ABSTRACT
A downside of rapid digitization in developing Pacific Island Economies (DPIEs) is that they are becoming attractive for cybercrime activities. This study examines the diffusion and effects of cybercrimes in DPIEs to present a framework for evaluating such crimes in the contexts of geographic, economic, social and institutional issues facing them. We analyze DPIEs' position the global cybercrime ecosystem and evaluate the roles of various formal and informal institutions in facilitating or hindering cybercrimes associated with DPIEs. Also investigated in the paper are the natures of various externality mechanisms in the cybercrimes associated with these economies. Finally, the paper compares DPIEs' performance with various international benchmarks and discusses implications of cybercrimes associated these economies for the rest of the world.

Keywords: Cybercrime, Pacific Island Economies, institutions, arbitrage, externalities

1. INTRODUCTION
Recent developments in information and communication technologies (ICTs) such as high speed broadband, mobile phones, social media and cloud computing have potential to spawn economic, social and political changes in developing Pacific Island Economies (DPIEs). The late-comer DPIEs may compete successfully or even leapfrog early movers. Broadband, for instance, is likely to create opportunities in offshoring and other areas. Many local banks in DPIEs have started offering online services (Tabureguci, 2009). New services such as mobile banking have potential to transform traditional ways of living. However, a potential downside of the rapid digitization is that these economies are becoming attractive for cybercrime activities in terms of perpetration, instrument, and victimization.

DPIEs have become victims and targets of almost all types of cybercrimes. Some DPIEs have attracted global attention by occupying the position as major sources and facilitators of various forms of cyber-offences. ICT infrastructures of DPIEs have been used as instruments for committing international cybercrimes. The situation is likely to worsen with the increase in penetration and speed of broadband (Tabureguci, 2010).

In order to discuss the possible threats associated with DPIEs’ digitization to these economies and the outside world, we can draw from the lesson books of other developing economies. In this regard, some observations that are recently made on other rapidly digitizing developing economies are relevant to the contexts of DPIEs. One such observation concerns the threat of Africa’s “Cyber WMD” to the world economy with the continent’s increased broadband penetration (Gady, 2010). In sum, economies
such as those in DPIEs which are most likely to benefit from ICTs are also among the most vulnerable to ICTs’ negative impacts.

Organized criminal networks operate from areas of least resistance and control. DPIEs have been laggards in the enactment of cybercrime laws and their enforcements, which have created difficulties in dealing with offenders (AusCERT, 2008). Cybercriminals are also benefitting from inter-jurisdictional arbitrage. In the current context of DPIEs, for potential cybercriminals, the benefits of locating cybercrime activities in these economies are large and there is virtually no visible danger. Unsurprisingly, while there are phishing and other forms of international cybercrimes originated from these economies, most of them are not committed by DPIE residents.

The promotion of a safe cyberspace has been of paramount importance to DPIEs as the future of their digital activities will be subjected to increasing international pressures and greatly influenced by the evolution of new technologies. Noncompliant behaviors may create a negative international image and lead to political and economic sanctions. The lessons learned from DPIEs’ lax banking regulations in the past are that they are likely to be penalized for negative externalities they create for the rest of the world.

Associated dangers of digitization such as cybercrimes have not been completely explored or appreciated in the case of DPIEs. This study attempts to contribute to filling this void by analyzing the diffusion and effects of cybercrimes in DPIEs to present a framework for evaluating such crimes in the contexts of geographic, economic, social and institutional issues facing the DPIEs. This paper specifically addresses the following research questions:

RQ1: How are DPIEs positioned in the global cybercrime ecosystem in terms of penetration, victimization and instrumentation related to cybercrimes?; RQ2: What are the roles of various formal and informal institutions in facilitating or hindering cybercrimes associated with DPIEs?; RQ3: What are the natures of various externality mechanisms in the cybercrimes associated with DPIEs?; RQ4: How do DPIEs perform in comparison with various international benchmarks?; RQ5: What are the implications of cybercrimes associated with DPIEs for the rest of the world?

The findings would enable DPIE policy makers to understand the complex correspondence between physical and virtual locations and take measures to formulate ICT strategies. The analysis would also help assess DPIEs’ vulnerability and readiness to deal with the next wave in cybercrimes, especially those involving social media and cellular technologies.

Before proceeding, some clarifying definitions are offered. Cybercrime is defined as a criminal activity in which computers or computer networks are the principal means of committing an offense or violating laws, rules, or regulations (Kshetri, 2009). By developing Pacific Island Economies, we mean developing economies consisting of the Pacific Islands in the south of the tropic of Cancer.

The remainder of the paper proceeds by first examining digitization of DPIEs and
cybercrimes associated with these economies. Next, a framework for explaining cybercrimes associated with DPIEs is presented. It is followed by a section on discussion and implications. The final section provides concluding comments.

2. DIGITALIZATION OF DPIES AND CYBERCRIMES ASSOCIATED WITH THESE ECONOMIES

2.1. DIGITALIZATION OF DPIES

Although DPIEs’ digitization started relatively late, their progress on this front has been striking (Table 1). Telecommunications in these economies have undoubtedly progressed beyond narrowband voice and single-kilobit/second Internet. Many DPIEs have been connected to sub-marine cables. Most DPIEs have or are in the progress of getting high speed broadband connections and advanced cellular networks. For instance, Vanuatu mainly relies on the satellite for Internet connection. Interchange and Alcatel-Lucent are planning to launch undersea optical fiber backbone cable linking the country to Fiji at a cost of US$30 million. At first, the system will be equipped to handle 20 GB/sec, which is about 200 times the country’s current capacity. Over time, it is expected to increase to 320 GB/sec (Murph, 2011).

