrastructure is crucial. There is a lack of methodology in this regard.

The ITU has developed a national cybersecurity/CIIP self-assessment tool which is a practical initiative by the ITU-D ICT Applications and Cyber Security Division to assist ITU member states who wish to elaborate on their national approach for cybersecurity and CIIP (Vandrianavaly, 2009).

Impact on economic development

The impact of cybersecurity on national security is a very real one. Likewise, ICTs impact economic development. Whilst an increase in ICT penetration throughout Fiji can bring economic growth, the illicit use of ICT can also adversely affect Fiji's economy. According to the ITU toolkit for cybercrime legislation, 'The interconnected networks of the Internet have enabled unprecedented economic opportunities and linked populations around the globe in ways never before possible' (ITU, no date b). ICT has revolutionized economic development in developing economies, as suggested by a World Bank Study in 2009 that observed that for developing countries every 10% increase in broadband penetration leads to 1.38% increase in GDP (Wei and Rossotto, 2009).

Figure 5 shows the capacity of ICT to impact economic growth for both high income and low and middle income economies. ICT is an enabler for trade, e-commerce, access to markets, education, and competition. However, the potential for economic growth can be aborted if cybersecurity is not managed:

> *The **benefits of the Internet**, however, are **being undercut** by those exploiting its capabilities to the detriment and harm of others. Improvements in security are required in order to ensure the continued positive contributions of the Internet. [Author's emphasis]*
>
> **(ITU Toolkit for Cyber Crime Legislation)**

Fiji is currently in the process of putting in place systems and mechanisms to enable it to measure the economic impact.

- *Example 1: Impact of shutting down the Internet in Egypt*

The recent Egyptian revolution, which lasted 18 days, cost the economy USD$30 billion (Rabin, 2011). This is contrary to what OECD had predicted, which was USD$90 million. This Egyptian scenario is interesting as it was inflicted by the Egyptian government in its own country.

- *Example 2: Cybercrime costs – US and UK*

Customers expect banks to foot the bill, when they have been defrauded. The cost of fraud is reported to cost the US banking industry, tens of billions of dollars (infosecurity.com,2010). UK Officials said e-crime is estimated to cost the UK several billion pounds a year (Corera, 2009). Cybercrime costs the UK economy some £27 billion a year and is thought to be endemic according to the first official government estimate of the issue published in February 2011 (MSNBC, 2011).

- *Example 3: Cybercrime costs due to social engineering in Australia*

In Australia, victims of scams via social engineering amount to hundreds of millions of dollars per annum (AusCERT, no date).

Mitigating cybersecurity risks

National strategies

In Fiji, there is no comprehensive national cybersecurity strategy in place to assess and mitigate the risks of cybersecurity. There are many countries around the world that recognise the need to address these challenges through their robust cybersecurity strategies, such as Germany, the UK, the USA. To show the level of priority that governments are placing on cybersecurity, a good example would be the USA.

Cybersecurity has been identified by President Obama as one of the most serious economic and national security challenges in the USA. Consequently, President Obama ordered a thorough review of federal efforts to defend the US information and communications infrastructure and the development of a comprehensive approach to securing America's information infrastructure (US National Security Council, no date).

The Cyberspace Policy Review is built on the Comprehensive National Cybersecurity Initiative (CNCI) launched by President George W. Bush

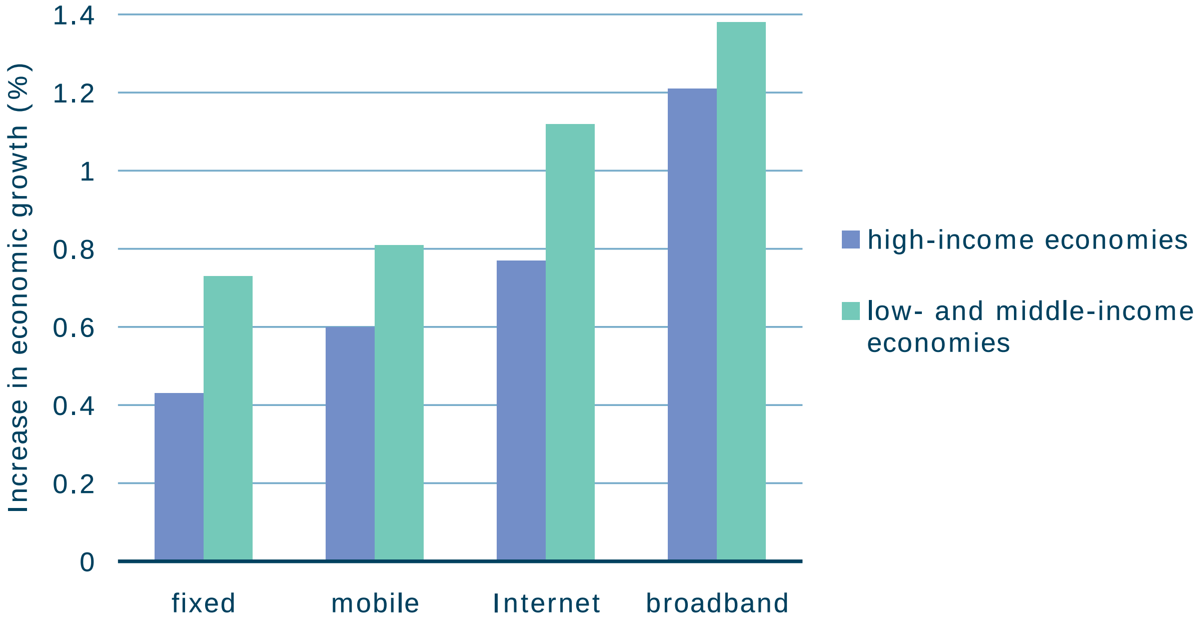


Figure 5. Economic Impacts of Broadband Information and Communications for Development 2009: Extending Reach and Increasing Impact – World Bank 2009 (Wei and Rossotto, 2009).

in National Security Presidential Directive 54/ Homeland Security Presidential Directive 23 (NSPD-54/ HSPD-23) in January 2008.

The CNCI's objectives are as follows:

- To establish a front line of defense against today's immediate threats.
- To defend against the full spectrum of threats.
- To strengthen the future cybersecurity environment.

In May 2009, President Obama endorsed recommendations of the Cyberspace Policy Review. The Executive Branch was directed to work closely with all key players in US cybersecurity, including state and local governments, as well as the private sector to ensure the following:

- A coordinated and cohesive response to future cyber-incidents.
- Strengthening public and private partnerships to find technology solutions.
- Investing in cutting edge research and developments to meet digital challenges.
- Campaigning to build digital awareness and digital literacy from the classroom to the boardroom and to build a digital workforce for the twenty-first century.

The President also directed that all these activities be conducted in a manner that ensured that privacy rights and civil liberties that were guaranteed in the constitution would be protected.

Lessons Fiji can learn

Fiji can review its structures and operations and identify how it can move towards a more coordinated and cohesive response. Fiji can also work towards strengthening public and private partnerships in the move towards developing robust policies in place. It can move towards campaigning to build digital awareness and digital literacy within primary schools, communities, villages, schools, etc.

Role of CERTS and CSIRTS

Computer Emergency Response Teams (CERTS, also referred to as CSIRTS – Computer Security Incident Response Teams) are essential tools for CIIP. According to the European Network and Information Security Agency (ENISA), every single country that is connected to the Internet must have capabilities at hand to effectively and efficiently respond to information security incidents (ENISA, no date). ENISA has been working towards establishing CERTs in Eastern Europe, Africa, and to a certain extent, in Asia Pacific.

