Pacific Studies Journal

Volume 47 | Number 1 Article 4

6-2024

CYBERSECURITY LAWS IN SOUTH PACIFIC NATIONS

Siuta Laulaupea'alu
University of Waikato, New Zealand

Te Taka Keegan
University of Waikato, New Zealand

Paora Mato
University of Waikato, New Zealand

Follow this and additional works at: https://digitalcollections.byuh.edu/pacific-studies-journal

 Part of the Anthropology Commons, History Commons, Indigenous Studies Commons, and the Pacific Islands Languages and Societies Commons

Recommended Citation

Laulaupea'alu, Siuta; Keegan, Te Taka; and Mato, Paora (2024) "CYBERSECURITY LAWS IN SOUTH PACIFIC NATIONS," *Pacific Studies Journal*: Vol. 47: No. 1, Article 4.
Available at: https://digitalcollections.byuh.edu/pacific-studies-journal/vol47/iss1/4

This Article is brought to you for free and open access by BYUH Digital Collections. It has been accepted for inclusion in Pacific Studies Journal by an authorized editor of BYUH Digital Collections. For more information, please contact francisca.marshall@byuh.edu.

CYBERSECURITY LAWS IN SOUTH PACIFIC NATIONS

Cover Page Footnote
Pacific Studies, Vol. 47, No. 1—Jun. 2024

This article is available in Pacific Studies Journal: https://digitalcollections.byuh.edu/pacific-studies-journal/vol47/iss1/4

CYBERSECURITY LAWS IN SOUTH PACIFIC NATIONS

Siuta Laulaupea'alu, Te Taka Keegan, and Paora Mato
University of Waikato, New Zealand

Cybersecurity practices and protocols should be updated in terms of human capacity development and legislative capability to support appropriate responses to cyberthreats within the island nations and beyond. Recommendations here discuss awareness and prevention strategies that combat cybercrimes and cyberattacks and offer pertinent suggestions within cybersecurity strategies aiming to combat the rapid growth of online fraudulence and crime affecting nations of the South Pacific. At a national level, suitable frameworks and response models are essential to instill cybersecurity prevention and awareness. Mandatory adoption of formal protocols and conventions by businesses and community and government organizations would underpin regional and national initiatives that provide local solutions for cyber-events while engaging with external international cybersecurity networks. Such networks and associations would also provide a channel for collaborative capability and a gateway for technological currency.

1. Introduction

The proliferation of new technologies has driven a multitude of social changes, disrupting social norms and underpinning wholesale shifts to the use of digital online technologies. This shift is probably best highlighted by the general fascination with the vicarious offerings of several social media platforms and by the increased adoption of online, borderless transactions. More specifically, the ability to shop, bank, and pay bills online has provided a convenience for the general populace where transactions can be completed without leaving the

Pacific Studies, Vol. 47, No. 1—Jun. 2024

house. Unfortunately, these examples of digital changes come with novel versions of risk that are exposing vulnerabilities, particularly in small, less-populated island nations.

As the variety of internet-based applications mushrooms, so too do the opportunities and incidence of cyberthreats. The ease of wider connectivity—between people, between objects, between people and objects—has transformed lives but also dramatically magnified the attack surface in cyberspace. Additionally, as technology grows and develops, so too do the avenues and methods of assault. Security solutions and strategies of defense against adversarial incursion must be at least as advanced and robust as the methods employed by the attackers. Given the rapid adoption of new technologies and the ensuing increase in exploitable touch points, the challenges of ensuring adequate protection and appropriate security measures will be complex.

