Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/CLSR

Computer Law & Security Review

Diffusion of the Budapest Convention on cybercrime and the development of cybercrime legislation in Pacific Island countries: '*Law on the books*' vs '*law in action*'

Dr. Chat Le Nguyen[a,*], *Dr. Wilfred Golman*[b]

[a] *School of Law, University of Canterbury, New Zealand*
[b] *School of Law, the University of the South Pacific, Fiji*

ARTICLE INFO

Keywords:
Budapest Convention
Cybercrime
The South Pacific

ABSTRACT

The Council of Europe Convention on Cybercrime,[1] referred to as the Budapest Convention on Cybercrime, has been diffused globally, and is serving as a benchmark or a 'model law' for drafting national cybercrime legislation in many countries worldwide. This paper argues that, through the mechanism of 'state socialization' combined with incentives, e.g. assistance in building law enforcement capacity, the diffusion of the Budapest Convention has had a profound influence on the development of cybercrime legislation in a number of Pacific Island Countries (PICs).[2] Some PICs have expressed their great interest in acceding to the Convention and 'imported' several provisions from the Convention. This article, nevertheless, contends that these PICs do not seem to consider carefully whether the 'imported' law is applicable to their existing law enforcement capacity. It is evident that various domestic factors, such as lack of resources, have deterred the enforcement of cybercrime laws in these countries. As the result, although those PICs would have adequate cybercrime laws 'on the books', 'law in action' is still feeble.

1. Introduction

Recent developments in information and communication technology (ICT) across PICs have spawned a rapid increase in access to the Internet and social media, which has greatly influenced the economic, social and political systems in the region. While the benefitsare enormous,[3] the potential detrimental effects on the countries are significant. Cybercrime has been perceived as one of the greatest threats to

* Corresponding author.
E-mail addresses: chat.nguyen@canterbury.ac.nz (Dr.C.L. Nguyen), wilfred.golman@usp.ac.fj (Dr.W. Golman).

[1] CoE, Convention on Cybercrime - ETS No. 185 (2001).

[2] This paper will focus on examining the cybercrime legislation of ten developing South Pacific countries: Cook Islands, Fiji, Kiribati, Nauru, Papua New Guinea, Samoa, Solomon Islands, Tonga, Tuvalu, and Vanuatu.

[3] Michael Minges and Christoph Stork, 'Economic and Social Impact of ICT in the Pacific' (Pacific Region Infrastructure Facility, 2015) <https://www.theprif.org/documents/regional/information-communication-technology-ict/economic-and-social-impact-ict-pacific-0> accessed 19 June 2020.

https://doi.org/10.1016/j.clsr.2020.105521
0267-3649/

the national and regional security, economic prosperity and public safety.[4] Cybercrime and cybercrime-related acts identified and reported in the region include: spam, hacking, virus, pornography, identity theft, data theft, data manipulation, ransomware, distributed denial-of-service (DDoS) attacks, business e-mail compromise, email spoofing, banking frauds, social media abuse, and intellectual property rights (IPR) infringements.[5] International criminals are starting to perpetrate cyber-financial crimes, such as credit card fraud and financial scams.[6] There are also reported incidents of cyberbullying, cyber-harassment, 'revenge porn', and the spread of 'fake news'.[7] Cyber-threats and the challenges grow as rapidly as technology evolves.[8]

The international standardization of communication technology and services allows users to have access to the same worldwide internet services from anywhere around the world, thus cybercrime acts have no physical national borders. Developing countries with inadequate legal and technical foundation are more vulnerable to cyber-attacks.[9] Adequate and effective safeguards against cybercrime, of which the national legal framework is a fundamental component, should be required in all countries. Every country should enact the comprehensive cybercrime legislation that can be enforced to eliminate 'havens' for cyber-criminals.

Being aware of the growing cyber-threats, motivated and supported by different regional organizations and countries, a number of PICs have prioritized legal reform in the cybercrime area. The Council of Europe (CoE), Australia and New Zealand are the main donors to the development of cybercrime legislation in PICs. PICs are primarily drafting their cybercrime laws by 'importing' provisions from the Budapest Convention, the Commonwealth Model Law on Computer and Computer Related Crime,[10] and the Cybercrime Act 2001 of Australia.[11]

This article, first, briefly examines the Budapest Convention and its diffusion to the Pacific. It then scrutinizes the current cybercrime legal framework of ten PICs in comparison with the Budapest Convention, including the criminalization of cybercrime and criminal procedure related to cybercrime investigation. These selected PICs have already, to different extents, provided for cybercrime legislation. The ongoing legal development and the building of law enforcement capacity in combating cybercrime are also discussed. The main argument will be made based on the observation and assessment of whether the novel cybercrime legislation could be enforced in the selected PICs.

2. The Budapest Convention on cybercrime and its diffusion

2.1. *The Budapest Convention as a global instrument against cybercrime*

The Budapest Convention on Cybercrime is a collective response to cybercrime by the member states of the Council of Europe and some non-member states. The Convention is the first binding multinational treaty to comprehensively address cybercrime, and it has had a profound impact on the international anti-cybercrime legislation. The Council of Europe, which represents 47 states in the European region, plays an important role at the international level in combating cybercrime. The Council of Europe has initiated works in computer crime since the 1970s.[12] In 1989, the Council of Europe provided guidelines for national legislatures in its Recommendation, and the European Committee on Crime Problems adopted the Report on Computer-related Crime to develop the necessary substantive criminal law against electronic crimes.[13] A further Recommendation dealing with criminal procedural laws related to information technology was adopted in 1995.[14] Based on these Recommendations, between 1997 and 2001 a Convention on Cybercrime was developed and negotiated by 'the Committee of Experts on Crime in Cyber-space (PC–CY)', who were appointed by the Committee of Ministers.[15] Canada, Japan, South Africa, and the United States (US) were invited to participate in the negotiations. The Council of Europe Convention on Cybercrime was opened for signatures at a Conference in Budapest, Hungary, on 23 November 2001.

[4] Commonwealth Secretariat, Pacific to Establish Cybercrime Collaborative Platform as Threat Escalates (2016).

[5] See, ITU, Capacity Building and ICT Policy, Regulatory and Legislative Frameworks Support for Pacific Island States (ICB4PAC 2013) 7-8; and Shelveen Pandey and others, 'Cybersecurity Situation In Fiji' (2016) 5(7) International Journal of Scientific & Technology Research 215, 215-17.

[6] Natadola Jyoti Pratibha, 'How Cyber Criminals Defraud Fijians' FijiSun (Suva, 08 December 2018) <https://fijisun.com.fj/2018/12/08/how-cyber-criminals-defraud-fijians/> accessed 18 June 2020; Talebula Kate, '$5 m Loss to Scams' The Fiji Times (Suva, 14 December 2018) <https://www.fijitimes.com.fj/5m-loss-to-scams/> accessed 18 June 2020.

[7] Parliament of the Republic of Fiji, Report on the Online Safety Bill 2018 (Parliamentary Paper No 66, 2018) 4.

[8] Commonwealth Secretariat, Report of the Commonwealth Working Group of Experts on Cybercrime (Meeting of Commonwealth Law Ministers and Senior Officials, 2014) 16.

[9] ITU, Understanding Cybercrime: Phenomena, Challenges and Legal Response (International Telecommunication Union (ITU), 2015) 4-5.

[10] The Commonwealth, 'Model Law on Computer and Computer Related Crime' (Commonwealth Secretariat, 2017) <https://thecommonwealth.org/sites/default/files/key_reform_pdfs/P15370_11_ROL_Model_Law_Computer_Related_Crime.pdf> accessed 21 June 2020.

[11] Cybercrime Act 2001 (Australia, Act No. 161 of 2001, as amended in 2004).

[12] The first initiative on computer crime in Europe was the Council of Europe Conference on Criminological Aspects of Economic Crime in Strasbourg in 1976. See Stein Schjolberg and Amanda M. Hubbard, Harmonizing National Legal Approaches on Cybercrime (WSIS Thematic Meeting on Cybersecurity, 2005) 8.