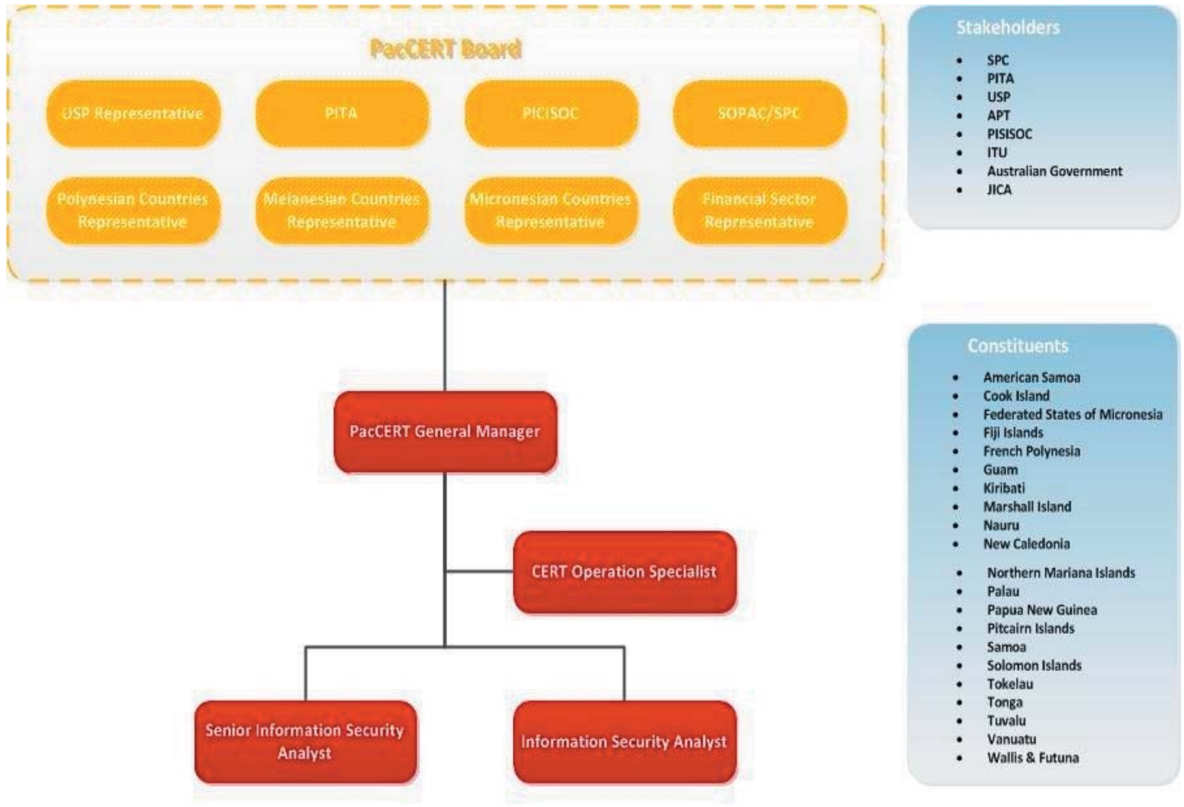
APCERT have been active in raising awareness within the Asia Pacific region. Izumi Aizu, a member of ICANN's At-Large Advisory Committee, believes that one of the first steps in establishing cybersecurity mechanisms within a country is establishing a CERT (pers. comm. 2010).

In the Pacific, most countries cannot afford their own CERT let alone the capacity to manage their CERTs for the time being. In the absence of national CERTs, PacCERT is in place to assist Pacific Island Countries like Fiji. In time, Fiji will have the capacity to have its own CERT.

- *PacCERT*

Pacific Island Countries (PICs) have a CERT in place called PacCERT. The ITU has the support of the Australian Government, which enabled it to commission AusCERT to conduct a preliminary assessment of the feasibility of having a CERT for the Pacific (Kim, 2009). Reports were tabled before the ITU Pacific ICT Ministerial Meeting in Tonga 2009 which noted and supported the efforts towards the establishment of a PacCERT. Forum officials endorsed the establishment of a CERT for the Pacific at the APT Telecommunications ICT Policy at the Regulatory Meeting for the Pacific in 2009.

PacCERT's mission is to facilitate, coordinate, and monitor activities related to cybersecurity and safety and to secure fast and effective response to cybersecurity and threats.



* Source : PacCERT Presentation for the Pacific Regional Information Technology Officials and Ministers Meeting 16 – 18 June 2010 Nukualofa Tonga

Figure 6. PacCERT's organisation chart.

- *FijiCERT*

Fiji does not yet have a CERT in place because it simply cannot afford to. One of the challenges that developing countries like Fiji face, is the capacity to have sustainable means of generating its revenue to be able to self-sustain work on the ground. ICT stakeholders from within the government should ensure that the government is kept informed of issues such as cybersecurity that affect developments. It is critical that Fiji's ICT policy also be revised to address regulatory overlaps and matters of national security such as cybersecurity.

The regulatory framework has direct links to development.

Brief overview of Cybersecurity the regulatory framework in Fiji

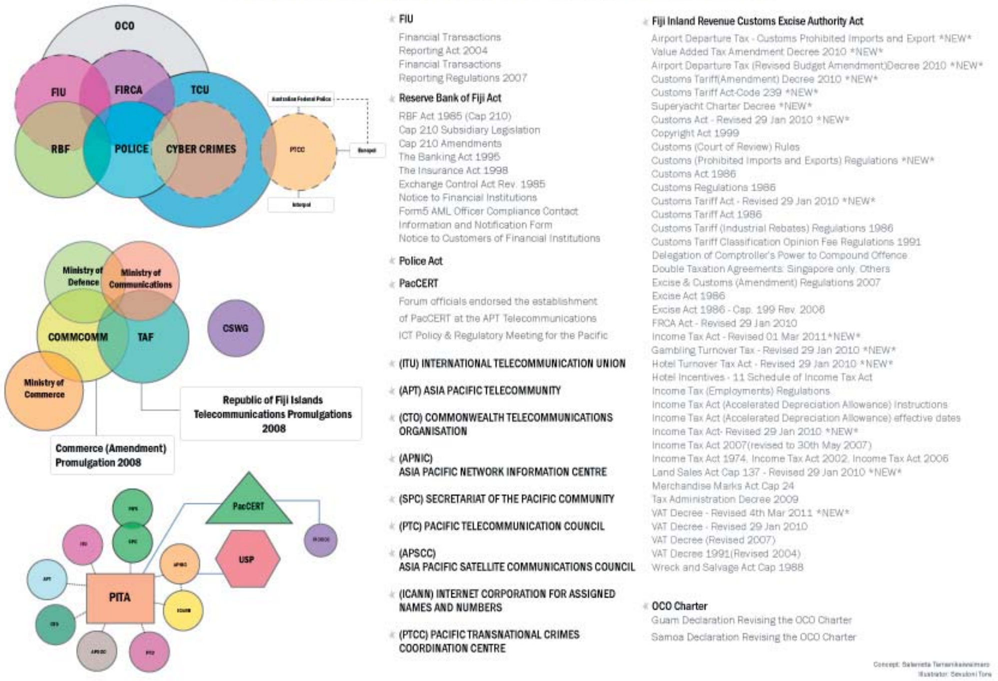
Some of these organisations do not deal directly nor specifically with cybersecurity but are part of the regulatory landscape.

- *Commerce Commission*

The Commerce Commission, established by the Commerce Act, which has since been repealed and is now enacted through the Commerce Commission Decree 2010, has extensive powers. Through the new decree, the Commerce Commission's decisions on telecommunication services cannot be legally challenged. The Commerce Commission regulates competition (preventing anti-competitive behaviour, exploitation of significant market power, and price control such as price determinations, price ceilings, and price floors).

- *Cybercrimes Unit*

The Cybercrimes Unit, which is a unit within Fiji's police force that deals with cybercrimes and cybersecurity issues. The government recognised the need to create a Cybercrimes Unit within its police force to enforce the Crimes Decree and the Criminal Procedure Code. They work in close partnership with the Ministry of Defence.