This paper raises concerns with cybersecurity laws affecting South Pacific nations; they are finding that geographic isolation is not a protection from criminal intent in cyberspace and are currently experiencing almost all types of cybercrime (Kshetri 2013). Introduction of high-speed internet to Tonga, via broadband connectivity, provided novel possibilities (e.g., e-commerce, e-government, data and information sharing), but these possibilities could also be exploited by cybercriminals (Council of Europe 2024). The selected examples in this paper highlight a distinct susceptibility to cybercrimes and cyberattacks. Recent development and introduction of various forms of information and communication technologies (ICTs) were supported by limited prevention and awareness practices, constraining cyberpolicies of the nations involved and emphasizing susceptibility. Specific cybercriminal cases that have occurred in some Pacific Islands are discussed to highlight shortfalls in legislative responses to cybercrimes and cyberattacks. Cybersecurity legislation enacted in other larger countries is examined as comparative models to identify possible limitations or shortfalls of the frameworks used within South Pacific nations. The comparisons provide a way to discuss awareness and prevention strategies regarding cybercrimes and cyberattacks; the analysis offers recommendations and suggestions of pertinent cybersecurity strategies and solutions that will combat the rapid growth of online fraudulence and cybercrime currently affecting nations of the South Pacific.

2. Cybersecurity Breaches in South Pacific Nations

Cybersecurity affects everyone from the general populace to public organizations, the private sector, and national governments. Vulnerabilities in small island states such as Fiji and Tonga can be attributed to poorly structured cybersecurity frameworks that are exacerbated by the absence of appropriate

national policy and the application of inadequately framed protective laws (Taminkaiwaimaro 2010). Recent examples indicate the inability of poorly framed laws to successfully prosecute online fraudsters and therefore act as a deterrent to further cybercrime (Taminkaiwaimaro 2010; Pandey et al. 2016).

2.1 Fiji

The Pink Window Creations case of 2013 is an example of the inadequacy of Fijian cybersecurity law; items were advertised, sold online, and then purchased through an online payment system (Pandey et al. 2016). The online business, Pink Window Creations, failed to deliver an estimated US$70,000 worth of paid items to their online customers (Prakash 2016). According to the investigative report, the charges would have been dropped if full refunds of money were made before the first hearing date (Pandey et al. 2016); however, Fiji did not have cybercrime laws specific to online sales and purchasing. The owners of the Pink Window Creations business created other online boutique accounts, trading as Desi Fashion House and again as Fashion Bure, and, after a time, perpetrated similar scams (Pandey et al. 2016; Consumer Council of Fiji 2013). Following short periods of building trust, large orders were placed and paid for but then never delivered to customers. About 203 complaints worth "$67,871 were registered against this online boutique" (Consumer Council of Fiji 2013, 15).

Further examples of cybercrimes investigated by the Fiji Intelligence Unit from 2013 to 2015, include the following:

- 2013—A Suva-based company lost US$65,000 in one transaction when payment was diverted from Taiwan to India via the United Arab Emirates.
- 2013—A Suva-based company lost US$44,000 in three separate transactions when payment for goods was diverted from China and Belgium to the United Kingdom.
- 2014—A Savusavu company lost NZ$58,000 in one transaction when payment was diverted from New Zealand to Scotland.
- 2014—A Suva-based agency lost US$101,000 when payment was diverted to the United Kingdom from Israel.
- 2014—A Suva-based company lost US$10,000 when payment was diverted to a different bank account in China.
- 2015—A Nausori company lost US$13,000 when payment was diverted from Pakistan to the United Kingdom.
- 2015—A Suva-based company lost US$14,000 when payment was diverted to a different bank account in China.

In summary, from 2013 to 2015, investigations of 18 instances of this type of cyberlaundering, in which payments were diverted from legitimate suppliers' accounts to other accounts, total just more than Fijian dollars (FD) 1 million, of which FD300,000 were successfully stymied and FD60,000 recovered. The remaining 13 cases represent online theft of FD724,000 (Pandey et al. 2016).

Under Fiji's Crimes Decree 2009, which covers computer-based offenses, the sentencing is considered woefully light, and the lack of adequate legislative provisions for addressing online fraudulence and cybercrime is not stringent enough to act as a deterrent (Taminkaiwaimaro 2010; Pandey et al. 2016). Therefore, a range of similar crimes are being re-committed under different guises (Consumer Council of Fiji 2013; Prakash 2016). Although the Consumer Council of Fiji (2013) is investigating consumer complaints and advising caution to those shopping online, online shoppers cannot reliably depend on Fijian cybersecurity laws for safety and protection against cybercrimes and cyberattacks (Taminkaiwaimaro 2010; Pandey et al. 2016; Prakash 2016). Additionally, given the changing nature of ICT, Fijian legislation must implement inbuilt robustness and incorporate specific and stringent laws that are sufficiently punitive and can be applied to instances of online offenses and cybercrimes in ways that minimize or equitably redress acts of fraudulence (Taminkaiwaimaro 2010; Pandey et al. 2016).