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>Early 1990s</td>
<td>Limited email services became available in some DPIEs.</td>
</tr>
<tr>
<td>1996</td>
<td>Full Internet services established with a six-month initiated by Telecom Fiji. It was connected via the University of Waikato in New Zealand.</td>
</tr>
<tr>
<td>2000</td>
<td>Launch of the Southern Cross cable, which linked Australia and New Zealand with Hawaii and included a landing in Fiji.</td>
</tr>
<tr>
<td>March 2003</td>
<td>The Internet Users Society - Niue launched free broadband Internet services for the local Internet community at its Internet Cafe.</td>
</tr>
<tr>
<td>June 2003</td>
<td>Cable &amp; Wireless announced plans for a $0.5 billion project to cable DPIEs. This included undersea fiber cable links to Papua New Guinea, the Solomon Islands, New Caledonia, Vanuatu, Fiji, Samoa, Tahiti, Norfolk Island, Tonga, the Cook Islands, Nauru, Tuvalu and Tokelau.</td>
</tr>
<tr>
<td>2003</td>
<td>Tonga enacted Computer Crimes Act 2003, which defines computer-related offences.</td>
</tr>
<tr>
<td>2004</td>
<td>Kiribati’s Telecommunications Act 2004 includes a section on computer Misuse.</td>
</tr>
<tr>
<td>June 2008</td>
<td>The Marshall Islands experienced a two-day loss of all external email due to a denial of service attack.</td>
</tr>
<tr>
<td>2008</td>
<td>Samoa enacted Electronic Transactions Act 2008, which also covered the legal recognition of communication and ownership of electronic records.</td>
</tr>
<tr>
<td>2009</td>
<td>Fiji included computer offences in the 2009 Crimes Decree under Section 336.</td>
</tr>
<tr>
<td>April 2011</td>
<td>Vanuatu’s Interchange Limited and Alcatel-Lucent signed an agreement to deploy Vanuatu’s first international submarine cable system linking Port Vila, Vanuatu, to Suva, Fiji. It is scheduled to be completed in mid-2012.</td>
</tr>
</tbody>
</table>

*Network Strategies (2010); †Fiji Times (2009); ‡APNIC (2004); §APNIC (2004); ¶Zwimpfer (2004).
Most impressive of all, the rural population is realizing the benefits of ICTs. For instance, Solomon Islands and Secretariat of the Pacific Community (SPC) have teamed up to launch satellite broadband internet access in rural centers to improve government service delivery. The government will use Pacific Rural Internet Connectivity System (PacRICs) to provide internet access to over 20 hospitals and schools (Rufino, 2011).

2.2. DPIES AND CYBERCRIMES

The global cybercrime industry serves as a starting point for a discussion of cybercrime activities in DPIEs. In this regard, by all accounts, the global cybercrime industry is much bigger than most of the major and well-known underground and underworld industries such as illegal drugs trade and human trafficking\(^1\). The most often cited figure for the annual worldwide loss to cybercrime is US$1 trillion\(^2\).

Moving to the specific context of DPIEs, while both the Internet and cybercrime are a more recent phenomenon, their growth rates have been striking. Some DPIEs are widely considered as economies among the most unsafe cyberspace behaviors that are internationally notorious for high levels of cybercrime activities. A SiteAdvisor study in 2007 indicated that Tokelau (.tk) had among the world’s largest proportion of domains infected with malware. One reason was that one can get a .tk domain for free and set it in a day (Patrizio, 2007). Likewise, Tokelau earned a 10.1% risk rating in 2007 compared to 4.1% for all websites (McAfee, 2008). In the second quarter of 2010, 2533 attacks originated from Tokelau and about 95% were launched from legitimate .tk domains while the rest were launched from hacked .tk websites (Pauli, 2011).

It is also apparent that businesses and individuals in DPIEs are becoming victims of diverse forms of cybercrimes. According to the Fiji police, cybercrime in the country started in 2000 and has been growing rapidly since then (SPAMfighter News, 2007). In 2009, Fiji’s police cybercrimes unit spokesman Jemesa Lave noted that cybercrimes in the country would grow by 50% within the next two years (newslinkservices.com, 2009).

A Microsoft-sponsored computer crime and security survey conducted in 2008 revealed that about a third of the organizations in DPIEs had become victims of cybercrimes and 15% of them had experienced more than 10 attacks. The survey also indicated that half of the respondents had become victims of Nigerian-style cyber scams (Phair 2008).

As of 2009, two DPIEs had been hit at national levels with distributed denial of service (DDOS) attacks, bringing national internet email grid to a halt for several days. Cybercrimes created a major disruption of nationwide telecoms systems of the Marshall Islands, which suffered a two-day loss of all external email due to a denial of service attack (Network Strategies, 2010).

There are reports of phishing attacks targeting local banks which has caused a great deal of customer anxiety. One bank had issued warning to its customers (pita.org.fj, 2009). In Fiji for instance, online banking users are reported to receive emails that pretend to come from the local branches of Westpac and ANZ banks, telling them to log
on to a site and update information online (Tabureguci, 2009).

In addition to extrinsically motivated cybercrimes, these economies are also experiencing intrinsically motivated cybercrimes. For instance, it was reported that a team of police officers was investigating a suspected pedophile ring operating in DPIEs, which allegedly reached children via social networking sites (Tabureguci, 2007). In 2001, a disgruntled former employee of Fiji’s Information Technology Centre in Suva office entered in the main server room and could change the administrative passwords, which prevented ITC staff to access the system (Fonua, 2002). Cyber bullying and other social media-related crimes are also rising in these economies.

Overall, DPIEs’ current major problem is mainly one of origination and facilitation of cybercrime activities. With the rapid broadband diffusion and the digitization of economic activities and in line with worldwide trends, cybercrime victimization rates in these economies are likely to escalate.