OCO
FIU
FIRCA
TCU
RBF
POLICE
CYBER CRIMES
Australian Federal Police
PTCC
Interpol
Ministry of Defence
Ministry of Communications
COMMCOMM
TAF
CSWG
Ministry of Commerce
Republic of Fiji Islands Telecommunications Promulgations 2008
Commerce (Amendment) Promulgation 2008
PacCERT
USP
ITU
SPC
APT
APNIC
PITA
CTO
ICANN
APSCC
PTC
FIU
Financial Transactions Reporting Act 2004
Financial Transactions Reporting Regulations 2007
Reserve Bank of Fiji Act
RBF Act 1985 (Cap 210)
Cap 210 Subsidiary Legislation
Cap 210 Amendments
The Banking Act 1995
The Insurance Act 1998
Exchange Control Act Rev. 1985
Notice to Financial Institutions
Form5 AML Officer Compliance Contact
Information and Notification Form
Notice to Customers of Financial Institutions
Police Act
PacCERT
Forum officials endorsed the establishment
of PacCERT at the APT Telecommunications
ICT Policy & Regulatory Meeting for the Pacific
(ITU) INTERNATIONAL TELECOMMUNICATION UNION
(APT) ASIA PACIFIC TELECOMMUNITY
(CTO) COMMONWEALTH TELECOMMUNICATIONS ORGANISATION
(APNIC) ASIA PACIFIC NETWORK INFORMATION CENTRE
(SPC) SECRETARIAT OF THE PACIFIC COMMUNITY
(PTC) PACIFIC TELECOMMUNICATION COUNCIL
(APSCC) ASIA PACIFIC SATELLITE COMMUNICATIONS COUNCIL
(ICANN) INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS
(PTCC) PACIFIC TRANSNATIONAL CRIMES COORDINATION CENTRE
Fiji Inland Revenue Customs Excise Authority Act
Airport Departure Tax - Customs Prohibited Imports and Export *NEW*
Value Added Tax Amendment Decree 2010 *NEW*
Airport Departure Tax (Revised Budget Amendment)Decree 2010 *NEW*
Customs Tariff(Amendment) Decree 2010 *NEW*
Customs Tariff Act-Code 239 *NEW*
Superyacht Charter Decree *NEW*
Customs Act - Revised 29 Jan 2010 *NEW*
Copyright Act 1999
Customs (Court of Review) Rules
Customs (Prohibited Imports and Exports) Regulations *NEW*
Customs Act 1986
Customs Regulations 1986
Customs Tariff Act - Revised 29 Jan 2010 *NEW*
Customs Tariff Act 1986
Customs Tariff (Industrial Rebates) Regulations 1986
Customs Tariff Classification Opinion Fee Regulations 1991
Delegation of Comptroller's Power to Compound Offence
Double Taxation Agreements: Singapore only. Others
Excise & Customs (Amendment) Regulations 2007
Excise Act 1986
Excise Act 1986 - Cap. 199 Rev. 2006
FRCA Act - Revised 29 Jan 2010
Income Tax Act - Revised 01 Mar 2011*NEW*
Gambling Turnover Tax - Revised 29 Jan 2010 *NEW*
Hotel Turnover Tax Act - Revised 29 Jan 2010 *NEW*
Hotel Incentives - 11 Schedule of Income Tax Act
Income Tax (Employments) Regulations
Income Tax Act (Accelerated Depreciation Allowance) Instructions
Income Tax Act (Accelerated Depreciation Allowance) effective dates
Income Tax Act- Revised 29 Jan 2010 *NEW*
Income Tax Act 2007(revised to 30th May 2007)
Income Tax Act 1974, Income Tax Act 2002, Income Tax Act 2006
Land Sales Act Cap 137 - Revised 29 Jan 2010 *NEW*
Merchandise Marks Act Cap 24
Tax Administration Decree 2009
VAT Decree - Revised 4th Mar 2011 *NEW*
VAT Decree - Revised 29 Jan 2010
VAT Decree (Revised 2007)
VAT Decree 1991(Revised 2004)
Wreck and Salvage Act Cap 1988
OCO Charter
Guam Declaration Revising the OCO Charter
Samoa Declaration Revising the OCO Charter

Concept: Salanieta Tamanikaiwaimaro
Illustrator: Sevuloni Tora

Figure 7. Illustration showing cybersecurity regulatory environment in Fiji.

- *Cybersecurity Working Group*

The Cybersecurity Working Group was established in 2010 through a memorandum jointly sent by the Cybercrimes Unit and the Ministry of Defence, inviting multistakeholders to form a Cybersecurity National Working Committee and Group. This is based on a public private partnership model. The group is comprised of the government ICT, Ministry of Defence, Cybercrimes Unit, Finance Intelligence Unit(FIU), licensed operators, network service providers, banks, etc.

- *Financial intelligence unit*

The Financial Transactions Reporting Act 2004 established the Finance Intelligence Unit (FIU). The unit is regulated by the Financial Transactions Reporting Regulations 2007. It is responsible for monitoring illicit activities, such as money laundering and drug trafficking. FIU has had seven cybercrimes referred to the Fiji police.

- *Fiji Inland Revenue and Customs and Excise Authority (FIRCA)*

FIRCA, which was established by the FIRCA Act, regulates the revenue, customs, and excise controls. Tax evasion also occurs electronically and falls within cybercrimes and cybersecurity.

- *Reserve Bank of Fiji*

The reserve bank of Fiji, established by the Reserve Bank of Fiji Act 1985, is responsible for regulating the financial market. It relies on other legislations to regulate the financial market: The 1995 Banking Act 1995. The 1998 Insurance Act 1998, and the 1985 Exchange Control Act Rev.

- *National Anti-Money Laundering Council*

The Financial Transactions Reporting Act 2004 established the National Anti-Money Laundering Council.

- *Pacific Transnational Crimes Coordination Centre (PTCC)*

In 2004, the Australian federal police assisted Pacific Island countries in establishing the Pacific National Crimes Coordination Centre.

- *TAF*

The Telecommunications Promulgation of 2008 established the Telecommunications Authority of Fiji (TAF), which regulates telecommunications. This encompasses the telecommunications networks and the interconnections amongst licensed operators and ISPs.

- *Transnational Crimes Unit (TCU) (Fiji)*

The Transnational Crimes Unit (TCU) was established following the establishment of the PTCC.

Diversity of approaches and categorisation of cybersecurity and cybercrime

Diversity of approaches to definition

The EU's comprehensive version of cybercrime differs from that of the USA and likewise from other countries around the world. The EU Council, being the first to attempt to create an international convention to define cybercrime, also recognises the difficulty in defining what cybercrime is, despite efforts made by legislators, researchers, and LEA personnel (Europol, 2007). The difficulties were attributed to the different domestic legislation within the different countries that results in diverse approaches.

Categorisation

Cybersecurity has both a civil and criminal aspect to it. The civil aspect is where matters are not prosecuted as criminal infringements, and criminal matters are those which infringe on clear statutory provisions within the law. Countries differ in the manner in which they categorise cybercrime. For example, consider the EU, Australia, and the USA.

- *The EU's categorisation*

EU's Cybercrime Convention categorises computer crimes into five main categories, namely:

1. Crimes against the confidentiality, integrity, and availability of computer data and systems.
2. Computer related traditional crimes.
3. Content-related offences.
4. Offences related to infringement of copyright and related rights.
5. Infringement of privacy.

- *Australia's categorisation*

The Australian Institute of Criminology (Grabosky and Smith, 1998) categorises cybercrime into nine different categories:

1. Theft of telecommunication services.
2. Communications in furtherance of criminal conspiracies.
3. Telecommunications piracy.
4. Dissemination of offensive materials.
5. Electronic money laundering and tax evasion.
6. Electronic vandalism, terrorism, and extortion.
7. Sales and investment fraud.
8. Illegal interception of telecommunications.
9. Electronic funds transfer fraud.

- *The USA's categorisation*

The US Computer Fraud and Abuse Act of 1986 categorises computer fraud and abuse as follows:

1. Obtaining national security information.
2. Compromising the confidentiality of a computer.
3. Trespassing in a government computer.
4. Accessing a computer to defraud and obtain value.
5. Knowing transmission and intentional damage.
6. Intentional access and reckless damage.
7. Intentional access and damage.
8. Trafficking in passwords.
9. Extortion involving threats to damage computer.

- *Fiji's categorisation*

Fiji has yet to develop its categorisation of cybercrime. Whilst the crimes decree has provisions within that describe computer-related crimes, they do not efficiently address the broad spectrum of cybercrime.