2.2 Tonga

The Kingdom of Tonga aims to create a knowledge-based society that accelerates economic growth and development and improves quality of life for all citizens in Tonga. The vision is largely reinforced by a commitment to fully incorporate the innovative potential of global connectivity tempered by a mandate whereby all technology-based changes and advancements should strengthen rather than compromise Tongan culture and values (Lutui and Maeakafa 2018). In line with that vision and commitment, the government of Tonga is cognizant of the difficulties and risks inherent in the implementation of a broad technology-based strategy and the wide-ranging issues and challenges that must be overcome before sustainable benefits are realized.

Tonga must tailor cybercrime legislation while developing capability in key areas of investigation, enforcement, and prosecution. Several issues regarding Tonga's Computer Crimes Act (TCCA) 2003 and the need to review and update the legislative framework in Tonga were raised in 2011 by the former Solicitor General of Tonga (Kefu 2011). The occurrence of cyber-related crimes in Tonga (e.g., credit card fraud, forgery, counterfeit currency, bank fraud) highlighted the need to heighten legislation-supported cybersecurity; to strengthen specific procedural powers covering investigation, acquiring, and submitting electronic evidence for prosecution; and to develop enforcement capacity. Four focal areas were identified.

- Review and update legislation
- Train (forensic investigation and law enforcement)
- Enforce (cybercrime legislation)
- Establish and increase public awareness

Recent reports identified exposure to cyberthreats and cyberattacks by 73 percent of the surveyed organizations in Tonga and outlined the effects of a bogus email scam that resulted in a significant loss of money from an organization within the Government of Tonga (Laulaupea'alu 2022; Laulaupea'alu and Keegan 2018a, 2018b).

2.3 Other Pacific Nations

Examples of cyberbreaches experienced by other nations within the South Pacific include hijacked telephone numbers that caused a four-hour interruption to the Public Switch Telephony Network, resulting in a monetary loss of more than US$100,000. A similar denial of service (DoS) attack occurred in the Republic of the Marshall Islands and halted their network for two days (Finau, Samuwai, and Prasad 2013).

A country code top-level domain (ccTLD) is an extension assigned to a particular country, sovereign state, or territory. For example, New Zealand's ccTLD is .nz. The country domain for Tokelau (a group of three islands' atolls with a resident population of 1,400) is .tk; it is regarded as the world's first free top-level domain (i.e., by anyone), and in 2011, it was listed as the third-highest registered ccTLD (Domain Registration Services 2011), only behind .uk (United Kingdom) and .de (Germany; Jackson 2011; Merrill 2018). A Dutch company owns the country domain for Tokelau (Jackson 2011; Ksherti 2013), and, according to Australian Domain Registration Services, it is now ranked as the second largest country domain with 21.5 million registered users, only behind China (22.5 million; Domain Registration Services 2019).

The supposed popularity of the .tk domain brings a wealth of security issues. The Tokelau domain was identified as one of two free services heavily abused by fraudsters, a major source of phishing emails, and a domain heavily infected with malware (Jackson 2011; Merrill 2018). The .tk extension has the dubious reputation of being one of the top four malicious domain registrations in the world (Domain Registration Services 2011). Of the 2,533 cyberattacks initiated from Tokelau, 95 percent were launched from the .tk web domain, and the remaining attacks were launched from hacked .tk websites (Kshetri 2013).