2.2.1. INTERNATIONAL CYBERCRIMES ASSOCIATED WITH DPIES

DPIEs seem to provide a fertile ground for carrying out criminal activities. Cyberspaces of some DPIEs have acquired a reputation as among the world’s most dangerous and these economies are referred as cybercrime heavens or cybercrime capitals. In a study, a search of the domain registry for top child porn sites by BusinessWeek reporters showed that some of the most notorious owners were based in Tonga (Sager et al., 2002).

Many organized crime groups have typically used DPIEs as staging points for their crime operations. For instance, according to a 2008 report published by the security company, Sophos, in terms of spam generation per capita, the world’s top three economies were Pacific Island economies: Pitcairn Island (.pn), Niue and Tokelau (itsecurity.com, 2008). According to the Anti-Phishing Working Group, in the second half of 2010, .tk domain name came second only to .com in terms of malicious registrations (The Sydney Morning Herald, 2011).

As another example of international cybercrimes associated with DPIEs, in 2008, cybercriminals created fake websites involving .tk, which pretended to be of the UAE Ministry of Education (www.ministryofeducationuae.tk) and Ministry of Labor (www.uaeministryoflabour.tk) to dupe unsuspecting job seekers. They lured teachers from all over the world to apply for job vacancies that did not exist and asked the potential applicants to pay a visa fee (Menon, 2008).

Some firms are taking advantage of weak industry specific legislations to engage in cybercrime activities by locating their businesses in DPIEs. A study conducted by the WHO found that Micronesia and Tonga had loopholes in legislation which have allowed companies and individuals to import and wholesale pharmaceutical products without a license (WHO Drug Information, 2001). This would allow criminal enterprises to establish rogue Internet sites and operate with ease.
There are also instances in which DPIEs are used by international cybercriminals to launder cybercrime proceeds. In one such example, cybercriminals stole more than $685,000 from the superannuation fund of 121 individuals in Australia. The fund was transferred to the Philippines and some DPIEs using low-value international funds transfers (Fife-Yeomans, 2011). In another case, cyber Crime Investigations Unit of Fiji police reported that three people in Fiji were working in partnership with foreign nationals to launder money by using Fiji as a transit point (Scheiche, 2011). The Fiji residents were recruited through popular social networking sites.

3. A FRAMEWORK FOR EXPLAINING CYBERCRIMES ASSOCIATED WITH DPIES

3.1. INSTITUTIONS RELATED TO CYBERCRIMES IN DPIES

The nature of activities of cyber-criminals fits squarely with what Baumol (1990) calls destructive entrepreneurship. Baumol (1990) hypothesized that the distribution of productive, unproductive, and destructive entrepreneurs in a society is a function of the “relative payoffs” offered to these activities by the society’s “rules of the game”. These rules are also referred as formal and informal institutions, which embed economic activities and actors (Granovetter, 1985; North, 1990; Parto, 2005). These institutions in the context of DPIEs’ cybercrime landscape are discussed below.

3.1.2. Formal institutions

DPIEs are characterized by weak formal institutions against cybercrimes. They lag behind the curve in enacting and enforcing cybercrime related regulative laws and have very little legislation specific to cybercrime and cyber-security (Ahmadu, 2006; Angelo, 2009). In many DPIEs, hacking someone’s computer over a network connection is not yet considered as a crime. The most often cited case was that of an expatriate in 2008, who went to Fiji and engaged in a number of cybercrime activities with impunity. He accessed local firms’ networks in an unauthorized manner (Tabureguci, 2010).

While some have enacted cybercrime laws, they have little capacity to enforce them. According to the Pacific Islands computer crime & security survey in 2008, perpetrators were charged with an offence only in 5% of the reported cases. Factors such as inadequate legislation, insufficient evidence and international jurisdictional issues were among the most critical barriers to act on the reported cases (Phair, 2008). Siaosi Sovaleni, a manager at the ICT Outreach Program of Secretariat of the Pacific Community (SPC) under the Economic Development Division recently put the issue this way: “Measures include criminal law and criminal justice action. Currently, most island states of the Pacific region are not sufficiently equipped to protect their societies against cybercrime through criminal law, nor are they in a position to engage in efficient international cooperation in this respect” (MIC, 2011).

3.1.2. INFORMAL INSTITUTIONS

There has been a low level of awareness among governments, businesses and consumers about cybercrimes and protection measures. One expert noted: “It (awareness) is still pretty low, as most enforcing agencies and legal agencies are not
aware of the issues, let alone have the tools to fight” (Tabureguci, 2009). In general, proportionally less cybercrime activities are reported than conventional crimes. According to the Pacific Islands computer crime & security survey conducted in 2008, only 20% respondents reported cybercrime incidents to law enforcement agencies (Phair, 2008).

**Industry and trade/professional associations**

Various professional and trade associations as well as non-governmental organizations in DPIEs, which can be considered as informal institutions, are constantly emerging and influencing organizations and individual behaviors in new ways as a result of their expertise and interests in this issue. For instance, the non-profit organization, Pacific Islands Telecommunications Association (PITA) has made efforts to provide ICT and security awareness trainings to its members (AusCERT, 2008). Likewise, the Pacific Internet Society (PICISOC) is concerned with what it believes is the lack of awareness in the Pacific region of identity theft (Tabureguci, 2009). In an attempt to create cyber-security awareness, PICISOC is working on Internet Trust and Identity. An ad hoc group meets regularly to exchange cyber security information. PICISOC members also created an Advisory on 'Identity Theft' attacks (http://www.miniwiki.org/wiki/index.php?wiki=content.www.picisoc.org%2Fphishing). Likewise, in April 2011, SPC teamed up with the Australian Government, the Council of Europe and the Government of Tonga to organize a cybercrime workshop.