[13] CoE, Recommendation of the Committee of Ministers to Member States on Computer-Related Crime (No R (89) 9, 1989); and European Committee on Crime Problems, Report on Computer-related Crime (Strasbourg, 1990).

[14] CoE, Recommendation No R (95) 13 of the Committee of Ministers to Member States Concerning Problems of Criminal Procedural Law Connected with Information Technology (Committee of Ministers, 1995).

[15] CoE, Explanatory Report to the Convention on Cybercrime (European Treaty Series - No 185, 2001) para 12.

The Budapest Convention is intended to harmonize the domestic criminalization of specific conduct related to computer systems and data; provide national criminal justice authorities with necessary means for the investigation and prosecution of such criminal offences; and establish an effective mechanism of international co-operation in combating these offences.[16] The Convention, accordingly, consists of four chapters. *Chapter 1* defines fundamental terms: computer system, computer data, service provider and traffic data. *Chapter 2*, first, stipulates nine offences categorized in four groups, then deals with ancillary liability and sanctions. The following offences are defined by the Convention: illegal access, illegal interception, data interference, system interference, misuse of devices, computer-related forgery, computer-related fraud, the offences related to child pornography and offences related to infringements of copyright and related rights. It then provides for investigative means, including expedited preservation of stored computer data, production orders, search and seizure of stored computer data, and real-time collection of computer data. The application of these provisions goes beyond the above defined offences, and they also apply to any other criminal offences committed by means of a computer system and to the collection of evidence in electronic form of a criminal offence. Article 15 sets out conditions and safeguards, applicable to all procedural powers, to protect human rights. The last section of the chapter deals with jurisdiction. *Chapter 3* on international co-operation contains general principles and procedures relating to extradition, and to traditional and computer crime-related mutual legal assistance. *Chapter 4* provides for the final clauses mainly in accordance with standard provisions in the Council of Europe treaties. The Convention is supplemented by Protocols[17] and Guidance Notes.[18]

The Budapest Convention is unique in that, although being a regional treaty, it is always intended to apply internationally.[19] According to article 37 of the Convention, in addition to the member states of the Council of Europe and those who 'participated in its elaboration', any state may be a contracting Party. The Committee of Ministers, on its own initiative or upon request, can invite a state to accede to the Convention after having consulted with and obtained the unanimous consent of the contracting states.[20] By February 2020, 65 states are Parties to the Convention, and 9 states are Signatories or have been invited to accede.[21] This Convention is an important development and a historic milestone in international law combating cybercrime. However, it has also attracted criticisms, such as failing to keep pace with technological developments,[22] lack of extensive input from developing countries,[23] inadequate privacy protections,[24] and national sovereignty vulnerability.[25]

Despite the criticisms, the Convention is diffused globally beyond membership. So far, it is perceived as having the broadest reach and influence in the international legal framework against cybercrime. The Convention now serves not only as a legal instrument for transnational cooperation against cybercrime, but also as a guideline or a 'model' law for the drafting of national anti-cybercrime legislation in almost 80% of states worldwide.[26] It is also supported by a number of important international organizations, such as The International Criminal Police Organization (INTERPOL) and the Asia-Pacific Economic Cooperation (APEC).[27] There are various reasons for the diffusion of the Convention and states' accession.[28] Firstly, a comprehensive legal framework for investigating and prosecuting cyber-criminals is essential for every state. Most states are now dependent on ICT, and thus vulnerable to cybercrime. Secondly, given the transnational dimension of cybercrime, the harmonization of national criminal law against cybercrime is important. The Convention currently provides the most extensive benchmark for national criminal law and the legal basis for international cooperation in combating cybercrime. While the United Nations (UN) has not yet finalized a treaty on cybercrime, the Convention arguably remains the most internationally agreed and complete standard against cybercrime to date.

It should be noted that the negotiations on a global convention against cybercrime is favored by the Russian Federation and a number of developing countries. Recently, a resolution on cybercrime called 'Countering the use of information and communications technologies for criminal purposes', led by the Russian Federation, was adopted by the UN General Assembly. Nevertheless, most European and Western powers oppose it.[29] As the result, an open-ended ad-hoc intergovernmental committee of experts from all regions will be set up 'to elaborate a comprehensive international convention on countering the use of information and communications technolo-

[16] ibid para 16.

[17] CoE, Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems - ETS No.189 (2003).

[18] Cybercrime Convention Committee (T-CY), 'Guidance Notes' (Council of Europe, 2012 - 2019) <https://www.coe.int/en/web/cybercrime/guidance-notes> accessed 15 March 2020.

[19] CoE, Project on Cyberime (September 2006 - February 2009): Final Report (ECD/567, 2009) 5.

[20] CoE, Explanatory Report to the Convention on Cybercrime (n 15) para 306.

[21] CoE, The Global State of Cybercrime Legislation 2013 – 2020: A Cursory Overview (C-PROC, 2019) 5.

[22] See, e.g., Jonathan Clough, 'The Council of Europe Convention on Cybercrime: Defining 'Crime' in a Digital World' (2012) 23 Criminal Law Forum 363, 374 - 87.

[23] Jonathan Clough, 'A World of Difference: The Budapest Convention of Cybercrime and the Challenges of Harmonisation' (2014) 40 Monash University Law Review Monash University 698, 723

[24] See, e.g., Laura Huey and Richard Rosenberg, 'Watching the Web: Thoughts on Expanding Police Surveillance Opportunities under the Cyber-Crime Convention' (2004) 46(5) Canadian Journal of Criminology and Criminal Justice 597.

[25] Jonathan Clough, 'A World of Difference: The Budapest Convention of Cybercrime and the Challenges of Harmonisation' (2014) 40 Monash University Law Review 698, 718-23.

[26] CoE, The Global State of Cybercrime Legislation 2013 – 2020: A Cursory Overview (n 21) 6.

[27] ITU, Understanding Cybercrime: Phenomena, Challenges and Legal Response (n 9) 133.

[28] CoE, Project on Cyberime (September 2006 - February 2009): Final Report (n 19) 5.

[29] UN, Countering the use of information and communications technologies for criminal purposes (A/RES/74/247, 2019).

gies for criminal purposes'.[30] However, the United States (US), the United Kingdom, Canada, Australia and New Zealand argue in favour of the Budapest Convention as an effective global framework against cybercrime.[31]

2.2. *The diffusion of the Budapest Convention*

International norms and policies are diffused in a given community or transferred from one state to another through various mechanisms, that have been conceptualized in the researches of global governance,[32] policy transfer,[33] global diffusion of public policy,[34] norm diffusion in globalization of combating transnational crime,[35] consensus and compliance,[36] and diffusion of international anti-money laundering policies.[37] This paper argues that the Budapest Convention is being diffused, particularly into developing countries, by the mechanism of 'state socialization' or similar concepts (e.g., transnational channels of communication).[38]

'State socialization' appears to be one of the most popular mechanisms for international diffusion of norms. Although the definition of 'state socialization' may vary when being applied in different contexts,[39] it usually works in a similar way. For instance, it is conceptualized as 'a process of inducting actors into the norms and rules of a given community … [i]ts outcome is sustained compliance based on the internalization of these new norms'.[40] 'State socialization' is normally operated through 'normative persuasion' combined with incentives.[41] 'Normative persuasion' often takes place through dynamic communication in international institutions when agents present arguments and try to convince each other of the rightness of the norms. Agents then actively and reflectively internalize the new understanding of appropriateness.[42] This process can occur at conferences, workshops and training sessions.[43] In addition, transnational learning facilitates 'normative persuasion'. For example, governmental officials and private sector employees are invited and encouraged to participate in conferences, seminars and training courses organized by various countries, international organizations or private actors, where an international norm is introduced. At these events, the participants can learn and 'draw lessons' from experts, their counterparts and other countries about how the norm would be nationally adopted.[44].

---

[30] ibid 3.

[31] Quintet of Attorneys General, 'Quintet of Attorneys General Statement on international cooperation on cybercrime' (Quintet Meeting of Attorneys General, 2019) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/822317/Cybercrime_statement_signed.pdf> accessed 27 April 2020.