Kazaa Media Desktop is a file-sharing application operated by Sharman Networks, which was incorporated in Vanuatu (BBC News 2006). The application became popular for sharing music, mainly in mp3 form, videos, and several other

types of files. At one time, the Kazaa software had been downloaded 239 million times and had more than four million simultaneously active users (BBC News 2006). After multiple ongoing legal battles, because of copyright infringement and unpaid taxes, Sharman Networks was sued by the Music Industry Piracy Investigations in 2004 under the Australian Copyright Infringement Legislation, resulting in the payout of £53 million in damages to the record industry—an amount that, in 2006, represented half of the legitimate music downloads in Europe (Pearce 2004; BBC News 2006).

Problems with the levels of cybercrime and a perceived lack of policing and redress in the South Pacific have led some to conclude that Vanuatu and other South Pacific nations are less likely to get help from wealthier neighbors and law-enforcement agencies because of a lack of interaction, treaties, or similar collaborative relationships and partnerships with other nations and economies in the battle against online crime (Kshetri 2013).

3. Cybersecurity Laws in South Pacific Nations

Regarding combatting cybercrime, Tonga and Fiji are two South Pacific island nations showing leadership, especially in the development of relevant legislation. The establishment of the TCCA 2003, updated by the Computer Crimes Bill 2019, and Tonga's accession to the Budapest Convention and the Crime Decree 2009 in Fiji are evidence of actions taken thus far.

3.1 Tonga Cyberlegislation

Tonga and Fiji are the two leading nations in the South Pacific to establish acts focused on computer crime. The TCCA was legislated in September 2003 (World Intellectual Property Organisation 2003). The main components of TCCA forbid the tampering or unauthorized interference in another's device, data, or operating system and trafficking in illegal computer devices (Blythe 2006). Some suggest that the TCCA should also require the electronic-transactions statute to deliver legal recognition of e-signatures and endorse taxes for foreign bodies that used Tongan-based websites for global e-commerce transactions (Blythe 2006).

Major target areas of the TCCA aim to combat cybercrime and provide for the collection and use of electronic transactions. Furthermore, concerns about the existing TCCA address the following.

- No legislation for privacy and data protection
- No law to protect young people from online sexual violence
- No digital forensic resources for Tonga Police

- No ability for Tonga law enforcement to investigate cybercrimes
- Lack of expert judges and police in the cybercrime field

According to the Council of Europe (2024):

> There are only currently two judges that sit on the bench in the Supreme Court of Tonga. They are not specialized in the area of cybercrime however they have tried some cases involving electronic evidence. (paragraph 4, Specialised Institutions Section 4)

A former Solicitor General of Tonga published a report about the cybercrime legislation in Tonga. The report confirmed that the occurrence of cybercrime cases in Tonga mainly targeted bank fraud, credit card fraud, counterfeit currency, illegal requests for electronic data, and digital document forgery (Kefu 2011).

The report raised the following issues:

- that Tonga Computer Crimes Act (TCCA) should cover emails and similar online activities (e.g., email spam, phishing);
- that Tonga has only a limited number of forensic investigators;
- that law practitioners (e.g., investigators, enforcers, prosecutors, judges) should be provided appropriate cybersecurity training;
- that the TCCA should include online fraud, including bank fraud;
- and that the capacity to enable the presentation of evidence before a jury is established.

In 2019, the Government of Tonga (2019) passed the Computer Crimes Bill 2019. The bill contains 78 sections (57 pages) that are divided into five main parts:

1. computer offenses,
2. interpretation,
3. miscellaneous provisions, and
4. procedural powers.

The new bill replaces the TCCA 2016 and is an outcome of Tonga's accession in 2017 to the Convention on Cybercrime of the Council of Europe, which resulted from joint initiatives between Tonga and the Council of Europe over seven years (Council of Europe 2024).

The Convention on Cybercrime of the Council of Europe (CETS No. 185) is the first international treaty on crimes committed via the internet and

other computer networks. The CETS No. 185, also known as the Budapest Convention, is currently the only binding international instrument of its type and serves as a guideline for developing comprehensive national legislation against cybercrime within a framework for international cooperation between state parties to this treaty (Council of Europe, Treaty Office 2024). The Convention's main objective is aimed at protecting from cybercrime by pursuing common criminal policy implemented using appropriate legislation that fosters international networks of cooperation. The CETS No. 185 particularly addresses infringements of copyright, child pornography, computer-related fraud, and network security violations (Council of Europe, Treaty Office 2024). Additionally, other clauses in the Convention specifically target other areas, including botnets, identity theft, distributed DoS, transborder access, critical infrastructure attacks, terrorism, election interference, malware, and spam.