Legal framework

International law

The United Nation's (UN) General Assembly's Resolutions (UNGA Res) 55/63 and 56/121 established the legal framework on countering the criminal misuse of information technologies:

1. *UNGA Res: 57/239* on the creation of a global culture of cybersecurity.
2. *UNGA Res: 58/199* on the creation of a global culture of cybersecurity and the protection of essential information infrastructures.
3. *UNGA Res: 41/65* on principles relating to remote sensing of the Earth from outer space.

Within the Geneva Declaration of Principles, the World Summit on the Information Society (WSIS) in 2003 supported the activities of the UN to prevent the potential use of ICTs for purposes that are inconsistent with the objectives of maintaining international stability and security and which may adversely affect the integrity of the infrastructure within the States to the detriment of their security.

According to the declaration, it is necessary to prevent the use of information resources and technologies for criminal and terrorist purposes whilst respecting human rights. The Council of Europe's Convention on cybercrime was open for signing on 23 November 2001.

Domestic law

Table 1 shows the wide array of legal instruments and organisations that overlap and potentially whose scope of works covers cybersecurity.

Sir Carleton Allen in *Legal Duties* (Smith and Hogan, 1992) wrote that a crime is crime because it is wrongdoing which has direct consequences and seriously threatens the security or well-

Table 1. *EU's cybercrime convention categories and corresponding Fiji laws*

EU's CYBER CRIME CONVENTION CATEGORIES	FIJI's DOMESTIC LAWS
1. Crimes against the Confidentiality, Integrity and Availability of computer data and systems	s.340 -s.346 Crimes Decree 2009
2. Computer related traditional crimes	s.340 -s.346 Crimes Decree 2009 (not adequately codified)
3. Content-related offences	
4. Offences related to infringement of copyright and related rights	
5. Infringement of privacy	s12,s14 of Compulsory Registration of Customers for Telephones Services Decree 2010
AUSTRALIAN INSTITUTE OF CRIMINOLOGY's CATEGORISATION OF CYBERCRIME (Grabosky and Smith, 1998)	
1. Theft of Telecommunication Services	
2. Communications in Furtherance of Criminal Conspiracies	
3. Telecommunications Piracy	s2 Copyright (Amendment) Decree 2009
4. Dissemination of Offensive Materials	
5. Electronic Money Laundering and Tax Evasion	Customs Act, Customs Tariff Act, Excise Act, Gambling Turnover Decree, Income Tax Act, Land Sales Act, Merchandise Marks Act, Value Added Tax Decree, Wreck and Salvage Act
6. Electronic Vandalism, Terrorism and Extortion	
7. Sales and Investment Fraud	s317, 318 Crimes Decree 2009; Part 7 Commerce Decree 2010
8. Illegal Interception of Telecommunications	
9. Electronic Funds Transfer Fraud	s344 of Crimes Decree 2009 and s.3-s.21 of Financial Transactions Reporting Act 2004
UNITED STATES DPT OF JUSTICE CATEGORISATION OF COMPUTER CRIMES (US Government, 1986)	
1. Obtaining National Security Information	
2. Compromising the Confidentiality of a Computer	s.340 -s.346 Crimes Decree 2009
3. Trespassing in a Government Computer	s.340 -s.346 Crimes Decree 2009
4. Accessing a Computer to Defraud and Obtain Value	s.340 -s.346 Crimes Decree 2009
5. Knowing Transmission and Intentional Damage	
6. Intentional Access and Reckless Damage	
7. Intentional Access and Damage	
8. Trafficking in Passwords	
9. Extortion Involving Threats to Damage Computer.	

being of society, where it is not safe for it to be re-dressed only by compensation of the injured party.

Cybersecurity is a very real and tangible threat that affects everyone. It fits into Allen's definition, where the illicit use of ICTs consists of wrongdoing that directly and in serious degree threatens the security or well-being of society or the global community and because it not safe to merely compensate the parties injured.

The first reported case of computer crime in the world arguably dates back to 1958 (Bequai, 1987) and the first federal prosecution to 1966 in the USA. Since then, the definitions of cybercrime vary from jurisdiction to jurisdiction and each due to sovereignty of nation states as is made clear from the varying categorisation of cybercrimes. This is obvious from Table 1 which shows the EU's cybercrime convention categories and corresponding Fiji laws.

- *Crimes Decree*

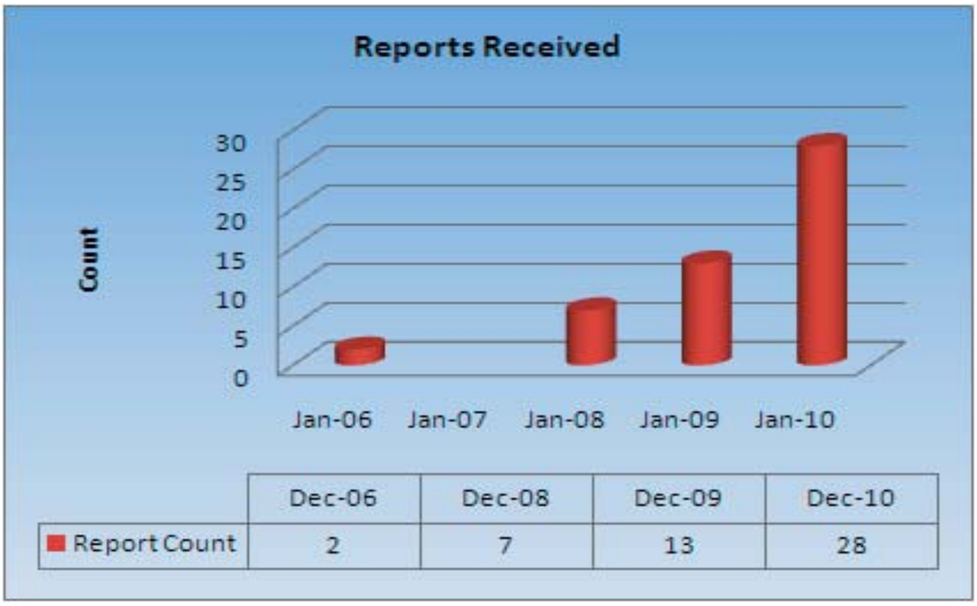
Fiji has embryonic legal provisions that attempt to create computer offences. The Crimes Decree is the principal legal instrument that criminalises computer offences. The Crimes Decree does not begin to capture the complexities and the diverse range of cybersecurity breaches that occur in Fiji and that affect the cyber-environment and infrastructure in Fiji. The cybercrimes provisions within the Crimes Decree do no canvass the elements that are involved in the illicit use of ICTs and which are restricted to computers.

Fiji currently does not have a proper records capturing system. The reporting system is currently deficient as it merely records instances when charges are brought and does not capture the record of incidences or complaints that come in the first instance. One of the challenges for the cybercrimes unit and law enforcement authorities are that when complaints are investigated, criminal charges cannot be brought against alleged offenders for the simple reason that there was no express legislative provision criminalising the behaviour.

There is a need for better coordination in how statistics are kept. This data was furnished by the cybercrimes unit. The 2010 data range is strictly from January 2010 to November 2010.

The reports in Figure 8 are of alleged acts that were digital in nature and where no crimes were committed, the data is not captured. The statistics that are compiled are insufficient to determine the extent of the cybersecurity threats in Fiji. It is recommended that clear categorisation of threats be made that will enable law enforcement authorities to keep track.

According to the Cybercrimes Unit, as of December 2010 only two cases from 2006 made it to court. However, the suspects were charged



	Dec-06	Dec-08	Dec-09	Dec-10
🟥 Report Count	2	7	13	28

Figure 8. Cybercrimes Unit (Fiji Police Force, 2011).

for other offences that were not cybercrimes and only one of the cases was successfully prosecuted.

One of the challenges that the unit has found is that whilst there are reports made of the crimes, the crimes themselves do not constitute a criminal act under the current legislative instruments. The reports above are only those that could be charged under the existing laws.

The current approach to the existing drafting, in particular s340 – s346 of the Crimes Decree 2009, shows a 'real law approach' (Kurbalija, 2010).