[32] See Helge Jörgens, 'Governance by Diffusion-Implementing Global Norms through Cross-National Imitation and Learning' in William M. Lafferty (ed), Governance for Sustainable Development: The Challenge of Adapting Form to Function (Edward Elgar Publishing Limited 2004) 248-57. Helge Jörgens and other scholars contend that there are three mechanisms of global governance: harmonization, imposition and diffusion. International stimuli generally influence domestic politics through multilateral harmonization, unilateral imposition and cross-national diffusion.

[33] See David Dolowitz and David Marsh, 'Who Learns What from Whom: A Review of the Policy Transfer Literature' (2006) 44(2) Political Studies 343, 346-49. The authors argue that there are three forms of policy transfer from one country to another: voluntary transfer, direct coercive transfer and indirect coercive transfer.

[34] Frank Dobbin, Beth Simmons and Geoffrey Garrett, 'The Global Diffusion of Public Policies: Social Construction, Coercion, Competition or Learning?' (2007) 33 Annual Review of Sociology 449.

[35] See Paulette Lloyd, Beth Simmons and Brandon Stewart, 'Combating Transnational Crime: The Role of Learning and Norm Diffusion in the Current Rule of Law Wave' in Michael Zürn, André Nollkaemper and Randall Peerenboom (eds), Rule of Law Dynamics: In an Era of International and Transnational Governance (Cambridge University Press 2012) 164-70. The authors discuss the global diffusion of norms and policies to address transnational crime, with a focus on human trafficking. They develop two possible mechanisms of normative diffusion: negative externalities and hegemonic pressure.

[36] See Susan Kneebone and Julie Debeljak, Transnational Crime and Human Rights: Responses to Human Trafficking in the Greater Mekong Subregion (Routledge 2012). The authors use the notion of "communicative action" or "argumentative rationality" to explain why States comply with the obligation set out by international law, with a focus on the obligation of combating human trafficking.

[37] J.C. Sharman, The Money Laundry: Regulating Criminal Finance in the Global Economy (Cornell University Press 2011) 99-164, the author points out that the international AML standards have diffused through soft tools of governance: blacklisting, ranking, structuring incentives for uncoordinated private actors, socialization and regulatory competition. And in Sebastian Heilmann and Nicole Schulte-Kulkmann, 'The Limits of Policy Diffusion: Introducing International Norms of Anti-Money Laundering into China's Legal System' (2011) 24(4) Governance: An International Journal of Policy, Administration, and Institution 639, 644 - 50, the authors argue that China has engaged with the international AML regime under diffusion by transnational communication, imposition, legal harmonization and regulatory competition.

[38] Helge Jörgens, Governance by Diffusion-Implementing Global Norms through Cross-National Imitation and Learning (n 32), 255; and Sebastian Heilmann and Nicole Schulte-Kulkmann, The Limits of Policy Diffusion: Introducing International Norms of Anti-Money Laundering into China's Legal System (n 37) 644-46.

[39] Various concepts of socialization are given in Dawson E. Richard and Kenneth Prewitt, Political Socialization : An Analytic Study (Little, Brown and Company 1969); G. John Ikenberry and Charles Kupchan, 'Socialization and Hegemonic Power' (1990) 44(03) International Organization 283, 289; Jeffrey T. Checkel, 'International Institutions and Socialization in Europe: Introduction and Framework' (2005) 59(04) International Organization 801, 804; and Kai Alderson, 'Making Sense of State Socialization' (2001) 27(03) Review of International Studies 415, 417.

[40] Jeffrey T. Checkel, International Institutions and Socialization in Europe: Introduction and Framework (n 39) 808-13.

[41] G. John Ikenberry and Charles Kupchan, Socialization and Hegemonic Power (n 39) 290-92; and Jeffrey T. Checkel, International Institutions and Socialization in Europe: Introduction and Framework (n 39) 808-13. How the FATF persuade countries to implement and comply with the AMLSs was also illustrated by Kenneth S. Blazejewski, 'FATF and Its Institutional Partners: Improving the Effectiveness and Accountability of Transgovernmental Networks' (2008) 22 Temple International and Comparative Law Journal 1, 16-18.

[42] Jeffrey T. Checkel, International Institutions and Socialization in Europe: Introduction and Framework (n 39) 812.

[43] J.C. Sharman, The Money Laundry: Regulating Criminal Finance in the Global Economy (n 37) 138-50.

[44] In Richard Rose, 'What Is Lesson-Drawing?' (1991) 11(1) Journal of Public Policy, 6-10, the author considers "lesson-drawing" as a popular means used to transfer an effective 'programme' from one state to another.

The diffusion of the Budapest Convention is encouraged and underpinned by various bodies, initiatives and activities.[45] The process of 'state socialization' occurs at various platforms, such as the Cybercrime Convention Committee (T-CY) meetings, training provided by the Programme Office on Cybercrime (C-PROC), and at Octopus Conferences & Workshops, where 'normative persuasion' is conducted and 'lessons' are drawn. T-CY assesses the implementation of the Convention by the Parties, and encourages the accession of states which are not CoE members to the Convention.[46] Representatives of state Parties, Observers and international organisations (e.g., the Commonwealth Secretariat, INTERPOL, the International Telecommunication Union (ITU), the United Nations Office on Drugs and Crime (UNODC) and others) participate as members or observers in T-CY.[47] In 2014, the Cybercrime Programme Office of the Council of Europe (C-PROC) was established to assist countries worldwide in strengthening their legal system against cybercrime and dealing with electronic evidence on the basis of the Budapest Convention.[48] The assistance includes training judges, prosecutors and law enforcement officers; establishing specialized cybercrime and forensic units; and promoting the effectiveness of international cooperation. In addition, from 2013 to 2016 there was a joint project of the European Union and the Council of Europe named Global Action on Cybercrime (GLACY), which aimed at supporting countries globally in the implementation of the Budapest Convention, with the focus on harmonizing national legislation, judicial training, information sharing and enhancing law enforcement capacities.[49] This project has been followed by GLACY+ (2016–2024), which supports fifteen priority and hub countries in Africa, Asia-Pacific, Latin America and the Caribbean region, including Benin, Burkina Faso, Cabo Verde, Chile, Costa Rica, Dominican Republic, Ghana, Mauritius, Morocco, Nigeria, Paraguay, Philippines, Senegal, Sri Lanka and Tonga. These countries are expected to be hubs that share their experience within their respective regions.[50] Cybercrime@Octopus, a CoE project, assists the organisation of the annual Octopus conferences; co-funds and supports the functioning of T-CY with its enlarged membership; and provides assistance to states prepared to implement the Convention, the related instruments on data protection and the protection of children.[51] Held every 12 to 18 months by the Council of Europe, the Octopus Conference is one of the biggest and best international exchange forums featuring cybercrime experts from 80 countries, international organizations, the private sector and academia.[52] Each Octopus Conference normally focuses on the latest cybercrime issue. As can be seen, T-CY, C-PROC and Cybercrime@Octopus play important roles in diffusing the Convention and ensuring that states joining the Convention are able to implement and comply with its provisions, and to cooperate with other Parties.

In the Pacific, the Council of Europe, through the GLACY+ project, has co-funded three regional workshops in the context of the Pacific Islands Law Officers' Network (PILON) to facilitate the exchange of knowledge and experience on combating cybercrime among law enforcement officers from the region.[53] The workshops focused on international standards and good practices in legislation, e-evidence and cooperation mechanisms in fighting cybercrime.[54] Since 2015, the fight against cybercrime has been prioritized in the PILON's agenda.[55] Under the PILON Strategic Plan 2016 - 2018, the legal framework against cybercrime was recognised as a priority for PILON. A Cybercrime Working Group has subsequently been formed to strengthen the regional response to cybercrime, with an emphasis on the development and implementation of legislation in line with the Budapest Convention.[56]

As part of the GLACY and extended GLACY+ project, Tonga has been provided with judicial training, advice on legislation and law enforcement capacity building. Tonga legislated a Computer Crime Acts 2003,[57] which was the first comprehensive legislation against cybercrime in the Pacific. In preparation for joining the Convention, Tonga made amendments to the Act in 2016.[58] Tonga consequently acceded to the Budapest Convention in 2017. In compliance with the Convention, an

[45] See e.g., CoE, Project on Cyberime (September 2006 - February 2009): Final Report (n 19) 6-40.