Tonga's accession to the Budapest Convention is hailed as an example of cybersecurity leadership in the South Pacific. Wide-ranging procedures and powers that facilitate across-the-board interception and the searching of computer networks highlight the efforts of the government of Tonga to enact regulations that strengthen their capacity to address online criminal injustices (Council of Europe, Treaty Office 2024; Council of Europe 2024).

3.2 Vanuatu Computer Act

The Vanuatu E-Business Act permits overseas entities to rent a Vanuatu e-commerce website as a tax haven, attracting little or no tax, without any prior formal consultation (Republic of Vanuatu 2017). Vanuatu computer crime laws must address this situation. Vanuatu Computer Cybercrime Act No. 22 was enacted in 2021. The Act is subjected to criminalize authorized actions; protect citizens from computer offenses; empower procedures for collecting and obtaining electronic evidence; provide privacy, safeguards, and accountability; and provide efficient and effective mechanisms for international cooperation (Republic of Vanuatu 2020).

3.3 Fiji Computer Act

The main legal instrument being used to criminalize computer crimes in Fiji is the Crime Decree 2009 (Pandey et al. 2016). Unfortunately, this decree allows Fijian authorities and the cybercrime unit limited powers of arrest for various computer breaches (Pandey et al. 2016). Several have laid complaints regarding cybercrime offenses, but, as of yet, no criminal charges have been brought under the current legislation to address the issues. Inappropriate legislation

> . . . makes Fiji incredibly susceptible in terms of the ability to criminalize cyber offenses under the current Crimes Decree, especially considering the complex types of cybercrimes committed in more developed countries and their associated and existing cybercrime laws. (Pandey et al. 2016, 216).

Many prevalent cyberthreats in Fiji are not covered in Crime Decree 2009. Some of these cyberthreats and illegal use of technology are not confined to computers (Taminkaiwaimaro 2010, 17). The deficiencies of Crime Decree 2009 include illegal access and interception, online child pornography, computer-related fraud and forgery, modification and data interference, and misuse of devices. The review of existing legislation and empirical examination of research findings has driven the drafting of new Fijian legislation. The proposed new laws target cybercriminals and enable the enforcement of child pornography-related offenses that include individual fines of up to FJ$50,000 and FJ$200,000 penalties for business organizations (RNZ 2020). The proposed bill also enables authorities to search and seize computers, data, or devices of any person or business and would compel telecommunications providers to provide the identity and other personal information of any customer (RNZ 2020). In the interim, it might be beneficial for Fiji to embrace the Australian Cybercrime Legislation Act 2012, which covers all computer offenses and potentially enables the apprehension of cybercriminals and lawbreakers in Fiji (Pandey et al. 2016).

4. Cybersecurity Strategies in the South Pacific

4.1 Information Security Policy

An Information Security Policy (ISP) is normally drafted by organizations to determine, outline, and appraise what is acceptable (and what is not) in terms of employees' online-based interactions while using the organization's technology. The purpose of the policy is to define and disseminate the organization's regulations and requirements and how those affect ICT security and safety (Flowerday and Tuyikeze 2016). According to Laulaupea'alu and Keegan (2018a), an ISP

> provides policies to ensure that IT users comply with guidelines and rules to safeguard information stored within organizations, to regulate employees' security performances, and to prevent misuse of information security systems. The ISP plays a significant role in outlining the responsibilities and roles of users regarding ICT security. Without an ISP, the possibility that the ICT system would be compromised is significant. (190)

The ISPs are designed to manage, control, and maintain active ICT relationships within an organization and workplace and to ensure employees understand the internal roles and responsibilities of the employer (and the employees) to keep the technology-based activities safe and secure. The policy should ensure employees know the limitations and boundaries in terms of the use of an organization's technology. An ISP is a tool within an organization to maintain legal compliance and enforce appropriate technology-based behavior. Operating outside and beyond the boundaries of an information policy should incur some level of censorship and might include legal charges. Implementing and managing security policies effectively minimizes potential transgressions and reduces the occurrence of adverse effects on the employee and employer.