In light of the reported attacks to some of the world's most sophisticated and developed countries, one can only imagine the extent of Fiji's vulnerability. The Internet has commonly been touted as the 'network of networks', therefore the vulnerability of the network's infrastructure and systems needs to be addressed through the development of a national cybersecurity strategy.

- *Complexity*

Given that the Internet comprises multiple layers and elements that are attributed to various interlinking components, which are part of the Internet architecture, it follows that there are numerous variables and factors that investigators and prosecutors need to consider. Criminal law thrives on linking causation, where the criminal acts must be linked to the offence.

Internet users leave traces when they use Internet services, which can be used to identify them if they exploit a system or network weakness and which can incriminate a person who may have been nowhere near the source of the attack. According to a World Bank study facilitated by the World Bank Treasury Security Team (entitled *Cyber Zombies*), one in three machines are enslaved to attack other machines, and cybercriminals are becoming increasingly sophisticated as they network with each other worldwide. In the process, cybercriminals now set up a crew to split the technical activities. This hinders investigations and in particular the ability to identify criminals. A criminal project can be prepared by different individuals namely (Europol, 2007):

- the coder – who is the writer and creator of the malicious code;
- the launcher – who will run it;
- the miner – who will extract the data; and
- the washer – who will launder the revenue, for instance in an e-payment system.

One of the difficulties that Europol faces is that often these threats come from abroad. Also, because of the lack of data available, police forces within the EU face serious problems in investigating BOTNETS or BOTS,[6] because of the lack of proper legislation and the slowness of legal procedures to source data from abroad. This is due to the growing phenomenon as well as the increase in criminal groups and their sophistication. There are those whose medium of choice is to use public Internet cafes that do not require identification. In those cases, investigations will often fail. The same is relevant if offenders are making use of open wireless networks to mask their identity.

The phenomenon of BOTNETS or BOTS is currently considered to be one of the most dangerous cyberthreats on an international level due to difficulty in detection. There is little data available compared to the enormity of the issue, and police forces around the world sometimes have inconsistent legal tools with which to investigate them. Criminal activity is often outside the victim's country and it is common for victims to fail to report the issue to the police (Europol, 2007).

BBC reported that a coder, a 23-year-old hacker known as Iserdo, who created the Maripora virus code named 'butterfly', was arrested in Slovenia (BBC News Technology, 2010). After the arrest, the virus was dismantled after infecting 12.7 million computers. The three people who were running it were arrested in Spain in December 2009 (BBC News Technology, 2010).

[6] BOTNETS or BOTS refers to robotic networks which is a script which can remotely undertake a computer (or a number of computers), eventually attacking other machines over the internet. This means that a computer connected to the Internet can be compromised by a hacker who takes control over the machine remotely through, e.g. an installed Trojan. The compromised machine (called Zombie or Drone) becomes a robot under in the control of the hacker and is used to attack other computers over the internet with the aim of extorting money, industrial espionage, theft of personal data, theft of bank account details, theft of credit card numbers etc.

Deficiencies of crimes Decree

The definitions of s.336 of the Crimes Decree, do not begin to capture the complexities and the diverse range of cybersecurity breaches. Access to data held in computers is limited to mean the following:

- display of the data by the computer or any other output of data from the computer;
- copying or moving of data to any other place in the computer or to a data storage device; and
- in the case of a program – the execution of the program.

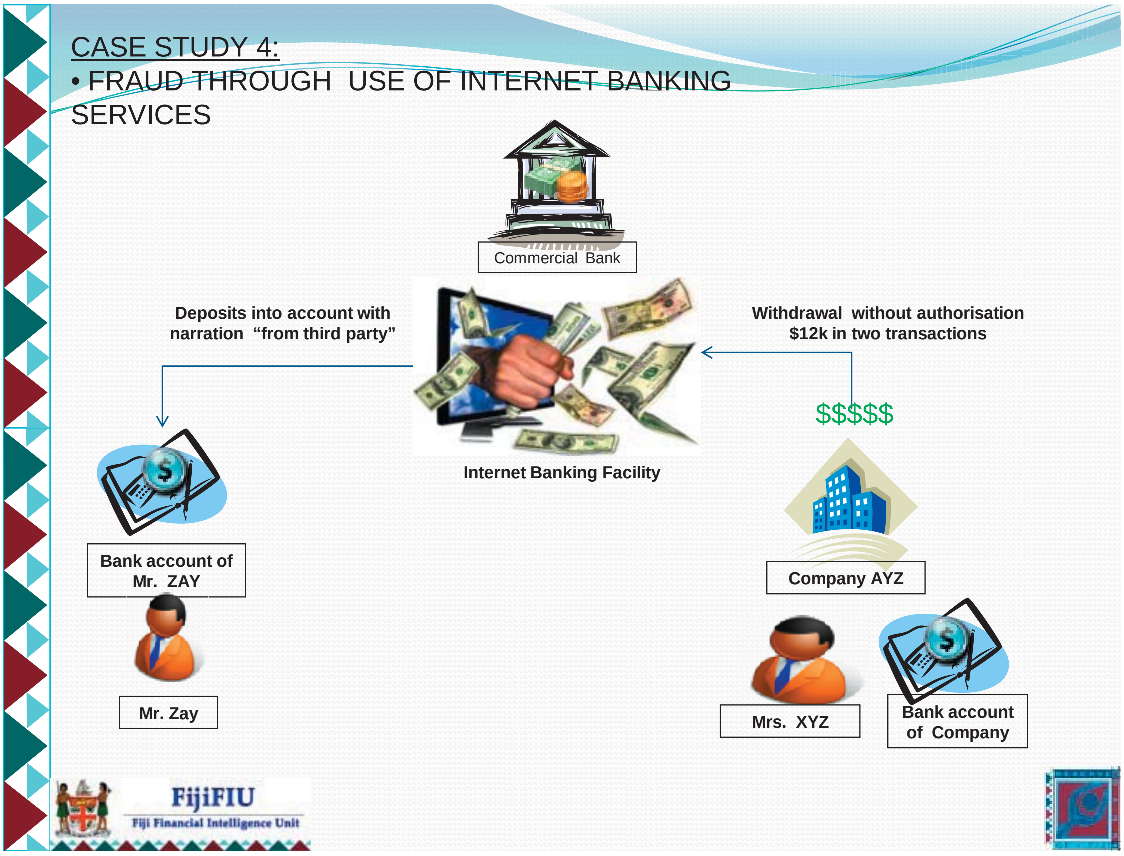
Criminal law is based on proving elements of an offence beyond reasonable doubt. Many of the cybersecurity threats that are prevalent in Fiji and around the world are not properly described within s340 – s346.

Some of these cybersecurity threats include those involved in the illicit use of ICTs and are not confined to computers. There is no mention of crimes that could be perpetuated through ICT, for example telecommunications.

Some of the deficiencies include the lack of the following:

- Definitions of criminal offences.
- Illegal access – the limitations of the current wording of drafting of illegal access.
- Illegal interception – there is no clear definition of what is lawful and what is unlawful, which makes the work of regulators challenging.
- The use of modification is a hindrance as there is no mention of data interference or system interference.
- The misuse of devices.
- Computer-related forgery.
- Computer-related fraud.
- Production and distribution of child pornography over the Internet.
- Online intellectual property infringements and related rights.
- Prosecutorial and procedural requirements.
- Real-time collection of traffic data.

To begin addressing these deficiencies, Fiji needs to develop a form of categorisation and a review of existing legislative instruments that is



CASE STUDY 4:

• FRAUD THROUGH USE OF INTERNET BANKING SERVICES

Commercial Bank
Deposits into account with narration "from third party"
Withdrawal without authorisation $12k in two transactions
$$$$$
Internet Banking Facility
Bank account of Mr. ZAY
Company AYZ
Mr. Zay
Mrs. XYZ
Bank account of Company
FijiFIU
Fiji Financial Intelligence Unit

Figure 9. Fraud through the use of Internet Banking Service.

both a substantive and procedural analysis. The Cybersecurity Working Group will initiate comprehensive research and organise empirical analysis of research findings.