[46] Cybercrime Convention Committee (T-CY), T-CY Rules of Procedure (Council of Europe 2019) 3. The Rules of Procedure, adopted by the 10th Plenary of the T-CY (3 December 2013), had subsequently been revised by 12th Plenary (3 December 2014) and the 18th Plenary (28 November 2017).

[47] CoE, 'T-CY Plenaries' (Council of Europe, 2019) <https://www.coe.int/en/web/cybercrime/t-cy-plenaries> accessed 17 April 2020'.

[48] CoE, 'About C-PROC' (Council of Europe, 2020) <https://rm.coe.int/cproc-about-eng-v20-april-2020/16809e32f1> accessed 25 May 2020.

[49] CoE, 'Global Action on Cybercrime' (Council of Europe, 2013) <https://www.coe.int/en/web/cybercrime/glacy> accessed 27 May 2020.

[50] CoE, 'Global Action on Cybercrime Extended (GLACY)+' (Council of Europe, 2020)accessed 10 June 2020.

[51] CoE, 'CyberCrime@Octopus (DG1/3021)' (Council of Europe, 2019) <https://rm.coe.int/summary-of-the-cybercrime-octopus/1680968ab0> accessed 15 June 2020.

[52] CoE, 'Octopus Conferences 2007 - 2019′ (Council of Europe, 2019) <https://www.coe.int/en/web/cybercrime/octopus-conference> accessed 15 June 2020.

[53] PILON is a network of senior law officers from PICs, Australia and New Zealand, who work together to address domestic and regional law and justice issues.

[54] Government of Tonga, 'Second Pacific Islands Law Officer's Network Cybercrime Workshop on Combatting Online Child Abuse' (Ministry of Information and Communications, 2018) <http://www.mic.gov.to/news-today/press-releases/7336-tonga-hosts-the-second-pacific-islands-law-officers-network-pilon-cybercrime-workshop> accessed 18 June 2020; and Vanuatu, 'PILON 3rd Cybercrime Workshop - May 2019′ (Council of Europe, 2019) <https://www.coe.int/en/web/cybercrime/third-annual-pilon-cybercrime-workshop> accessed 18 June 2020.

[55] During the 34th PILON Annual meeting in Honiara (Solomon Islands), the member countries decided and approved that cybercrime legislation is one of the priorities in PILON's policy agendas.

[56] PILON, Pacific Islands Law Officers' Network Cybercrime Workshop, 23–25 May 2017 (Talanoa, 2017) 1.

[57] Computer Crimes Act 2003 (Tonga, Act 14 of 2003).

[58] Computer Crimes Act 2003 (Tonga, 2016 Revised Edition).

updated Computer Crimes Bill 2019 will be introduced to the Tongan Legislative Assembly. As the first Pacific Island state to have joined the Budapest Convention, Tonga is set to become a model for the neighboring states and to share its experience of becoming a Party to the Convention.

Other states, such as Samoa,[59] Vanuatu[60] and Fiji,[61] have also benefited from the Council of Europe's projects on cybercrime, and expressed an intention to accede to the Budapest Convention. The first draft of the Fiji Cybercrime Bill 2020 was introduced to the public for feedback in early 2020.[62] The Bill has incorporated the amendments suggested by the Council of Europe to align itself with the Budapest Convention. Within the framework of the GLACY+ and the Cybercrime@Octopus Projects, Vanuatu is also being assisted to amend its current Cybercrime Bill.[63] In 2016, Papua New Guinea passed the Cybercrime Code Act 2016,[64] the drafters having taken the Convention into account.

It can be argued that the mechanism of 'state socialization' combined with incentives, such as capacity building, is working effectively in diffusing the Budapest Convention among PICs. The Convention is now the benchmark for these countries in reforming and drafting their anti-cybercrime legislation. In the near future, a number of PICs will have national cybercrime laws in line with the Convention. This article now examines how cybercrime-related laws have been and/or will be developed in PICs, and then argues that various internal factors will deter the enforcement of these laws.

3. The development of cybercrime legislation in PICs

It appears that PICs have reformed and developed their cybercrime legislation by the process of 'legal transplant', in which international and foreign legal norms are adopted into a domestic legal system.[65] PICs have a long history of borrowing foreign laws, including criminal law.[66] In terms of cybercrime laws, it is evident that the lawmakers of many PICs have 'transplanted' statutory provisions deriving from foreign jurisdictions (e.g., Australia) and the Budapest Convention. The Crimes Act 2009 of Fiji is substantially based on the Model Criminal Code of Australia.[67] Computer offences are provided for in sections 336 to 351 of the Act, which are similar to the provisions in Cybercrime Act 2001 of Australia.[68] In 2012, the Australian Government passed the Cybercrime Legislation Amendment Act 2012 (Cth),[69] which enables Australia to accede to the Budapest Convention. The Cybercrime Bill 2020 of Fiji has followed the Australian model. The Convention also had clear influence on the Tongan Computer Crimes Act 2003 (amended 2016).[70] An updated Computer Crimes Bill 2019 of Tonga was recently drafted with the assistance of the Australian Attorney General's Department.[71] In addition, the GLACY+ project organized an in-country advisory mission on the Bill. The Cybercrime Bill 2015 of Vanuatu and the Cybercrime Code Act 2016 of Papua New Guinea also imported several provisions of the Budapest Convention,[72] and were significantly influenced by the Commonwealth Model Law on Computer and Computer Related Crime.[73]

3.1. *Criminalization of cybercrime*

Some PICs have criminalized cybercrime offences in their cybercrime statues or criminal laws at different extent, others have the relevant legislation (e.g., Telecommunications Acts) in place applicable to various typologies of cybercrime. The below Table 1 details the existing criminalization of cybercrime in ten PICs. In order to identify what types of cybercrime have

[59] In 2018, the Council of Europe and the Attorney General's Office of Samoa organized two workshops to assess the Samoan legislation, and provide trainings for judges, prosecutors and law enforcement agencies on cybercrime and electronic evidence. See, CoE, 'GLACY+: Samoa takes first steps towards the Budapest Convention' (Samoa, 2018) <https://www.coe.int/en/web/cybercrime/-/glacy-samoa-takes-first-steps-towards-the-budapest-conventi-1> accessed 18 June 2020.

[60] In 2018, Vanuatu was invited to attend the Octopus Conference on Cybercrime. The Council of Europe will assist the country with the drafting of the Cybercrime Bill. See, 'Vanuatu participates in Octopus Conference on Cybercrime in France' Dailypost (Vanuatu 17 July 2018) <https://dailypost.vu/news/vanuatu-participates-in-octopus-conference-on-cybercrime-in-france/article_ab95c39c-5588-52bf-8797-ec4fe41c6d4b.html> accessed 18 June 2020.

[61] In 2019, following the declared intention of the Fijian government to accede to the Convention, the draft of the first Cybercrime Bill of Fiji was assessed in the framework of the GLACY+ and the Cybercrime@Octopus Projects. See, CoE, 'GLACY+: Advisory mission on cybercrime legislation in Fiji' (Suva, 2019) <https://www.coe.int/en/web/cybercrime/-/glacy-advisory-mission-on-cybercrime-legislation-in-fiji> accessed 19 June 2020.

[62] Cybercrime Bill 2020 (Fiji, 2019).

[63] Bill for the Cybercrime Act (Republic of Vanuatu, 2015); and CoE, 'Vanuatu on the way to develop cybercrime legislation' (GLACY+ Activities, 2018) <https://www.coe.int/en/web/cybercrime/-/vanuatu-on-the-way-to-develop-cybercrime-legislation> accessed 19 June 2020.