4.2 Computer Emergency Response Team

In the South Pacific, Tonga was recognized as the first island in the South Pacific nations to establish its Computer Emergency Response Team (CERT) in 2016 and the first island to become a member of the Asia-Pacific CERT. Tonga CERT is the first point of contact for cybersecurity issues. Their main task is ensuring a safe cybersecurity environment for Tongan citizens. They seek intimate global working relationships with investors to manage cyberthreats on a global platform (Laulaupea'alu 2022, 14, 210).

The significance of the establishment of CERT organizations for South Pacific nations is embodied in the establishment of local and cross-national inward/outward points of contact and collaboration between other CERTs and stakeholders internationally. For example, cross-national initiatives would provide an opportunity for individual nations to connect with other more established initiatives and organizations, such as the Asia-Pacific CERT, the Forum of Incident Response and Security Teams (FIRST), and the European Union's response center for cybersecurity issues (the European Network and Information Security Agency [ENISA]). In terms of assistance and support, the coverage and effect of FIRST and ENISA would promote and boost the efforts of South Pacific nations to develop their capabilities and to provide their support to other national CERTs to counter cybercrimes and cyberattacks internally and globally.

4.3 Lack of Cybersecurity Law Expert

Law-enforcement capability is severely disadvantaged because of technological gap between cybercriminals and "law enforcement officials who are much less equipped with technology" in the South Pacific Nations. (Tropina 2016, 18).

Additionally, other countries (e.g., Africa) have a lack of regulation for digital proof, that is, it is not allowed as evidence in court (Cole et al. 2008, 23). In countries such as Nigeria, Kenya, Tanzania, and Tunisia, the potential for cybercriminals to evade detection and capture is due largely to a dearth of appropriate technologies combined with a lack of effective cybersecurity laws and policies. Moreover, cybercriminal investigations are difficult to enact because of inadequate technical knowledge and the shortage of skilled law-enforcement officials, which is exacerbated by toothless legislation (Mohammed, Mohammed, and Abiodun 2019). The development of specialists and constant training regimes are paramount. Such regimes should also occur in academic tertiary institutions, such as universities, where specialist courses and qualifications equip future generations of legislation development and law enforcement who are proficient in the detection, capture, and prosecution of cybercriminals and perpetrators of online attacks (Dushi and Bërdufi 2017; Mohammed, Mohammed, and Abiodun 2019).

Laulaupea'alu (2022) reinforces that cybersecurity gaps occur between cybercriminals and law officials. The enforcement of cybersecurity laws is essential to lessen these gaps because cybercriminals always look for ways to cheat technology. Additionally, Laulaupea'alu (2022, 100) informs that there are a lack of cybersecurity-law experts and that part of the solution for these issues is to send students overseas to participate in cybersecurity courses and training. About 96 percent of the survey participants "agreed with the idea of sending students overseas for further studies on cybersecurity and bringing new knowledge to assist Tonga" (155). Although the main idea is subjected to Tonga, this suggestion applies to all the South Pacific nations because of "lack of cybersecurity training" (145) and "lack of cybersecurity experts" (12).

5. Conclusion

The current susceptibility of South Pacific nations to cyberthreats, cybercrimes, and cyberattacks is identified. Cybersecurity practices and protocols need to be influenced, both in terms of human capacity development and legislative capability, to support an appropriate response within the island nations and beyond. The ISPs at an organizational level and CERTs at a national level are essential parts of instilling cybersecurity prevention and awareness. The mandatory adoption of such formal protocols by businesses and community and government organizations would be beneficial. Regional and national initiatives would provide local solutions for cyber-events while supporting, and being supported by, external international cybersecurity networks. Such networks provide a channel for collaborative capability and a gateway for technological currency. Effective policy minimizes the risk of employee and business

exposure to cyberthreats and reduces the consequent requirement for legal recourse.