### 3.2. EXTERNALITY MECHANISMS ASSOCIATED WITH CYBERCRIME

According to Demsetz, “[e]very cost and benefit associated with social interdependencies is a potential externality” (1967, 348). Put differently, economic actors with interdependent relations jointly produce an externality and whether it is positive or negative is a function of how it is produced and who produces it (Frischmann & Lemley, 2007). To put things in context, DPIEs and the world economy may experience various types of externalities as a result of a unique combination of economic, socio-political and cognitive feedbacks. Table 2 presents the nature of feedback systems in DPIEs that generate externalities via various mechanisms.

#### 3.2.1. FEEDBACK SYSTEMS

**Economic feedbacks**

A central feature of the Internet economy is a near zero transaction cost. Among DPIEs, Niue began offering .nu domains for free in 1997. Tokelau domain names are also free. Tokelau sold its .tk domain name to the Dutch company, BV Dot TK, which provided the island with free high speed broadband and royalties from the domain sales is estimated to be "a few thousand dollars" each year (Pauli, 2011). Thus an appealing combination for a cybercriminal is to combine the low transaction costs of with low “production” costs due to free domains. Moreover, Niue allows anonymous domain registration (Lincoln, 2007). Cybercrime associated with anonymous domains are low-risk. Overall, cybercrimes’ significant financial benefits, low costs (free domain names) a low probability of being caught and prosecuted (due to inter alia anonymous domain names and weak laws and enforcement mechanisms) give them a high positive
economic feedback (Becker, 1995; Kshetri, 2006). Free domain names have a magnetic attraction for cybercriminals. Thanks to free domain names, .tk has become the third largest country code top-level domain only behind .de (Germany) and .uk (the U.K.) (The Sydney Morning Herald, 2011). As of the mid-2011, Tokelau had more than 4 million registered domains for a population of 1400 residents (Pauli, 2011).

**Sociopolitical feedbacks**

Sociopolitical feedbacks are related to formal and informal institutions (North, 1990; Scott, 2001). Due to increasingly transnational and international nature, cybercrimes benefit from jurisdictional arbitrage. Organized cybercrimes are initiated from countries with few or no laws and little enforcement capacity.

While the virtual world of DPIEs’ has globalized rapidly, these economies’ integration with the outside world is limited. For instance, Vanuatu is not a member of the world trade organization (WTO) and the country is not obligated to comply with the Agreement on Trade Related Aspects of Intellectual Property Rights (TRIPS). While many forms of cybercrimes are associated with and facilitated by infringements of intellectual property rights (IPR), Vanuatu has no IPR enforcement mechanisms.

Some DPIEs’ jurisdictions offer attractive risk/reward profiles for locating firms engaged in or facilitating cybercrime activities. Among the six countries blacklisted by the Organization for Economic Cooperation and Development in April 2002, three were DPIEs: the Marshall Islands, Nauru and Vanuatu (Olson, 2002). An example of illegal and extra-legal firms using jurisdictional arbitrage to evade laws is Kazaa, the popular file-sharing service, which made money principally by bundling its clients with adware and spyware. Embroiled in legal difficulties, in the U.S. and in Europe, it was sold to Sharman Networks for $500,000 in January 2002 (Vitzthum & Konsynski, 2009).

Sharman Networks was incorporated in Vanuatu but the identities of the real owner and operator of Kazaa were hidden in a maze of corporate entities. Vanuatu has absolute respect for the secrecy of companies and such information is legally protected from disclosure in the country. Vanuatu is considered as a tax haven as it does not levy income tax, and has no tax treaties with other countries (Healey, 2002). The country imposes prison terms to any party disclosing financial information (Sharman, 2010). This means that Kazaa also avoided paying taxes on its advertising revenue, which was estimated as $60 million a year (Sharman, 2010). A related point is that Vanuatu and other DPIEs’ are less likely to receive help from law enforcement agencies of wealthier neighbors due to their alienation from the latter. In addition, most DPIEs have no extradition treaties with most of the world economies, which makes them ideal places to commit cybercrimes targeting victims all over the world as (Tabureguici, 2010).

Institutional development in DPIEs is taking place more slowly. Cybercrimes’ newness presents challenges to the court systems in DPIEs. Also explaining cybercrimes to judges is a difficult task in these economies. This problem is further compounded by the fact that there are traditional types of court systems operating at the village level such as Tikina Courts in Fiji or local customary courts known as Island Courts in Vanuatu (UN, 2004). As to the informal institutions, the level of stigmatization of cybercriminals has not been so great in DPIEs.
Cognitive feedbacks

The cognitive feedback loops are associated with cognitive programs that are built on the mental maps of individuals engaged in cybercrime activities and thus function primarily at the individual level. Factors such as the novelty of the technology, a lack of previously developed mechanisms and established codes, policies, and procedures; and non-existence of an easily identifiable victims are likely to lead to much less in cybercrimes guilt compared to conventional crimes.

The cyberspace provides a variety of opportunities to commit crimes. Like the rest of the world, pervasiveness and ease of use of tools such as social media and instant messaging have led to an increase in peer-to-peer harassment and cyberbullying in DPIEs. In August 2011, two Facebook groups (anti Labasa club’ and anti-Suva’) in Fiji were found to make derogatory, defamatory, discriminatory and offensive comments about residents of Suva and Labasa districts. Most of the offenders in the acts were believed to be high school students (radiofiji.com.fj, 2011).

3.2.2. EXTERNALITY MECHANISMS

Inefficiency and congestion in the law-enforcement system

Law-enforcement systems in DPIEs are characterized by congestion and inefficiency due to, inter alia, the lack of law enforcement resources, scale of crimes, newness of cybercrimes, a low-governmental priority, a lack of cross-border and industry–government cooperation, and victims’ unwillingness to report (Jones, 2007; Kshetri, 2006). It is suggested that there is “a significant break down in law and order” in DPIEs (Tabureguci, 2010). Conventional crimes such as those involving drug trafficking have overburdened law-enforcement agencies. For instance, Fiji’s ex-Police Commissioner, Andrew Hughes noted that transnational organized crime groups have used the country as a “staging ground” for illegal activities (Keith-Reid, 2004).