It is envisaged that a detailed study of the Council of Europe Convention on Cybercrime and other existing policies will be carried out.

- *Telecommunications promulgation*

Section 13 of the Telecommunications Promulgation expressly stipulates that chapters 11 and 40 of the Penal Code (Cap.17) applies to any member of the board, the Tribunal, or any committee or body established under the Promulgation. Whilst the Penal Code has since been repealed and replaced by the Crimes Decree, the provisions are more or less related to the abuse of office, corruption and secret commissions provisions. There is no direct reference to the computer related offences nor illicit use of ICTs.

Section 72 of the Telecommunications Promulgation creates a statutory duty for the Telecommunications Authority of Fiji to prevent the illicit use of ICTs. Also, it must assist officers and authorities in enforcing criminal laws and imposing pecuniary penalties, protecting the public revenue, and safeguarding national security.

Section 73 of the Telecommunications Promulgation also creates a statutory duty for the licensees to prevent the telecommunications networks and telecommunications services and facilities from being used in, or in relation to, the commission of offences against the laws of Fiji. There are deficiencies in the Telecommunication Promulgation.

Deficiencies of the Telecommunication Promulgation

There are no clear provisions against the illicit use of ICTs. The second phase of research can look into outlining these. There have been complaints registered by licensed operators but to date this has yet to be addressed since there is no regulatory framework that encompasses these.

- *Financial Transactions Reporting Act*

The Financial Transactions Reporting Act endeavours to criminalise fraud through the use of Internet banking services. Figure 9 is an example of a case study as prepared by the FIU to show fraud through Internet banking services.

- *Commerce Decree 2010*

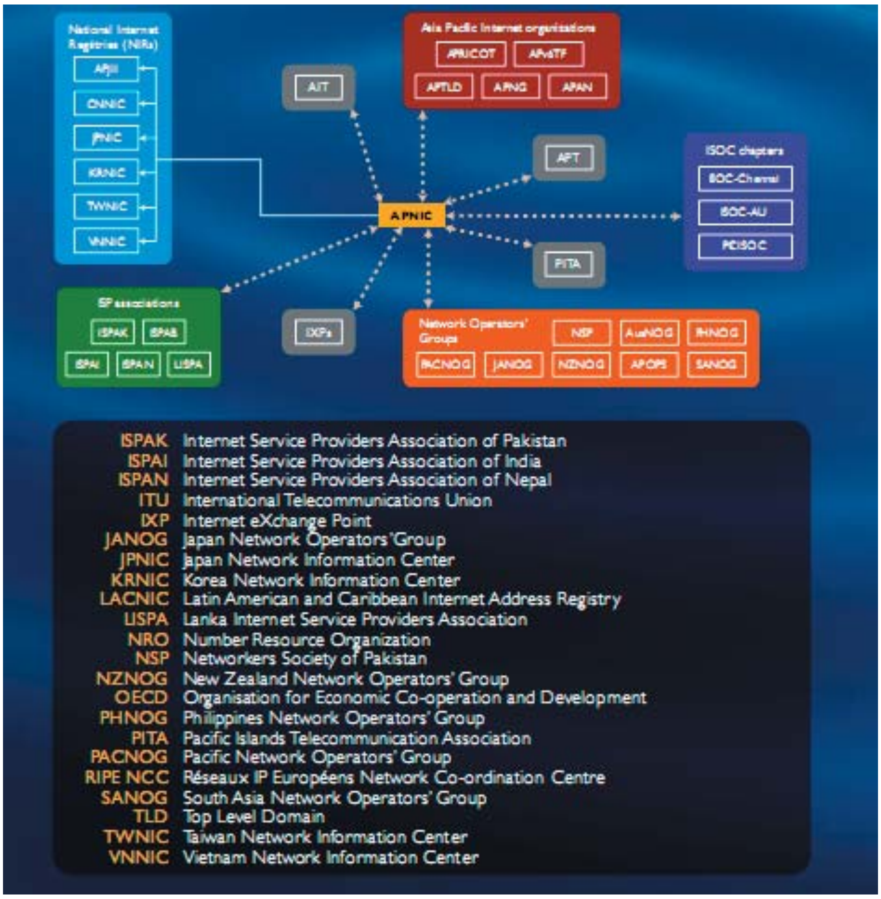
Part seven of the Commerce Decree deals with consumer protection and unfair trade practices, such as misleading or deceptive conduct, unconscionable conduct, false or misleading misrepresentation, and false and misleading advertisements that could be widely read to canvass conduct taking place through the illicit use of ICTs.

Joint cooperation

There needs to be an increased cooperation amongst all stakeholders, and we can learn from Europe, the USA, Japan, and Australia about the increasing need for partnerships to combat cybersecurity threats. Given the nature of the Internet, it goes without saying that there is increasingly a need to have joint cooperation that is both vertical and horizontal. An example of joint cooperation is Europol's Joint Cooperation (Strategic and Operational) with non-EU countries.

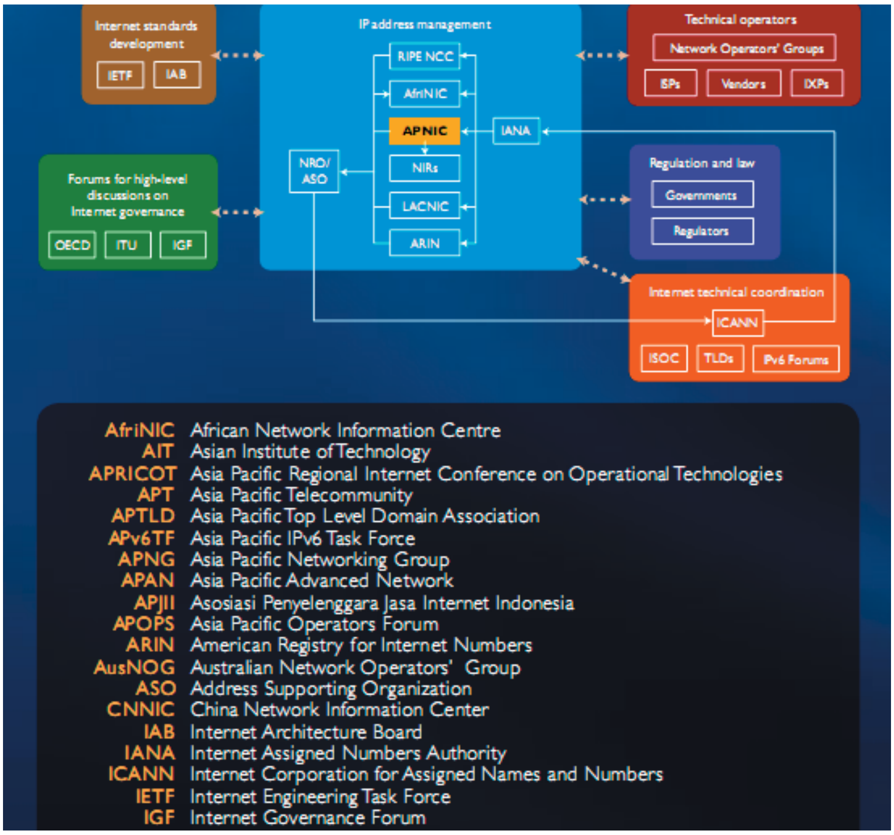
The European Commission's 2009 draft strategy includes the CIIP policy, which 'complements existing measures in the area of police and judicial co-operation to prevent, fight, and prosecute criminal and terrorist activities targeting CIIs (Europol, 2007). The European Commission is exploring utilising a public – private sector model. The USA is already moving towards increased collaboration and engagement with the private sector.

In January 2011, Australia and the UK announced a cyberpartnership to combat cybersecurity threats in an effort at joint cooperation. The countries, along with the USA, Canada, and New Zealand, cooperated on cybersecurity issues in an organisation unofficially called the 'Five Eyes'.