Education and personal development programs are appropriate long-term solutions that will address the lack of cybersecurity experts in the South Pacific nations. In the short term, expertise in cybersecurity and cybersecurity should be acquired from trusted sources to create capacity in the interim. Strategies must be implemented and enacted to ensure technological competence and embrace global cybersecurity protocols and expertise. The development of cybersecurity legislation should be augmented by robust training and ongoing personnel development, aimed at acquiring and maintaining the requisite local faculties of knowledge. Additionally, the appropriate currency of expertise enables the confidentiality, integrity, and availability of online technologies for users, organizations, businesses, the public and private sectors, the government, and the wider technology-based infrastructures.

Although the voices of South Pacific nations are often ignored or unacknowledged in international forums, the battle against cybercrimes and cyberattacks by the smaller nations should not be deterred. The establishment of safe cyberspace and the protection of local and personal data should remain paramount. Forming joint stances within the islands and island groups and forging strategic alignment with international protocols and conventions will ensure a louder voice and stronger defenses. Partnerships with other nations, including New Zealand and Australia, will favorably position small island nations to combat the ever-growing incidence of cyberthreats, cybercrimes, and cyberattacks.

6. REFERENCES

BBC News
2006 Kazaa site becomes legal service, updated July 17, 2006. http://news.bbc.co.uk/2/hi/science/nature/5220406.stm

Blythe, Stephen E.
2006 South Pacific computer law: Promoting e-commerce in Vanuatu and fighting cyber-crime in Tonga. *Journal of South Pacific Law*, 10 (1) [accessed January 1, 2006]. http://www.paclii.org/journals/fJSPL/vol10/2.shtml

Cole, K., M. Chetty, C. LaRosa, F. Rietta, D. K. Schmitt, S. E. Goodman, and G. A. Atlanta
2008 *Cybersecurity in Africa: An assessment.* Atlanta, Georgia: Sam Nunn School of International Affairs, Georgia Institute of Technology.

Consumer Council of Fiji
2013 2013 Annual report, March 10, 2022. https://consumersfiji.org/annual-reports/2013-annual-report/

Council of Europe
2024 Cybercrime policies/strategies [accessed April 3, 2024]. https://www.coe.int/en/web/octopus/-/tonga

Council of Europe, Treaty Office
2024 Details of Treaty No. 185 [accessed April 3, 2024]. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

Domain Registration Services: Domain name registrar (Australia)
2011 Little territory, big domain name, December 26, 2011. https://www.domainregistration.com.au/news/2011/1112-tk-domain.php
2019 The world's biggest and smallest country code top level domains, February 11, 2019. https://www.domainregistration.com.au/news/2019/0211-cctld-statistics.php

Dushi, D., and N. Bërdufi
2017 Law enforcement and investigation of cybercrime in Albani. Paper presented at the 7th International Scientific Forum, Oxford, United Kingdom, February 2017.

Finau, G., J. Samuwai, and A. Prasad
2013 Cybercrime and its implications to the Pacific [accessed April 4, 2024]. https://eprints.qut.edu.au/69108/2/69108.pdf

Flowerday, S. V., and T. Tuyikeze
2016 Information security policy development and implementation: The what, how and who. *Computers and Security*, 61, 169–83 [accessed April 7, 2024]. https://doi-org.ezproxy.waikato.ac.nz/10.1016/j.cose.2016.06.002

Government of Tonga
2019 Computer Crimes Bill 2019 [accessed April 7, 2024]. https://ago.gov.to/cms/images/LEGISLATION/BILLS/2019/2019-0025/ComputerCrimesBill2019.pdf

Jackson, W.
2011 Phishing economy: Why tiny Tokelau is 3rd largest country domain [accessed April 7, 2024]. https://www.route-fifty.com/cybersecurity/2011/12/phishing-economy-why-tiny-tokelau-is-3rd-largest-country-domain/283322/

Kefu, A.
2011 Tonga's cybercrime legislation [accessed April 7, 2024]. https://rm.coe.int/16802f2474

Kshetri, N.
2013 Cybercrime and cybersecurity in the developing Pacific Island economies. *Cybercrime and Cybersecurity in the Global South*, 171–89 [accessed April 7, 2024]. https://www.researchgate.net/publication/317847658_Cybercrime_and_Cybersecurity_in_the_Global_South

Laulaupea'alu, S.
2022 The vulnerability to online scamming in contemporary Tongan Society [Ko e laveangofua ʻi he Ngaue Kākā ʻoe Naluope ʻi he Sosaieti Tonga lolotonga]. PhD diss., Univ. of Waikato.