Due to capacity and resource constraints, technological and organizational capabilities required to operate safe online systems are costly and difficult to procure for the DPIEs (UN, 2004). The governments are facing challenges to develop updated ICT policies and legislation, including cybercrime policies. Only a small proportion of law enforcement agencies, lawyers, Judiciary members and their staff are familiar with laws related to e-commerce and cybercrime (UN, 2004). Inefficiency and congestion in the law-enforcement system in DPIEs generate positive externalities for criminals and negative externalities for the society (Gaviria, 2000; Sah, 1991).

Technology and know

Various technological and know-how-related factors have attracted cybercriminals in virtual spaces associated with DPIEs. While free domain names perform poorly in terms of functionality, they are more than sufficient for carrying out most cybercrime functions. For instance, .tk and .nu domain names do not provide FTP access and users are not allowed to specify their own DNS servers. They use a simple redirect script to point to another address. They are popular with webmasters on free hosting and also for
renaming long URLs (internetblog.org.uk. 2009). While these domains may not be appropriate for performing cybercrime functions requiring sophisticated functionality, performance and direct interfaces, they are sufficient for most cybercrimes such as phishing and sending spams (internetblog.org.uk, 2009).

Criminals, irrespective of their focus, may generate externalities by making crime-related specialized knowhow, inputs and services available, forming a specialized “labor market”; and facilitating the exchanges and spillovers of information and technology (Marshall, 1920). In this regard, criminal enterprises have created agglomeration economies in DPIEs for the production, trafficking and trade in illegal drugs (Reid et al. 2006). The presence of such agglomeration economies is likely to facilitate “inter industry knowledge spillovers” (between illegal drug industry and cybercrime industry). Such spillovers are referred as Jacobs externalities (Jacobs 1969).

**Predisposition and propensity to commit cybercrimes associated with DPIEs**

There has been an increase in predisposition and propensity to commit cybercrimes targeting to and/or originating from DPIEs. DPIEs’ lax regulations in virtual space, coupled with tighter regulations in some economies such as China, have caused many foreign cybercriminals to use domain names associated with DPIEs to commit various cybercrimes. For instance, it was found that most phishing activities associated with .tk domain names actually originated from China and also targeted Chinese e-commerce sites. Estimates suggest that 80% of Tokelau-registered names used for phishing were targeting Chinese institutions (Field, 2011). While 28% of the phishing domains worldwide were registered for malicious purposes, 100% domain used for phishing associated with .tk was maliciously registered (Rashid, 2011).

Since 2009, China’s new rules do not allow individuals to register .cn domains. To register for businesses, it is required to submit a copy of the business license. The number of phishing attacks from .cn domains targeting Chinese businesses reduced from 2,826 from 228 domains in the second half of 2009 to 162 from 120 domains in the second half of 2010. Tighter regulations in China forced Chinese fraudsters to find poorly regulated top-level domains such as .tk for phishing activities (Rashid, 2011).

<table>
<thead>
<tr>
<th>Externality mechanisms ⇒</th>
<th>Inefficiency and congestion in the DPIEs’ law enforcement system</th>
<th>Technological, and know-how-related factors attracting cybercriminals in virtual spaces associated with DPIEs</th>
<th>Increased predisposition and propensity to commit cybercrimes targeting to and/or originating from DPIEs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feedback system ↓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Economic</td>
<td>• Law enforcement agencies’ lack of resources and competencies to fight cybercrimes.</td>
<td>• Improving connectivity in DPIEs is attracting cybercrimes.</td>
<td>• Availability of free domain names—cheap/free web addresses appeal to scammers since they</td>
</tr>
<tr>
<td></td>
<td>• Conventional crimes have</td>
<td>• Criminal enterprises have created</td>
<td></td>
</tr>
</tbody>
</table>
overburdened law-enforcement agencies.

agglomeration economies-- Jacobs externalities.

need to switch domains often as they are constantly blacklisted.

Sociopolitical
- Weak cybercrime laws in DPIEs.
- Jurisdictional arbitrage.
- Some DPIEs’ are less likely to receive help from foreign law enforcement agencies due to their alienation.

Cognitive
- Victims’ unwillingness to report cybercrimes: low reporting rates
- Ease of use of tools to commit cybercrimes (e.g., social media and instant Messaging have facilitated peer-to-peer harassment and cyberbullying).
- Less guilt in cybercrimes.

3.3. CONTROLS, RESTRICTIONS AND REGULATIONS AGAINST CYBERCRIMES

While legitimate firms strive to build public confidence in the value of their products and services, which would facilitate the firm’s efforts to attract customers and obtain their loyalty and patronage for the long term, cybercrime firms must overcome and avoid various controls, restrictions and regulations set and enforced by governments, potential victims and other actors. Regulation is defined as “controlling human or societal behavior by rules or restrictions” (Koops et al., 2006, p. 81). Various forms of regulations include the government’s legal restrictions, self-regulation, social regulation (e.g. norms), co-regulation and market regulation. Formal and informal institutions provide various offensive and defensive control mechanisms against cybercrimes. Individual internet users’ defense and control mechanisms play an important role.