ISPAK	Internet Service Providers Association of Pakistan
ISPAI	Internet Service Providers Association of India
ISPAN	Internet Service Providers Association of Nepal
ITU	International Telecommunications Union
IXP	Internet eXchange Point
JANOG	Japan Network Operators'Group
JPNIC	Japan Network Information Center
KRNIC	Korea Network Information Center
LACNIC	Latin American and Caribbean Internet Address Registry
LISPA	Lanka Internet Service Providers Association
NRO	Number Resource Organization
NSP	Networkers Society of Pakistan
NZNOG	New Zealand Network Operators' Group
OECD	Organisation for Economic Co-operation and Development
PHNOG	Philippines Network Operators' Group
PITA	Pacific Islands Telecommunication Association
PACNOG	Pacific Network Operators' Group
RIPE NCC	Réseaux IP Européens Network Co-ordination Centre
SANOG	South Asia Network Operators' Group
TLD	Top Level Domain
TWNIC	Taiwan Network Information Center
VNNIC	Vietnam Network Information Center

Figure 9a. Effective Internet governance in the Asia Pacific (APNIC, no date)



AfriNIC	African Network Information Centre
AIT	Asian Institute of Technology
APRICOT	Asia Pacific Regional Internet Conference on Operational Technologies
APT	Asia Pacific Telecommunity
APTLD	Asia Pacific Top Level Domain Association
APv6TF	Asia Pacific IPv6 Task Force
APNG	Asia Pacific Networking Group
APAN	Asia Pacific Advanced Network
APJII	Asosiasi Penyelenggara Jasa Internet Indonesia
APOPS	Asia Pacific Operators Forum
ARIN	American Registry for Internet Numbers
AusNOG	Australian Network Operators' Group
ASO	Address Supporting Organization
CNNIC	China Network Information Center
IAB	Internet Architecture Board
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
IETF	Internet Engineering Task Force
IGF	Internet Governance Forum

Figure 9b. Effective Internet governance from a global perspective (APNIC, no date)

Australian Attorney General Robert McClelland, on 11 March 2011, announced the creation of a counter-cyber-espionage unit which will operate within the Australian Security Intelligence Organisation (ASIO), a domestic agency equivalent to the UK's Military Intelligence, Section 5 (MI5) (Espiner, 2011). The United Kingdom is assisting Australia in setting up this unit.

In the Pacific, the Australian federal police in 2004 assisted Pacific Island countries in establishing the Pacific National Crimes Coordination Centre, and this has resulted in the establishment of the respective Transnational Crimes Units in forum island countries within the Pacific.

The Fiji Cybersecurity Working Group, which was initiated through a memo dated 24 August 2010 and sent by the Cybercrimes Unit in conjunction with the Ministry of Defence, established a working group that was tasked at looking into cybersecurity issues facing the industry. The objectives of the group were to increase joint cooperation, ensure child online protection, and discuss Internet governance challenges.

Recommendations

Stakeholders need to seriously assess and appreciate the gravity of having proper mechanisms in place that will ensure protection against cybersecurity threats. The following actions are recommended:

1. A workshop to identify critical areas for development and create a strategic plan for the lead-up to the development of a national strategy.
2. A working group to jointly cooperate and identify categories of cybercrime.
3. Further research into the status of cybersecurity in Fiji and also into developing a sealed version and public version of the report to assess whether there is a need for a specific cybercrimes decree or to strengthen existing legal instruments.
4. Identify potential local, national, and regional partners.
5. Develop a holistic, cohesive, and effective policy and national strategy.

Conclusion

The Internet is, without a doubt, a world of its own and is made even more complex by the interdependency of networks and the infrastructure that allow it to exist. The challenges in managing cybersecurity in Fiji can easily be achieved through joint cooperation, dialogue, extensive research both beyond Fiji and within Fiji. It will also require strategic capacity development within Fiji.

Cybersecurity is a pressing issue that policymakers must consider as they deliberate on strategies. It is critical that the Ministry of Defence commission the national Cybersecurity Working Group to undertake field research for the purposes of empirical analysis and further diagnosis of areas that need to be strengthened, as well as provide a way forward in terms of the implementation of a national defence strategy.

In terms of reporting cybercrimes, stakeholders need to come to some form of agreement as to what form of categorisation it wishes to apply in Fiji and the levels of regulation.

It is critical that policy analysts and decision-makers understand that whilst ICT can be an enabler for economic growth, this can also be opposed by the illicit use of ICTs. The illicit use of ICT and its governance issues require the formation of clear policies through cohesive coordination of institutions and stakeholders towards a common vision.

Acknowledgements

These baby steps would not be possible if I were not able to stand on the shoulders of tuwawas whose commitment to empowering and developing capacity within emerging economies. I would like to thank Diplo for opening my eyes and helping me understand IG issues and for its coordinators and tutors who tirelessly show incredible energy and commitment in the multistakeholder process. I would also like to thank the Diplo Community, particularly the students in my research class who make the class what it is today. To my fellow colleagues in emerging and developing economies, this is our sea-

son to help build our nations. I would also like to thank the Advance Breakthrough Centre, its leaders for their incredible support and patience.

It is awesome to be part of the Fiji Cyber Security Working Group and the Ministry of Defence whose members are committed to building and developing Fiji. I would also like to thank the experts such as Yuliya Morenets and Izumi Aizu, who despite juggling post tsunami and nuclear effects in Japan endeavoured to give me feedback on my initial draft. I would also like to thank Jay Newdick for taking the time to edit my initial draft and my numerous grammatical errors so that my work could read better. I would also like to thank Ivan Fong for always encouraging us to grow. The views in this paper do not represent the views of the Fiji Cybersecurity Working Group, the Ministry of Defence or Telecom Fiji Limited and are my own personal views. This is still a progressive piece and I am still in the middle of editing and correcting a lot of the material.

This is dedicated to Tu, Ta and Na who have always been behind me.

References

1. APNIC (no date) *Effective Internet governance in the Asia Pacific: Internet number resource distribution as a model of enhanced cooperation.* Available at http://www.apnic.net/__data/assets/pdf_file/0019/11485/igf2008.pdf [accessed 23 April 2011].
2. AusCERT (no date) *Study to ascertain the readiness of Pacific Island nations to establish a regional Pacific Island CERT capability.* Available at http://www.itu.int/ITU-D/asp/CMS/Events/2009/PACCERT/Interrim_PacificCERT_Report.pdf [accessed 14 March 2011].
3. Barker C (2009) EC initiative aims to shield Europe from cyberattacks. Available at http://www.zdnet.co.uk/news/networking/2009/03/31/ec-initiative-aims-to-shield-europe-from-cyberattacks-39634620/ [accessed 12 March 2011].
4. Barrett J (2010) Hacker claims to be in New Zealand. *New Zealand Herald* 25 April 2010. Available at http://www.nzherald.co.nz/connect/news/article.cfm?c_id=1501833&objectid=10640757 [accessed 20 March 2011].
5. Baselala (2011) Housing payments made easy. *The Fiji Times Online*, 21 March. Available at http://www.fijitimes.com/story.aspx?id=168792 [accessed 20 March 2011].
6. BBC News Technology (2010) Botnet hacker caught in Slovenia. *BBC News*, 28 July. Available at http://www.bbc.co.uk/news/technology-10786701 [accessed 4 April 2011].
7. Bequai A (1987) *Techno-Crimes, The Computerization of Crime and Terrorism*. Lexington Mass.: Lexington Books.
8. Corera G (2009) Cyber-security strategy launched. *BBC News*, 25 June. Available at http://news.bbc.co.uk/2/hi/uk_news/politics/8118348.stm [accessed 23 March 2011].
9. Council of Europe's Convention on Cyber Crime Budapest, 23. X1.2001. Available at http://conventions.coe.int/treaty/en/treaties/html/185.htm [accessed 8 July 2011]
10. Cybernaut (2010) *Cyber Mafia*. Available at http://www.thecybernaut.org/2010/11/cyber-mafia/ [accessed 20 March 2011].
11. Dang ST (2011) *Issue Brief for the GA First Committee: Disarmament and International Security (DISEC) The Prevention of Cyberterrorism and Cyberwar* [was emailed to me by the Fiji UN office in New York in March 2011]
12. *Day Press News* (2010) Arab & Israeli Cyber-War. 22 September. Available at http://www.dp-news.com/pages/detail.aspx?l=2&articleid=55075 [accessed 20 March 2011].
13. DGTREN (2007) Security Directorate as quoted in p32 of Europol High Tech Crimes Within the EU: Old Crimes, New Tools, New Crimes New Tools Threat Assessment 2007 High Tech Crime Centre Public Version, August 2007.
14. Espiner T (2011) UK helps Australia's cyber-spy unit get to work | Security Threats | ZDNet UK. *ZDNet*, 11 March. Available at http://www.zdnet.co.uk/news/security-threats/2011/03/11/uk-helps-australias-cyber-spy-unit-get-to-work-40092111/ [accessed 12 March 2011].
15. European Network and Information Security Agency [ENISA] (no date) *ENISA's work in the field of CERTs / CSIRTs* Available at http://www.enisa.europa.eu/act/cert [accessed 23 March 2011].
16. Europol (2007) *Europol high tech crimes within the EU: Old crimes new tools, new crimes new tools Threat assessment 2007.* Available at http://www.europol.europa.eu/publications/Serious_Crime_Overviews/HTCThreatAssessment2007.pdf [accessed 14 March 2011].
17. FINTEL (2011) Fiji Wreck and Salvage Act. *Data communications*. Available at http://www.fintel.com.fj/pages.cfm/services/data-communications/ [accessed 28 February 2011].
18. Garrie DB *et al.* (2009) Mari Impersonations of Life: The Perils of Social Networking. Gillepspie LR [ed.]. *Convergence* 5(2), pp. 236 - 244.
19. Grabosky P (1998) *Crime in the Digital Age: Controlling Telecommunications and Cyberspace Illegalities*. Federation Press and the Australian