Laulaupea'alu, S., and T. T. Keegan
2018a Cybersecurity vulnerabilities in Tonga. Paper presented at the Cyber Forensic and Security International Conference (2018 CFSIC), Nuku'alofa, Tonga, July 2018.

Laulaupea'alu, S., and T. T. Keegan
2018b Data security assessment for organisations in Tonga. Paper presented at the Cyber Forensic and Security International Conference (2018 CFSIC), Nuku'alofa, Tonga, July 2018.

Lutui, P. R., and G. Maeakafa
2018 An analysis of personal wireless network security in Tonga. In *The Proceedings of the Cyber Forensic and Security International Conference*, ed. B. Cusack and R. Lutui, 69–78. Kingdom of Tonga: Christ's Univ. in Pacific.

Merrill, K. A.
2018 *Domains of convenience: Open country code top-level domains and the geopolitics of internet governance.* Washington, DC: American Univ.

Mohammed, K. H., Y. D. Mohammed, and A. Abiodun
2019 Cybercrime and digital forensics: Bridging the gap in legislation, investigation and prosecution of cybercrime in Nigeria. *International Journal of Cybersecurity Intelligence and Cybercrime*, 2 (1): 5 [accessed April 7, 2024]. https://vc.bridgew.edu/cgi/viewcontent.cgi?article=1014&context=ijcic

Pandey, S., N. Shah, A. Sharma, and M. Farik
2016 Cybersecurity situation in Fiji. *International Journal of Scientific & Technology Research*, 5 (7): 215–9. [accessed April 10, 2024] http://www.ijstr.org/final-print/july2016/Cybersecurity-Situation-In-Fiji.pdf

Pearce J.
2004. Aust music investigators head to Vanuatu to tackle Kazaa, February 8, 2004. https://www.zdnet.com/article/aust-music-investigators-head-to-vanuatu-to-tackle-kazaa/

Prakash, P.
2016 Thirty-eight complaints against Desi Fashion House [accessed May 23, 2016]. https://www.fbcnews.com.fj/news/thirty-eight-complaints-against-desi-fashion-house/

Republic of Vanuatu
2017 E-Business (Amendment) Act No. 30 of 2017 [accessed April 14, 2024]. https://www.vfsc.vu/wp-content/uploads/2015/12/E-Business-Amendment-Act-No.-30-of-2017.pdf

Republic of Vanuatu
2020 Bill for the cybercrime. Parliament of Vanuatu [accessed April 14, 2024]. https://parliament.gov.vu/images/Bills/2020/2nd_Ordinary/English/Bill_for_the_Cybercrime_Act_No_of_2020.pdf

RNZ
2020 Fiji's govt proposes new legislation to tackle cyber crime [accessed February 27, 2020]. https://www.rnz.co.nz/international/pacific-news/410480/fiji-s-govt-proposes-new-legislation-to-tackle-cyber-crime.

Taminkaiwaimaro, S.
2010 Cybersecurity in the Republic of Fiji [accessed April 24, 2024]. https://www.diplomacy.edu/wp-content/uploads/2021/06/IGCBP2010_2011_Tamanikalwalmaro.pdf

Tropina, T.
2018 Do digital technologies facilitate illicit financial flows? In *Max Planck Institute for Foreign and International Criminal Law*. World Development Report 2016: Digital Dividends. The Netherlands: Leiden Univ.

World Intellectual Property Organisation
2003 Tonga Computer Crimes Act 2003 [accessed April 24, 2024]. https://wipolex.wipo.int/fr/text/340817