In addition, de jure or de facto guardians in the private sector such as ISPs, IT security companies, technology providers as well as possessors of assets in digital/digitizable forms (e.g., financial institutions) can help regulate cybercrime activities. As evidenced and revealed by various security breaches, these actors have been ineffective to control cybercrimes in DPIEs. In 1999, some students at the University of the South Pacific in Suva, Fiji hacked the University’s system, retrieved other students’ passwords, and sent abusive messages to others using the hacked email accounts (Fonua, 2002). Likewise, in the early 2000s, hackers exploited a security hole in the system of Kalianet, an ISP in Tonga to crack the password system. They could get free access to the internet and had information about most of the emails (Fonua, 2002). In sum, the various forms of controls and regulations are currently weak in DPIEs. Nonetheless, some of them are improving (Table 3).
Table 3: Various forms of controls for cybercrime activities in DPIEs

<table>
<thead>
<tr>
<th>Actors</th>
<th>Nature of control</th>
<th>Improving signs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Government</td>
<td>• Weak cybercrime laws and enforcement mechanisms</td>
<td>• Collaboration with neighboring countries (e.g., Australian law enforcement agencies helping Fiji)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Collaboration with supranational agencies: Interpol conducted a workshop against cybercrime in Fiji in 2009 (Brennan, 2009).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Some have made significant progress in cybercrime legislation (e.g., Tonga’s Computer Crimes Act 2001).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Some measures are taken to educate judges and law enforcement agencies.</td>
</tr>
<tr>
<td>Potential victim</td>
<td>• Lack of awareness of cybercrimes (Tabureguci, 2009).</td>
<td>• Measures are being taken at various levels to create cybercrime awareness</td>
</tr>
<tr>
<td></td>
<td>• Two thirds of organizations considered their managers’ IT security qualification, training, experience and awareness insufficient (Phair 2008).</td>
<td></td>
</tr>
<tr>
<td>Control by informal institutions (social control)</td>
<td>• Underdeveloped ethical, moral, and social values against cybercrime.</td>
<td>• PICISOC is working to create cybersecurity awareness.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• PITA has made efforts to provide ICT and security awareness trainings to its members</td>
</tr>
<tr>
<td>De jure or de facto guardians in the private sector (ISPs, IT security companies, technology providers possessors of assets in digital/digitizable forms (e.g., financial institutions)</td>
<td>• Small anti-virus market</td>
<td>• Some banks have enhanced security measures.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• IT security companies such as AVG have an active presence in DPIEs (cso.com.au, 2011).</td>
</tr>
</tbody>
</table>

4.0. DISCUSSION AND IMPLICATIONS

DPIEs are digitizing rapidly. However, apart from desired effects of high economic production efficiency and improvement in political and social life, negative side effects have become apparent. In this regard, the above discussion provides an assessment of how their position vis-à-vis other developing and industrialized countries is likely to change over time and with increasing digitization.

Given DPIEs’ heterogeneity, a one size fits all approach may not work to tackle and address cybercrime problems. There is a wide variation among the DPIEs in terms of levels and patterns of cybercrime activities and associated factors. While many DPIEs have no specific cybercrime legislation, some have made significant progresses. In the same vein, creating awareness about cybercrimes may be a cost-effective approach for
relatively large DPIEs such as Fiji, Samoa and Vanuatu, but not for smaller economies in the regions such as Kiribati, Nauru, Niue and Tokelau (UN, 2004).

Due to various forms of cyber-offenses associated with DPIEs, the benefits and power of ICTs have not been fully utilized in these economies. The above discussion would help incorporate cybercrime related elements in their ICT strategies and take other measures to promote a safe cyberspace. This is important as restoring and preserving reputations and image tarnished by lax regulations in the past is of paramount importance for some DPIEs.

A consideration of behavioral and technological defense mechanisms in these economies is important. Individual and organizations who connect to the Internet without strong defense mechanisms create negative externalities by such activities as facilitating the generation spam, hosting phishing sites and distribution of illegal and objectionable contents. Prior research has indicated that organizations in developing countries that are adopting the Internet without considering the costs and efforts needed to secure the systems have generated a negative externality (Otis and Evans, 2003). Some ISPs in industrialized countries reportedly block contents originated from problematic networks based in DPIEs and other developing countries (Garfinkel, 2002).

To understand drivers and effects associated with cybercrimes in the DPIEs, let us revisit the research questions posed in the beginning (Table 4). Most DPIEs offer an attractive inter-jurisdictional arbitrage for cybercriminals to locate virtual and physical activities. Weak formal institutions against cybercrimes in these economies also offer an attractive benefit/cost ratio for cybercrime organizations. Factors such as congestion and inefficiency in law-enforcement systems, availability of free domain names that are more than sufficient for carrying out most cybercrime functions, agglomeration economies for the illegal drugs industry permit cybercriminals to benefit from positive externalities. Cyber-offenses’ tremendous economic costs are likely to affect bandwidth-starved nations such as DPIEs disproportionately. Finally, if other economies tighten laws and enforcement mechanisms against cybercrime, cybercriminals are likely to be pushed to operate from DPIEs. DPIEs’ role as instruments of such crimes may lead to rejection from and ostracization by developed countries.

Table 4: Revisiting the research questions

<table>
<thead>
<tr>
<th>Research questions</th>
<th>Our findings</th>
</tr>
</thead>
</table>
| RQ1: DPIEs' position in the global cybercrime ecosystem | - Cybercriminals benefitting from inter-jurisdictional arbitrage: large benefits to locate cybercrime activities in these economies and there is virtually no visible danger.  
  - Most cybercrimes associated with DPIES are not committed by their residents.  
  - Underdeveloped IT industries and lack super hacker skills.  
  - Increasing digitization is likely to make DPIEs more attractive targets. |
| RQ2: Nature of formal and informal institutions | - Weak formal institutions against cybercrimes-- a lack of cybercrime legislation in some DPIES.  
  - Low level of awareness among governments, businesses and consumers about cybercrimes and protection measures: A lack of effective Internet |
safety groups to educate users on cybercrimes (Tabureguci, 2007).