[64] Cybercrime Code Act 2016 (Papua New Guinea, No. 35 of 2016).

[65] Kahn-Freund clarifies the meaning of "transplant" by taking the example of transferring human organs (see Otto Kahn-Freund, 'On Uses and Misuses of Comparative Law' (1974) 37(1) The Modern Law Review 1, 5-6).

[66] See Jennifer Corrin and Don Paterson, Introduction to South Pacific Law (4th edn, Routledge 2017); and Eric Colvin, 'Criminal Procedure in the South Pacific' (2004) 8(1) Journal of South Pacific Law 1, 1.

[67] Crimes Act 2009 (Fiji, No 44 of 2009). See Eric Colvin, Criminal Law of Fiji (LexisNexis NZ Limited 2017) 3-4.

[68] Cybercrime Act 2001 (Australia, No. 161, 2001)

[69] Cybercrime Legislation Amendment Act 2012 (Australia, No. 120, 2012)

[70] Computer Crimes Act 2003 (Tonga, 2016 Revised Edition) (n 58).

[71] See Department of Foreign Affairs and Trade (Australia), 'Australia's International Cyber Engagement Strategy' <https://www.dfat.gov.au/publications/international-relations/international-cyber-engagement-strategy/aices/chapters/part_3_cybercrime.html> accessed 28 September 2020.

[72] Cybercrime Code Act 2016 (Papua New Guinea, No. 35 of 2016) (n 64).

[73] The Commonwealth, Model Law on Computer and Computer Related Crime (n 10).

Table 1 – Criminalization of cybercrime by PICs.[a]

Country	Statues	Forms of Cybercrime
Cook Islands	Telecommunications Act 2019[b]	Ss85–87: Interfering with telecommunications service
	Crimes Act 1969[c]	Ss135–138: Offences related to indecent material, which may apply to online child pornography
	Copyright Act 2013[d]	Offences for infringement of copyright
Fiji	Crimes Act 2009[e]	Part 17, Division 6: Offences for unauthorized modification of data to cause impairment; unauthorized impairment of electronic communication; unauthorized access to (or modification of) restricted data; unauthorized impairment of data held on a computer disk; and possession, control, production, supply or obtaining of data with intent to commit a computer offence; Part 11, Sub-division D: Forgery and related offences
	Posts and Telecommunications Decree 1989[f]	Part IV: offences for modification, interception and disclosure of messages
Kiribati	Telecommunications Act 2004[g]	Part VI: Offences for modification, interception and disclosure of messages; Part VII: Computer misuse offences - unauthorized access, modification, use or interception; Part VI: Grossly offensive use of a telecommunications system; Part VIII: Distribution and exhibition of obscene matter, including in electronic form, which may apply to child exploitation material
Nauru	Cybercrime Act 2015[h]	Part 2: Offences for illegal access, interception, data interference, data espionage, system interference, distributing/possessing software/a device for committing a crime; computer-related forgery and fraud, including identity theft; producing, offering, distributing, procuring, possessing or knowingly obtaining access to child pornography 'through an electronic system'; online solicitation of children; publishing of indecent material in electronic form
	Telecommunications Act 2002[i]	Ss43–44: Offences for intercepting, using, or disclosing communications (applicable only to telecommunications employees) and interfering with communications (by any person); S45: Sending messages of an offensive, indecent, obscene or menacing character (via telecommunications)
	Crimes Act 2016[j]	Ss139–143: Offences for pornography and exposing child to offensive material; S189: Offence for making or possessing device for making false document
Papua New Guinea	Cybercrime Code Act 2016[k]	Ss6–31: Extensive offences for Unauthorized access or hacking, illegal interception, data interference, system interference, data espionage, illegally remaining, electronic fraud, electronic forgery, electronic gambling or lottery by a child, identity theft, illegal devices, pornography, child pornography, child online grooming, animal pornography, defamatory publication, cyber bullying, cyber harassment, cyber extortion, unlawful disclosure, spam, cyberattack, online copyright infringement, online trade mark infringement, patent and industrial designs infringement, unlawful advertising.
	Protection of Private Communications Act 1973[l]	Part II: Offences for intercepting private communications and divulging such communications
	Criminal Code Act 1974[m]	Division 2B: Offences for producing and distributing child pornography
Samoa	Crimes Act 2013[n]	Part 18: Extensive offences for electronic systems - accessing without authorization, accessing for a dishonest purpose, illegal remaining, illegal interception, damaging or interfering with electronic data, illegal acquisition of electronic data, illegal system interference, and illegal devices; identity fraud, forgery of electronic data, spam, solicitation of children, and harassment utilizing means of electronic communication
	Telecommunications Act 2005(	S74: Offences for telecommunications networks or computer systems - unauthorized access, interception, alteration of data, hindering of a network or system, sale of devices or data to facilitate above offences, use of a telecommunications network to offend or harass
	Copyright Act 1998[p]	Criminal sanctions for copyright infringement
Solomon Islands	Telecommunications Act 2009[q]	Part 19: Telecommunications offences -infringing security to obtain data, intercepting messages, altering/destroying/deleting data, revealing contents of messages, impeding or delaying messages, and possessing a device to do any of the above

(*continued on next page*)

Table 1 (*continued*)

Country	Statues	Forms of Cybercrime
Tonga	Computer Crimes Act 2003[r]	Ss4–8: Offences for Illegal access, interfering with data, interfering with computer system, illegal interception of data, illegal devices
	Communications Act 2015,[s] Pornography Control Act 2002,[t], Copyright Act 2002[u]	Other offences for: Identity theft, fraud and forgery, child pornography
Tuvalu	Tuvalu Telecommunications Corporation Act (2008 Revised Edition)[v]	S33: Telecommunications offences -modifying or interfering with messages, interception, and disclosure of intercepted messages; sending of a grossly offensive message
Vanuatu	Penal Code ((Consolidated Edition 2006)[w]	S73C(vii): Computer offences limited related to terrorism; Ss147A&147B: child pornography offences
	Telecommunications Act (Consolidated Edition 2006)[x]	Part 10: Telecommunications offences - intentional damage, interception and disclosure

[a] Compiled and updated by the authors with reference to CoE, The Pacific Response to Cybercrime: Effective Tools and Good Practices (PILON Cybercrime Workshop, Vanuatu, 2017).
[b] Telecommunications Act 2019 (Cook Islands, No. 7, 2019).
[c] Crimes Act 1969 (Cook Islands, No. 20, 1969).
[d] Copyright Act 2013 (Cook Islands, No. 8, 2013).
[e] Crimes Act 2009 (Fiji, No 44 of 2009) (n 67).
[f] Posts and Telecommunications Decree 1989 (Fiji, No. 37, 1989).
[g] Telecommunications Act 2004 (Kiribati, No. 11 of 2004).
[h] Cybercrime Act 2015 (Nauru, No. 14 of 2015).
[i] Telecommunications Act 2002 (Nauru, 2002).
[j] Crimes Act 2016 (Nauru, Act No. 18 of 2016).
[k] Cybercrime Code Act 2016 (Papua New Guinea, No. 35 of 2016).
[l] Protection of Private Communications Act 1973 (Papua New Guinea, Chapter 272).
[m] Criminal Code Act 1974 (Papua New Guinea, Chapter 262).
[n] Crimes Act 2013 (Samoa, No. 10, 2013).
[o] Telecommunications Act 2005 (Samoa, No. 20, 2005).
[p] Copyright Act 1998 (Samoa, No. 25, 1998).
[q] Telecommunications Act 2009 (Solomon Islands, No. 20 of 2009).
[r] Computer Crimes Act 2003 (Tonga, 2016 Revised Edition) (n 58).
[s] Communications Act 2015 (Tonga, No. 12 of 2015).
[t] Pornography Control Act 2002 (Tonga, Act 33 of 2002).
[u] Copyright Act 2002 (Tonga, Act 12 of 2002).
[v] Tuvalu Telecommunications Corporation Act (Tuvalu, CAP. 35.05, 2008 Revised Edition).
[w] Penal code (Vanuatu, Chapter 135, Consolidated Edition 2006).
[x] Telecommunications Act (Vanuatu, Chapter 206, Consolidated Edition 2006).

been provided in these countries, the authors rely on the concept and categories of cybercrime stated in the Budapest Convention and in the Commonwealth Model Law on Computer and Computer Related Crime.