Institute of Criminology.

20. International Monetary Fund [IMF] (2010) *World economic and financial surveys world economic outlook database—WEO groups and aggregates information*. Available at http://www.imf.org/external/pubs/ft/weo/2010/01/weodata/groups.htm#oem [accessed 11 March 2011].
21. iNEWP.com (2010) Epic Cyber War (Full Story): Japan V.S Korea i*NEWP.com*, 1 March. Available at http://inewp.com/?p=1086 [accessed 19 March 2011].
22. infosecurity.com (2010) Banks pick up tab for billions of dollars in fraud. *infosecurity.com*, 29 September. Available at http://www.infosecurity-us.com/view/12850/banks-pick-up-tab-for-billions-of-dollars-in-fraud/ [accessed 4 April 2011].
23. ITU (2008) Overview of cybersecurity. Available at https://www.itu.int/rec/T-REC-X.1205-200804-I [accessed 19 March 2011].
24. ITU (2010) Resolution WGPL/1 *ITU's role with regard to international public policy issues relating to the risk of illicit use of information and communication technologies : The Plenipotentiary Conference of the Union.*
25. ITU (no date) ITU National Cybersecurity/CIIP Self-Assessment Tool. Available at http://www.itu.int/ITU-D/cyb/cybersecurity/projects/readiness.html [accessed 19 March 2011].
26. ITU (no date b) Toolkit for Cyber Crime Legislation, p 6. Available at: www.itu.int
27. Internet Society (2010) *The Internet Ecosystem*. Available at http://www.isoc.org/pubpolpillar/docs/internetmodel.pdf [accessed 19 March 2011].
28. ISOC (2010) *The Internet Ecosystem*. Available at http://www.isoc.org/pubpolpillar/docs/internet-model.pdf [accessed 3 April 2011l].
29. Fiji Times Online (2010f) Fiji site crucial to US interests. *The Fiji Times Online*, 14 December. Available at http://www.fijitimes.com/story.aspx?id=161892 [accessed 3 April 2011].
30. Fong I (2010) *Broadband Public Consultation.*
31. Kim E (2009) *Welcome speech* [speech at ITU PACCERT stakeholder meeting]. 25 January, Nada Fiji. Available at http://www.itu.int/ITU-D/asp/CMS/Events/2009/PACCERT/ITU-Opening-PACCERT.pdf [accessed 23 April 2011].
32. Kirk J (2007) *Estonia recovers from massive denial-of-service attack. IDG News Service.* Available at http://www.networkworld.com/news/2007/051707-estonia-recovers-from-massive-denial-of-service.html [accessed 28th February 2011].
33. Kurbalija J (2010) *An Introduction To Internet Governance*. Malta: DiploFoundation.
34. Katayama L (2007) 2-Channel gives Japan's famously quiet people a mighty voice. *Wired*. 19 April. Available at http://www.wired.com/culture/lifestyle/news/2007/04/2channel [accessed 20 March 2011].
35. Luff E (2010) *in the OECD Report in* Sommer P and Brown I (2011). Reducing Systemic Cyber Security Risk. Available at http://www.oecd.org/dataoecd/57/44/46889922.pdf [accessed 15 March 2011].
36. Min Sun-Young (2010) Cyber war breaks out between Japan and South Korea. *IT Times*, 4 March. Available at http://www.koreaittimes.com/story/7635/cyber-war-breaks-out-between-japan-and-s-korea [accessed 20 March 2011].
37. MSNBC (2011) UK urges Nations to fight against cyber crime. Available at http://www.msnbc.msn.com/id/43645149/ns/technology_and_science-security/ [accessed 15 July 2011].
38. Office of the President, Republic of the Marshall Islands (2011) RMI response to libelous news item by CBS International. Available at http://www.rmigovernment.org/news_detail.jsp?docid=383 [accessed 25 March 2011].
39. Press Europ (2010) Portugal, cyber mafia playground. *presseurop*, 2 September. Available at http://www.presseurop.eu/en/content/news-brief-cover/329311-portugal-cyber-mafia-playground [accessed 20 March 2011].
40. Rabin O (2011) Revolution costs $30b to Egyptian economy *Globes Israel's Business Arena*, 13 February. Available at http://www.globes.co.il/serveen/globes/docview.asp?did=1000622702&fid=1725 [accessed 15 March 2011].
41. rediff NEWS (2011) CAUTION! How cyber mafia exploits Japan disaster. *rediff NEWS*, 15 March. Available at http://www.rediff.com/news/report/caution-how-cyber-mafia-exploits-japan-disaster/20110315.htm [accessed 20 March 2011].
42. Smith JC and Hogan B (1992) *Criminal Law.* London, Dublin, Edinburgh: Butterworths.
43. Sommer P and Brown I (2011) OECD/IFP Project on Future Global Shocks: Reducing Systemic Cyber Security Risk. Available at http://www.oecd.org/dataoecd/57/44/46889922.pdf [accessed 15 March 2011].
44. Tabureguci D (2007) *Pacific telephone number fraud victims get ITU sympathy*. Available at http://www.islandsbusiness.com/islands_business/index_dynamic/containerNameToReplace=MiddleMiddle/focusModuleID=18505/overideSkinName=issueArticle-full.tpl [accessed 3 April 2011].
45. United Nations (2010) *Small island developing states assess sustainable development progress*, Prospects in Third of Series of Meetings. Grenada, 16–18 March. Available at http://www.un.org/News/Press/docs//2010/dev2789.doc.htm [accessed 28 February 2011].
46. US Government (1986) United States Computer Fraud and Abuse Act of 1986. Available at http://www.wipo.int/wipolex/en/details.jsp?id=5768 [accessed 15 July 2011].
47. US National Security Council (no date) The comprehensive national cybersecurity initiative. *The White House*, no date. Available at http://www.

whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative [accessed 23 March 2011].

48. Vandrianavaly V (2009) European Commission DG INFSO-A3 Presentation on EU Policy on CIIP.
49. Wei Qiang CZ and Rossotto CM (2009) Economic Impacts of Broadband. In World Bank *2009 Information and Communications for Development 2009: Extending Reach and Increasing Impact.* Available at http://allafrica.com/sustainable/resources/view/00011823.pdf [accessed 22 April 2011].
50. World Future Online Political Islam Portal (2009) Manohara sparks Malaysia-Indonesia cyber war. *World Future Online Political Islam Portal*, 28 April. Available at http://wfol.tv/index.php?option=com_content&task=view&id=177&Itemid=1 [accessed 3 April 2011].