- Only a small proportion of cybercrimes are reported to law enforcement agencies.

| RQ3: Externality mechanisms | Law-enforcement systems are characterized by congestion and inefficiency-- the lack of law enforcement resources, scale of crimes, newness of cybercrimes, a low-governmental priority, a lack of cross-border and victims’ unwillingness to report-- Conventional crimes have overburdened law-enforcement agencies.  
- While free domain names perform poorly in terms of functionality, they are more than sufficient for carrying out most cybercrime functions.  
- Agglomeration economies for the production, trafficking and trade in illegal drugs: inter industry knowledge spillovers or Jacobs externalities  
- Increasing pervasiveness and ease of use of tools such as social media and instant messaging have led to an increase in peer-to-peer harassment and cyberbullying. |

| RQ4: DPIEs’ comparison in terms of cybercrime impacts and its ingredients with various international benchmarks and trends | Cyber-offenses’ tremendous economic costs affect bandwidth-starved nations disproportionately: potential downsides large and costly: a high degree of vulnerability to cybercrime-- reliance on the Internet for emergency management and disaster recovery, limited or no redundancy in ICT infrastructure, a lack of knowledge, ability and experience to deal with cyber-attacks, and thin and dysfunctional formal and informal institutions. |

| RQ5: Implications for the rest of the world | If other economies tighten laws and enforcement mechanisms against cybercrime, cybercriminals are likely to be pushed to focus on DPIEs.  
- DPIEs’ role as instruments of such crimes may lead to rejection from and ostracization by developed countries. |

We make the following additional observations:

**4.1. DPIES’ UNUSUAL AND IDIOSYNCRATIC FEATURES FROM THE STANDPOINT OF CYBERCRIMES**

DPIEs have unique cultural, educational and social dispositions and orientation and many unusual and idiosyncratic features in the geopolitics of cybercrimes. They demonstrate a high degree of vulnerability to cybercrime due to, inter alia, a high reliance on the Internet for emergency management and disaster recovery, limited or no redundancy in ICT infrastructure, a lack of knowledge, ability and experience to deal with cyber-attacks, and thin and dysfunctional formal and informal institutions to deal with offenders (Network Strategies, 2010).

Cyber-offenses such as spam have the tremendous economic costs which affect bandwidth-starved nations such as DPIEs and landlocked countries. They suffer disproportionately from the clogging of their networks. The needs of these countries are often ignored or unacknowledged in international forums (ORDIG, 2005). The same seems to be true in international cybercrime related initiatives.

**4.2. PATH DEPENDENCE AND CYBERCRIME IN DPIES**

The path dependence approach argues that different events steer history in a particular direction, which can influence the path a technology undertakes (Arthur, 1988; North, 1990). Some DPIEs were among the easiest and cheapest ways to enter international
banking. In the 1990s, Nauru, Niue and Vanuatu encouraged the proliferation of rogue banking activities as a fast way to quick wealth (Wechsler, 2001). Nauru allowed anyone to set up banks for as little as $25,000 without the physical presence of the founders. In 1998 Russian criminals reportedly laundered about US$70 billion through 450 banks in Nauru (Seneviratne, 2000). Likewise, in 1999, in the US$7 billion money laundering scandal at Bank of New York, half allegedly went through Nauru. Consequently, Nauru suffered arguably the harshest sanctions imposed on any country, including those against Iraq and Yugoslavia. Western banks including Deutsche Bank and Bankers Trust do not permit dollar-denominated transactions involving Nauru. Hitt (2000) forcefully argued: “In the digital age, this action packs the same wallop as an old-fashioned gunboat blockade”. In 1999, Palau and Vanuatu were blacklisted by international banks over similar concerns (Ranmuthugala, 2001). Since the Internet has facilitated money laundering, DPIEs’ history makes them especially vulnerable.

Bank secrecy is becoming slowly eroded and diluted in economies such as Switzerland and the Cayman Islands. Criminals involved in online money laundering are finding DPIEs such as Nauru increasingly attractive thanks to their underregulated financial systems (Wasserman, 2002)

History has repeated itself. Some have considered the Internet as a heaven-sent opportunity to make quick money with minimum efforts and engaged in activities such as the establishment of Internet gambling, and renting or selling the cyberspace. If poorly implemented in practice, these strategies have potential to backfire by attracting unproductive and destructive entrepreneurial activities rather than the productive ones.

4.3. POSITIVE AND ENCOURAGING SIGNS

Some positive and encouraging signs have begun to emerge in DPIEs’ cybersecurity landscape. It is apparent that there have been efforts to build formal and informal institutions. For instance, many DPIEs have enacted laws to encompass key concepts in international conventions against cybercrime. Some DPIEs have strengthened their regulative institutions through international collaboration and partnership. In 2007, the Fiji police requested the help of two Australian federal police officers to investigate over 120 cybercrime cases (SPAMfighter News, 2007). As of 2009, Fiji’s special cybercrime unit had two cyber forensics specialists, a certified application forensics specialist, a mobile forensics specialist and 13 additional experts (newslinkservices.com, 2009).

Policy makers as well as businesses in the region have emphasized the importance of cybercrime education to the community and customers (vanuatunews.com, 2011). Businesses have provided an added measure of safety, security and control to the user. In the early 2010, the Australia and New Zealand Banking Group (ANZ) launched security features for internet banking in Fiji including data encryption, firewalls and the latest security technology (fijilive.com, 2010). ANZ educates consumers about online threats such as phishing, spyware, adware, viruses and worms, Trojans (e.g., ttp://www.anz.com/samoa/en/personal/ways-bank/internet-banking/protect-banking/internet-security-threats/). In June 2011, National Bank of Samoa (NBS) published Security Alerts warning its customers that they have been targeted with phishing emails which led them to fake bank websites (nbs.ws 2011). Similar alerts
were issued by ANZ banks for its customers in Tonga and other DPIEs (http://www.anz.com/tonga/en/personal/ways-bank/internet-banking/protect-banking/security-alerts/).