It can be seen that Fiji, Nauru, Papua New Guinea, Samoa and Tonga have provided for a broad category of cybercrime, which is closest to the provisions of the Budapest Convention and the Commonwealth Model Law on Computer and Computer Related Crime.

Nauru, Papua New Guinea and Tonga have their own Cybercrime/Computer Crimes statutes, which have include new forms of cybercrime. In other PICs, cybercrime is currently scattered in both their substantive criminal law and telecommunications legislation. Some of these countries, as mentioned earlier, are either amending their criminal law or designing a separate statute on cybercrime to ensure compliance with the Budapest Convention. However, adopting a cybercrime legislation separately might result in duplication or an overlap of some cybercrime provisions, which would confuse law enforcement agencies in the application of the laws. For instance, both the Cybercrime Code Act 2016 (section 18) and Criminal Code Act 1974 (sections 229R, 229S & 229T) of Papua New Guinea criminalize child pornography, and there is no guidance on how to distinguish these provisions. Equally, the majority of existing legal provisions might be applicable to various cybercrime typologies. For example, laws addressing frauds and forgery could be applied to electronic documents. It appears that some PICs have not carefully reviewed and identified gaps in the existing cybercrime legislation before passing the new laws. Thus, they do not have an inappropriate extent of criminalization of cybercrime acts (inadequate or over-criminalization).

It is also important to note that, in reforming the current cybercrime laws, PICs should take local contexts into account alongside global standards, as cybercrime can be committed domestically and internationally. Cybercrime typologies criminalized in particular countries may vary. For instance, PICs identified spam as the most cybercrime-related incident.[74] Thus, the fact that developed countries do not criminalize

[74] ITU, Capacity Building and ICT Policy, Regulatory and Legislative Frameworks Support for Pacific Island States (n 5) 4.

spam should not limit the scope of criminalization of spam in PICs.

3.2. *Procedural measures and international cooperation*

The investigation of cybercrime normally requires sophisticated techniques and legal instruments dealing with computer data, which includes expedited preservation of computer data, the disclosure of data, search and seizure, interception of computer data, and collection of traffic data.

Article 1(d) of the Budapest Convention defines 'traffic data' as 'any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service'. 'Traffic data' is produced within data-transfer processes, not the transferred data themselves. The analysis of traffic data is usually required to identify the IP address of the server, and then help to locate the server location and the offender. 'Content data' refers to the content of the Internet communication, for example, the subject of an e-mail, the content on a website, the content of a VoIP conversation.[75] Access to 'content data' allows competent authorities to analyse the nature of the communication. However, the computer data might be deleted or modified if the offender is aware of an investigation. Law enforcement agencies, thus, need to preserve and collect computer data, in real-time, as a crucial source of evidence. Articles 16, 17, 20 & 21 of the Convention obliges its state Parties to adopt legal provisions enabling competent authorities to order the expeditious preservation of stored computer data and traffic data, and collect computer data in real-time.

Search and seizure is often used in cybercrime investigations. Most current national criminal procedure laws provide the conditions and procedure for searching and seizing physical objects. These might not be applicable to, or sufficient for, data-related search and seizure.[76] For instance, traditional provisions would only allow authorised agencies to seize an entire server, but not make a copy of just the relevant stored data. This can cause problems in circumstances where the seized server stores not only the sought information, but also the data of other users; or where the server cannot be located. Article 19 of the Budapest Convention establishes and requires its Parties to adopt a legal framework that enables the search and seizure of a computer system and computer data stored therein.

The investigation of transnational cybercrime requires the cooperation of law enforcement agencies in all the related countries. The formal mechanisms of international cooperation in combating cybercrime are mutual legal assistance and extradition. Mutual assistance regarding provisional measures is particularly important, which includes expedited preservation of stored computer data, expedited disclosure of preserved traffic data, accessing of stored computer data, and the real-time collection of computer data.[77]

The below Table 2 examines the existing legislation of PICs with respect to the above mentioned procedural measures and international cooperation against cybercrime, in comparison with respective provisions of the Budapest Convention.

As we can see, only Tonga has an adequate legal framework for the specialized procedural measures often deployed in cybercrime investigations. Other countries do not have laws regulating the preservation of data and the real-time collection of data. All the countries have laws on criminal procedure (e.g., search and seizure), extradition and mutual legal assistance, but it is unclear if these laws are applicable to cybercrime. As the result, while the legal basis for international cooperation is available, PICs might not be able to process a request for assistance in conducting the provisional measures related to computer data.

4. Law enforcement capacity

In order to combat cybercrime, law enforcement authorities and courts must have the ability to investigate, prosecute and convict offenders. Most importantly, they should be able to deal with digital evidence. However, digital evidence is still a novel concept in most PICs. The countries discussed below are active in fighting cybercrime, but their law enforcement has been precluded by various challenges.

Being a state Party to the Budapest Convention and benefitting from the GLACY+ project, Tonga is expected to soon have the most comprehensive cybercrime legislation. Tonga is among PICs that have implemented legislation dealing with digital evidence. Several Tonga police officials, prosecutors and judges have been trained in the area of cybercrime and electronic evidence. Tonga was the first Pacific Island country to establish a national Computer Emergency Response Team (CERT) in 2016. Despite these efforts, at the time of writing this article, there has been only two cases formally prosecuted in the Tongan courts.[78] The implementation of cybercrime laws in Tonga is being closely observed, particularly in terms of data privacy safeguards as required by article 15 of the Budapest Convention.[79] It should be noted that Tonga currently lacks data protection laws, and is one of the few countries that have not yet ratified the 1966 United Nations International Covenant on Civil and Political Rights (ICCPR).[80]

[75] ITU, Understanding Cybercrime: Phenomena, Challenges and Legal Response (n 9) 260.

[76] ibid 252-254.

[77] CoE, Convention on Cybercrime - ETS No.185 (2001), articles 29-34.

[78] CR151/2008 Rex -v- Sione Tali Taufa Nau, and CR11-12/2010 Rex -v- Misi & Tovi.

[79] See further discussion about this matter in Luca Tosoni, 'Rethinking Privacy in the Council of Europe's Convention on Cybercrime' (2018) 34(6) Computer Law & Security Review, 1204-05.

[80] Article 17 reads: '1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. 2. Everyone has the right to the protection of the law against such interference or attacks.'

Table 2 – PICs Legislation on Procedure and International Cooperation in Combating Cybercrime.[a]

Country	Procedural Law	International Cooperation
Cook Islands	**Preservation of data – none** **Search and seizure**: S96 of *Criminal Procedure Act 1980–81* provides for general search and seizure powers (no clear application to electronic evidence).[b] Digital Registers Act 2011 amends Evidence Act 1968 to provide for admissibility of digital evidence.[c] **Real-time collection of data**: s3 of *Criminal Procedure Amendment Act 2003* provides for interception of communications involving organized crime.[d]	**Extradition:** *Extradition Act 2003 & Fugitive Offenders Act 1969* covers rules and procedure for extradition, for offences with a minimum penalty of 1 year.[e] **Mutual legal assistance**: *Mutual Assistance in Criminal Matters Act 2003* coves rules and procedures for mutual legal assistance in criminal matters, for offences with a minimum penalty of 1 year imprisonment or $5000 fine.[f]
Fiji	**Preservation of data**: *Posts and Telecommunications Decree 1989*,[g] s62 provides for the Minister to make regulations with respect to the period during which and the conditions subject to which messages and papers relating thereto, belonging to, or in custody of carriers shall be preserved . **Search and seizure**: *Posts and Telecommunications Decree 1989*, s61 provides for the President to require production of messages by warrant. Criminal Procedure Decree 2009, Part IX provides for general search and seizure powers (no clear application to electronic evidence).[h] **Real-time collection of data – none.**	**Extradition**: *Extradition Act 2003* covers rules and procedure for extradition, for an offence with a minimum penalty of 1 year and with dual criminality; and provides for the taking of evidence for the purpose of criminal proceedings in a requesting country.[i] **Mutual legal assistance**: *Mutual Assistance in Criminal Matters Act 1997* covers rules and procedures for mutual legal assistance in criminal matters, extending to any foreign country that has an arrangement or a reciprocal agreement on assistance in criminal matters with Fiji.[j]
Kiribati	**Preservation of data – none** **Search and seizure**: *Criminal Procedure Code*, Part IV provides for general search and seizure powers (no clear application to electronic evidence).[k] **Real-time collection of data – none.**	**Extradition**: *Extradition Act 2003* provides for rules and procedure for extradition, for an offence with a minimum penalty of 1 year and with dual criminality.[l] **Mutual legal assistance**: *Mutual Assistance in Criminal Matters Act 2003* provides rules and procedures for mutual legal assistance in criminal matters. Taking of evidence or production of documents can be undertaken/requested for the purposes of a proceedings or investigation in relation to any criminal matter. Search and seizure powers can be exercised/requested for offences with a minimum penalty of 1 year.[m]
Nauru	**Preservation of data**: *Cybercrime Act 2015*, Part 3 provides for production orders and expedited preservation of data.[n] **Search and seizure**: *Cybercrime Act 2015*, Part 3 provides search and seizure powers to electronic evidence as well as collection of traffic data. **Real-time collection of data**: *Cybercrime Act 2015*, Part 3 provides for interception of content data where reasonably required for the purposes of a criminal investigation, as well as use of 'remote forensic tools'.	**Extradition**: *Extradition of Fugitive Offenders Act 1973* provides for rules and procedure for extradition, for a limited list of offences with a minimum penalty of 1.[o] **Mutual legal assistance**: *Mutual Assistance in Criminal Matters Act 2004* provides for rules and procedures for mutual legal assistance in criminal matters for offences with a minimum penalty of 1 year and requiring dual criminality.[p]
Papua New Guinea	**Preservation of data:** *Cybercrime Code Act 2016*, s36 allows a member of the Police Force to order expedited preservation of data. **Search and seizure**: *Search Act 1977*, Part III provides for general search and seizure powers;[q] *National Intelligence Organization Act 1984* provides for general search and seizure powers;[r] *Evidence Act 1975*, Part IV, Division 5 establishes admissibility of 'computerized information';[s] *Cybercrime Code Act 2016*, ss32 & 33 refer to the search and seizure of electronic system/devices and data. **Real-time collection of data**: *Protection of Private Communications Act 1973*, s15 provides for interception warrants for the prevention or investigation of offences with a minimum penalty of 7 years, and s18 establishes evidentiary value of intercepted communications.[t]	**Extradition**: *Extradition Act 2005* provides for rules and procedure for extradition for an offence with a minimum penalty of 1 year.[u] **Mutual legal assistance**: *Mutual Assistance in Criminal Matters Act 2005* covers rules and procedures for mutual legal assistance in criminal matters. Search and seizure powers can be exercised/requested for offences with a minimum penalty of 1 year.[v]
Samoa	**Preservation of data – none.** **Search and seizure**: *Criminal Procedure Act 1972*,[w] s83 provides for general search and seizure powers which could apply to electronic evidence; *Police Powers Act 2007*,[x] s32(1)(d) provides powers to police to seize other things found at the premises in the course of the search that the executing officer or assisting officer believe on reasonable grounds to be evidential material in relation to an offence. **Real-time collection of data**: *Police Powers Act 2007*, Part 2 - Surveillance warrants allow police to gather information and evidence that will assist them in combating organized crime.	**Extradition**: *Extradition Act 1974* provides for rules and procedure for extradition for an offence with a minimum penalty of 1 year.[y] **Mutual legal assistance**: *Mutual Assistance in Criminal Matter Act 2007* covers rules and procedures for mutual legal assistance in criminal matters relating to 'serious offences'.[z]
Solomon Islands	**Preservation of data – none.** **Search and seizure**: *Criminal Procedure Code*,[aa] s101 provides for general search and seizure powers which could apply to electronic evidence. **Real-time collection of data - none**	**Extradition**: *Extradition Act 2010* provides for rules and procedure for extradition for an offence with a minimum penalty of 1 year.[ab] **Mutual legal assistance**: *Mutual Assistance in Criminal Matters Act 2002* covers rules and procedures for mutual legal assistance in criminal matters for offences with a minimum penalty of 1 year.[ac]

(*continued on next page*)

Table 2 (*continued*)

Country	Procedural Law	International Cooperation
Tonga	**Preservation of data**: *Computer Crimes Act 2003*,[ad] s13 allows police to order a person in control of a computer system to preserve for the purpose of a criminal investigation. **Search and seizure:** *Computer Crimes Act 2003*, s9 provides the procedure for search & seize electric evidence. **Real-time collection of data:** *Computer Crimes Act 2003*, ss14–15 provides for interception of electronic communications and content data where reasonably required for the purposes of a criminal investigation.	**Extradition**: *Extradition Act* provides for rules and procedure for extradition for an offence with a minimum penalty of 1 year and with dual criminality.[ae] **Mutual legal assistance:** *Mutual Assistance in Criminal Matters Act 2000*, s8 allows authorized officers to apply for search warrants or evidence-gathering orders related to requests for assistance.[af]
Tuvalu	**Preservation of data – none.** **Search and seizure:** *Criminal Procedure Code*,[ag] **s**101 provides for general search and seizure powers which could extend to electronic evidence; *Police Powers and Duties Act 2009*,[ah] s61 refers to search warrant powers including accessing and making copies of electronic evidence. **Real-time collection of data - none**	**Extradition**: *Extradition Act 2004* provides for rules and procedure for extradition for an offence with a minimum penalty of 1 year.[ai] **Mutual legal assistance**: *Mutual Assistance in Criminal Matters Act* covers rules and procedures for mutual legal assistance in criminal matters. Search and seizure powers can be exercised/requested for offences with a minimum penalty of 1 year.[aj]
Vanuatu	**Preservation of data – none** **Search and seizure**: *Criminal Procedure Code*,[ak] s55 provides for general search and seizure powers which could apply to electronic evidence **Real-time collection of data - none**	**Extradition**: *Extradition Act* provides for rules and procedure for extradition for an offence with a minimum penalty of 1 year.[al] **Mutual legal assistance**: *Mutual Assistance in Criminal Matters Act* covers rules and procedures for mutual legal assistance in criminal matters. Search and seizure powers can be exercised/requested for offences with a minimum penalty of 1 year.[am]