5. CONCLUDING REMARKS

Strengthened laws and enforcement mechanisms in some countries are pushing criminals to DPIEs, which have both the virtual and the physical environments under-regulated. Especially, criminals are finding DPIEs’ cyberspace as an attractive location for committing crimes. There are clusters of criminal organizations around virtual spaces associated with DPIEs.

DPIEs have underdeveloped IT industries and lack con artists or super hacker skills as found in cybercrime hotspots such as Nigeria, Russia and other former Soviet economies. Some DPIEs, nonetheless, have bad international reputation and image due to cybercrimes associated with them. Cheap and free domains appeal to scammers since they need to switch domains often because they are constantly being blacklisted. While some forms of cyber-offenses may not harm these economies, their role as instruments of such crimes may lead to rejection from and ostracization by developed countries. Some domains such as .tk and .nu are stigmatized, which are likely to face barriers to carry out legitimate e-commerce functions for businesses and government.

The potential downside associated with cyber-attacks can be large and costly to DPIEs. They need to incorporate lessons learned from their past mistakes, failures and experiences in the development of cyber strategy. The associated costs might outweigh the benefits in the absence of proper regulations. In this regard, DPIEs such as Tokelau (.tk) and Niue (.nu) can learn from the experience of Pitcairn Island’s efforts to win back its TLD from a Channel Islands- based company in 2000 (Lincoln, 2007).

While there have been many unfocused initiatives and piecemeal approaches to develop cybercrime related institutions, what DPIEs really need are customized programs that directly support the exact needs of various categories of professionals dealing with cybercrimes such as attorneys, judges and law enforcement agencies. Finally, it is especially important for DPIE youths to be exposed to the importance of cybersecurity, which is likely to promote safe online practices.

REFERENCES


Arrow, K. J. (1962). The economic implications of learning by doing. Review of


internetblog.org.uk.(2009,May 11) 15 Millionth .TK Domain Registered, Retrieved from 

itsecurity.com (2008 March 12th) Pacific Islands Infested with Spam, Retrieved from 
  ⟨http://www.itsecurity.com/blog/category/malware⟩


Scheiche, R. J. (2011, August 12). Cops Probe Cyber Crime, Retrieved from 


Menon, V (2008, December 4) Cybercriminals still targeting UAE Ministry, Retrieved from 

MIC (Ministry of Information & Communications). (2011, April 27). Pacific tackles cybercrime laws and protection in key workshop, Retrieved from 

Murph, D. (2011, April 14) South Pacific's Vanuatu grabbing fiber internet connection, sidesteps 'remote' stereotype, Retrieved from 
nbs.ws. (2011, June), Security Alerts, Retrieved from
secretariat: Review of Pacific Regional Digital Strategy, Part A: Technological
Capacity, Network Strategies Report Number 29029. Retrieved from
f%20Digital%20Strategy_PartA.pdf〉
newslinkservices.com (2009, November 29) Fiji Wary of Increased Cybercrime, 8,214H,
 Retrieved from 〈http://www.newslinkservices.com/edition/spip1sun.htm〉
Cambridge, UK: Cambridge University Press.
Olson, E. (2002, April 19). As Tax Havens Go, its Not Easy Being Liechtenstein, April
 havens-go-it-s-not-easy-being-liechtenstein.html?ref=vanuatu〉
ORDIG. (2005, June) Voices from Asia-Pacific: Internet Governance Priorities and
Recommendations, An ORDIG Input Paper for the UN Working Group on Internet
Governance and the World Summit on the Information Society, Open Regional
Dialogue on Internet Governance (ORDIG),〈
Issues, 39(1), 21–52.
Patrizio, A. (2007, March 14) Vikings Best, Polynesians Worst in Domain Safety,
 Retrieved from 〈http://www.internetnews.com/xSP/article.php/3665441〉
esecurity publishing, Retrieved from
〈http://www.esecurity.net.au/PICCSS08_survey.pdf〉
pita.org.fj. (2009) Invitation to participate in raising awareness of cybercrime and cyber
security, Pacific Islands Telecommunications Association, Retrieved from
〈http://www.pita.org.fj/_resources/files/Cybercrime%20seminar%20invitation%205
.pdf〉
radiofiji.com.fj. (2011, August 17) Facebook 'hate speech' profiles tracked, Retrieved
Rashid, F. Y. (2011 April 27) Cyber-criminals register free domains and subdomains for
phishing attacks, Retrieved from-
〈http://www.eweek.com/c/a/Security/CyberCriminals-Register-Free-Domains-and-
SubDomains-for-Phishing-Attacks-470147〉
Asia and pacific island countries. Drug & alcohol review, 25(6), 647-650


The Chronicle of Higher Education. (2007, January 5). We must educate young people about cybercrime before they start college. 53(18), B.29.


Vitzthum, S; Konsynski, B (2009). EBAY's Acquisition of Skype SA: Valuing the Voice of the Buyer, Communications of AIS, 24, 89-104


WHO Drug Information (2001), Regulatory information, 15, (3 & 4)


ENDNOTES

1 According to the UN's estimate, the illegal drug industry is worth some $320 billion a year (economist.com Mar 5, 2009). Likewise, it is estimated that global annual profits from the exploitation of all trafficked forced labor are US$ 31.6 billion (Besler, 2005, cited in UN.GIFT, 2010).

2 This figure has been quoted by U.S. president Obama (Economist, 7/3/2010), Sita Masamba, the Director and Head of Mission of the United Nations African Institute for the Prevention of Crime and the Treatment of Offenders (UNAFRI).

3 Not long ago, for small cybercrime cases, it was difficult to find an attorney even in the U.S. (Katz, 2005).

4 These are different from MAR externalities, which are related to spillover effects in firms in the same industry (Marshall, 1890; Arrow, 1962; Romer, 1986). MAR externalities represent the positive role of specialization on growth through knowledge spillovers (Bun & Makhloufi, 2007).