[a] Compiled and updated by the authors with reference to CoE, The Pacific Response to Cybercrime: Effective Tools and Good Practices (n 74).
[b] Criminal Procedure Act 1980–81 (Cook Islands, No. 28, 1981).
[c] Digital Registers Act 2011 (Cook Islands, No. 11, 2011).
[d] Criminal Procedure Amendment Act 2003 (Cook Islands, No. 4, 2003).
[e] Extradition Act 2003 (Cook Islands, No. 8, 2003) and Fugitive Offenders Act 1969 (Cook Islands, No. 1, 1969).
[f] Mutual Assistance in Criminal Matters Act 2003 (Cook Islands, No. 9, 2003).
[g] Posts and Telecommunications Decree 1989 (Fiji, Decree No. 37 of 1989).
[h] Criminal Procedure Decree 2009 (Fiji, Decree No. 43 of 2009).
[i] Extradition Act 2003 (Fiji, No. 4 of 2003).
[j] Mutual Assistance in Criminal Matters Act 1997 (Fiji, No. 28 of 1997).
[k] Criminal Procedure Code (Laws of the Gilbert Islands Revised Ediditon 1977, Chapter 17).
[l] Extradition Act 2003 (Kiribati, No. 7 of 2003).
[m] Mutual Assistance in Criminal Matters Act 2003 (Kiribati, No. 6 of 2003).
[n] Cybercrime Act 2015 (Nauru, No. 14 of 2015) (n 83).
[o] Extradition of Fugitive Offenders Act 1973 (Nauru, No. 5 of 1973).
[p] Mutual Assistance in Criminal Matters Act 2004 (Nauru, Act No. 16 of 2004).
[q] Search Act 1977 (Papua New Guinea, Chapter 341).
[r] National Intelligence Organization Act 1984 (Papua New Guinea, Chapter 405).
[s] Evidence Act 1975 (Papua New Guinea, Chapter 48).
[t] Protection of Private Communications Act 1973 (Papua New Guinea, Chapter 272) (n 85).
[u] Extradition Act 2005 (Papua New Guinea, No. 21 of 2005).
[v] Mutual Assistance in Criminal Matters Act 2005 (Papua New Guinea, No. 22 of 2005).
[w] Criminal Procedure Act 1972 (Samoa, No. 14, 1972).
[x] Police Powers Act 2007 (Samoa, No. 27, 2007).
[y] Extradition Act 1974 (Samoa, No. 12, 1974).
[z] Mutual Assistance in Criminal Matter Act 2007 (Samoa, No. 3, 2007).
[aa] Criminal Procedure Code (Solomon Islands, Chapter 7, Revised Edition 1996) .
[ab] Extradition Act 2010 (Solomon Islands, No. 3 of 2010).
[ac] Mutual Assistance in Criminal Matters Act 2002 (Solomon Islands, No. 4 of 2002).
[ad] Computer Crimes Act 2003 (Tonga, Act 14 of 2003) (n 58).
[ae] Extradition Act (Tonga, Acts 19 of 1972 and 46 of 1988).
[af] Mutual Assistance in Criminal Matters Act 2000 (Tonga, No.17 of 2000).
[ag] Criminal Procedure Code (Tuvalu, Cap.10.05, 2008 Revised Edition).
[ah] Police Powers and Duties Act 2009 (Tuvalu, No. 12 of 2009).
[ai] Extradition Act 2004 (Tuvalu, Act No. 4 of 2004).
[aj] Mutual Assistance in Criminal Matters Act (Tuvalu, Cap. 7.40, 2008 Revised Edition).
[ak] Criminal Procedure Code (Vanuatu, Chapter 136, 1988 Revised Edition).
[al] Extradition Act (Vanuatu, Chapter 287, 2006 Consolidated Edition).
[am] Mutual Assistance in Criminal Matters Act (Vanuatu, No. 14 of 2002).

Fiji has one of the most developed economies, and is a leader in ICT development in the Pacific.[81] It is quite active in combatting cybercrime, and is the first PIC to establish a specialized police cybercrime unit. However, the police cybercrime unit and the law enforcement authorities of Fiji are facing significant challenges in the fight against cybercrime.[82] One of the primary problems is the lack of detailed legislative articulation of computer offences in the Crimes Act 2009 to enable accurate criminal charges. Several cybercrime-related incidents have been reported, but as police officers, the prosecution and the judiciary lack expertise in cybercrime investigation and adjudication, only a few cases have been brought to the courts.[83] Further, some convictions have problems. For instance, in *State v Smeon Stefanov Minchev* et al.,[84] three Bulgarians travelled to Fiji and placed skimming devices over the card readers of various ATM machines. They were convicted of a computer offence, among others, of 'unauthorized access to restricted data'. Section 343(2) of the Crimes Act 2009 of Fiji states that 'restricted data means data: (a) held in a computer; and (b) to which access is restricted by an access control system associated with a function of the computer'. The definition of 'a computer', however, is not seen in any existing legislation.

In 2016, Papua New Guinea updated new cybercrime legislation with the adoption of the Cybercrime Code Act 2016, which was prepared in cooperation with Australian experts. The Act extensively criminalizes some 25 acts related to the use of electronic systems and devices, and provides for necessary procedural measures and international cooperation mechanisms in cybercrime investigation. A specialized Intelligence Unit and a cybercrime taskforce were established in the Royal Papua New Guinea Police in 2014. Papua New Guinea CERT was set up in 2018. Nevertheless, due to the novelty of the Cybercrime Code Act 2016 and the lack of enforcement capacity, little implementation has been achieved until now. Although there have been reports of many cyber-incidents, no cases have been brought to the courts as yet.[85]

Vanuatu currently does not have specific cybercrime legislation in place. Some forms of cybercrime are stipulated by various statutes, mostly outside of the typical criminal legal framework (e.g., the Telecommunications Act (Consolidated Edition 2006). A comprehensive cybercrime statute in line with the Budapest Convention is being developed by the General Prosecutors Office and Ministry of Justice of Vanuatu. The national cybercrime policy has been developed, but there is an absence of capacity for combating cybercrime. The country lacks human resources and technical ability in cyber-security and ICT.[86]

The lack of technical equipment necessary for digital forensics and a low level of knowledge held by police officers, prosecutors and judges in the field are among the greatest obstacles for sustainable and effective law enforcement against cybercrime in PICs.

5. Conclusion

The successful diffusion of the Budapest Convention, accompanied by capacity building assistance from the Council of Europe and other donors (mainly Australia and New Zealand), has resulted in a rapidly ongoing reform of national laws related to cybercrime in PICs. A significant number of PICs have expressed a strong desire to accede to the Convention, and align their cybercrime laws with the Convention's provisions. In fact, Tonga has ratified the Convention, while other countries are commencing the procedure for accession to the Convention by reforming their current cybercrime laws. It is evident that the approach of 'legal transplant' is applied to developing their cybercrime legislation. The majority of PICs, in the coming years, are expected to have a sound cybercrime legal framework 'on paper'.

Legal transplantation can be a quick and effective means of reforming and developing national legislation.[87] Nevertheless, the implementation of the 'imported' laws might be limited in practice, especially if the laws were drafted by states with different legal and political traditions, or by ones at a much higher level of development.[88] This would be the case for cybercrime laws in PICs. The transplantation of cybercrime legislation has resulted in the import of a whole body of law or parts of laws. However, it seems that PICs do not consider carefully whether the 'imported' law is practical and whether it is consistent with the existing domestic legislation. All the recently introduced cybercrime legislation by PICs consists of three main parts: criminalization of cybercrime acts, procedural measures, and international cooperation mechanisms in combating cybercrime. While it is important to have these statutory provisions in place to investigate and prosecute cyber-criminals, the capacity to enforce the laws does not exist or is inadequate. Most PICs currently lack resources and expertise, such as a lack of police capacity, including digital forensics, and prosecution capability in the courts.[89] Therefore, notwithstanding that some PICs will have comprehensive cybercrime legislation in the near future, the implementation will be precluded by various challenges that are not going to be resolved in the short term.

Declaration of Competing Interest

None.

[81] Fiji was elected 2nd Vice-Chair of the Executive Committee of the Commonwealth Telecommunications Organization (CTO) in 2016, the 1st Vice-Chair in 2017, and is the current Chair of CTO.

[82] Interview with a senior official of the Organized Crime Unit of the Fiji Police on 15th February 2020.

[83] For example, in FICAC v Viliame Katia (Criminal Case: 1958/2016, Fiji), the accused was convicted of Unauthorized Modification of Data contrary to section 341(1) of the Crimes Act 2009 of Fiji.

[84] Lautoka Cr Case No. 932 of 2017.

[85] Interview with a senior law enforcement official on 15th June 2020.

[86] See Standard Standards Australia, Pacific Islands Cyber Security Standards Cooperation Agenda (Australia, 2020) 47.

[87] See this argument in Helen Xanthaki, 'Legal Transplants in Legal Legislation: Defusing the Trap' (2008) 57 International and Comparative Law Quarterly 659, 659.

[88] This view is supported by e.g., Alan Watson, 'Legal Transplants and Law Reform' (1976) 92(Jan) Law Quarterly Review 79, 79.

[89] See more discussion in Standards Australia, Pacific Islands Cyber Security Standards Cooperation Agenda (n 149).