Critically Examine the Readiness of Tonga's Legislative Framework for e-Crimes

PAULA RAYMOND LUTUI

A dissertation submitted to
Auckland University of Technology
in partial fulfilment of the requirements for the degree of
Master of Laws (LLM)

2021
Law School

Declaration

"I hereby declare that this submission is my own work and that, to the best of my knowledge and belief, it contains no material previously published or written by another person (except where explicitly defined in the acknowledgements), nor material which to a substantial extent has been submitted for the award of any other degree or diploma of a university or other institution of higher learning."

…..... 27/12/2021

Signature Date

Acknowledgements

In light of this now completed work, I would like to firstly acknowledge and give thanks to our Heavenly Father who has been an amazing rock to lean on and great source of comfort and motivation throughout this journey. It has been extremely trying during these uncertain times, but it has also been a time of great reflection. It was then that I found Psalms 94:18 which reads, “when I said, “my foot is slipping,” your unfailing love, Lord, supported me” and the good Lord has guided me until the very end and for that, I thank Him. I would also like to thank my family, for your presence, patience, and prayers that has allowed me to take the time needed to bring this thesis together. This acknowledgement would not be complete without giving thanks to my supervisors, Professor Kris Gledhill and Associate Professor Dr. Guy C. Charlton. You have been a great source of help in completing this thesis. Thank you for your patience and motivation that has led this thesis to a successful completion.

Abstract

Governments and private organisations are heavily reliant on Information and Communication Technologies (ICT) to conduct daily businesses. We are living in a connected digital age, and the rapid growths and advancements in the ICT arena brings new opportunities. Criminals are welcoming these opportunities as well and exploiting it to conduct their illegal activities for their own personal gains. Criminal activities or crimes committed in cyberspace is often referred to as cybercrime or computer related crimes. At the time of conducting this study, a universal definition for the term "cybercrime" does not currently exist.

However, the most accepted definition is, "a criminal activity that either target or uses a computer or a computer system as a tool". Cybercriminals are organised, they possess high technical skills and use advanced methods. Their motivation behind their actions are usually personal, political, or monetary benefits, and result in serious economic impacts. In a recent study on cybercrime conducted by the Vienna office of the United Nations Office on Drugs and Crime revealed that 62% of global Internet users are from developing countries and, most of them are committed by young people. Cybercrimes implies significant procedural and jurisdictional issues.

For that reason, this study believes that it is vital to identify the weaknesses of cybercrime related legislations of the countries in the South Pacific. Therefore, Tonga, Fiji, Samoa, and Kiribati have been chosen as case studies to represent developing countries in the South Pacific. Their legislation frameworks will be analysed and compared; the outcome of this study will be referred to throughout this study as "TKFS". With New Zealand being a well-developed country in the South Pacific, its cybercrime related legislations will be analysed, and the results will then be compared with the TKFS. The outcome of this analysis and comparison will be used to answer the research questions, draw a conclusion and propose recommendations.

Since this study will involve analysing and comparing the legislative frameworks of five countries, Doctrinal Research Methodology (DRM) is found to be the most suitable research methodology to guide this study. Doctrinal research is defined as the research that asks what the law is in a specific area. Therefore, the

researcher will need to collect and analyse data from any relevant legislation within the concerned legal framework. The implication is that for cybercrime – a new, high-tech, sophisticated way of committing a crime. To effectively protect, prevent, and mitigate these implicated types of criminal offences, it requires a comprehensive cybercrime specific legislative framework to criminalise and prosecute cybercrimes. The completed study will contribute to the body of knowledge in the cybercrime related legislative framework. The professional significance is that the recommendations will help cybersecurity personnel in the field, and legislators in developing countries around the world.

TABLE OF CONTENTS

Chapter 6 Comparison and Conclusion

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

CI	Critical Infrastructure
CIA	Confidentiality, Integrity, and Availability
CoC	Convention on Cybercrime
CoE	Council of Europe
CPPA	Child Pornography Prevention Act
DDoS	Distributed Denial of Service
DRM	Doctrinal Research Method
ECOWAS	Economic Community of West African States
EGRIP	E-Government for Regional Integration Project
ENISA	European Union Agency for Cybersecurity
ERCoC	Explanatory Report of the Convention on Cybercrime
ETS 185	European Treaty Series number 185
FBI	Federal Bureau of Investigation
GPO	Government Publishing Office
HIPCAR	Harmonization of ICT Policies, Legislation and Regulatory Procedures in the Caribbean
ICB4PAC	Capacity Building and ICT Policy, Regulatory and Legislative Frameworks Support for Pacific Island Countries
ICT	Information and Communication Technology
IoT	Internet of Things
ISP	Internet Service Provider
ITU	International Telecommunication Union
MEIDECC	Ministry of Meteorology, Energy, Information, Disaster Management, Environment, Climate Change and Communications
NIIPA	National Information Infrastructure Protection Act
NIST	National Institute of Standards and Technology
NZ	New Zealand

OECS	Organisation of Eastern Caribbean States
PKI	Public Key Infrastructure
PNG	Papua New Guinea
TKFS	Tonga, Kiribati, Fiji, Samoa
UK	United Kingdom

Chapter 1

Introduction

1.0 INTRODUCTION

Information and Communication Technologies has become very much part of our everyday lives such as ubiquitous devices like smart devices. These devices are categorised as mobility, context awareness, and diversity on data sources (Mylonas et al., 2012, p. 250). As a result, these devices play a vital role in our lives today however, with the advancement in hardware and software, these devices store and carry a plethora of personal and private information which attracts the attention of cybercriminals (Joshi & Pilli, 2016, p. 167). The world is digitally connected and cybercrime activities over Information Communication Technologies are increasing as well (Goel, Tyagi & Agarwal, 2012, p. 297).

The nature of cybercrime identified in the literature can be classified into four categories. First, the cybercrime legislation that identifies and defines the set of laws that criminalise and prosecute criminal activities committed in cyber-space. Second, the academic philosophies that pursue understanding of the occurrence through computer science, information and data management, socio-legal and criminological disciplines. Third, expertise in the field the attempts to understand cybercrimes in order to offer clarifications that can inform solutions. Fourth, normal everyday user's that demonstrate common understanding of the crime (Zavrsnik, 2008, p. 2).

Although there is a universal understanding and presumably common definition of the term "cybercrime" yet still ambiguous. There are known factors that contribute to the ambiguity of the term "cybercrime". For instance, the variety and the range of the offences as several can be connected back to traditional crime. Appropriately, the necessary resolution must be identified whether an amendment of the existing legislation or a new legislation that is required (Hargreaves & Prince, 2013, p. 4). This study understands that cybercrime is a new type of crime and, government, law enforcement agencies, businesses and academics have been working come to an agreement on a global definition for the term.

Nevertheless, for the purpose of this study, the following terms “cybercrime, computer crime, computer-related crime, electronic crime” may be used interchangeably however carries the same meaning. As technology advances further, these commonly used terms were further developed in terms of its digital concepts. For instance, technologically enabled crime (Gordon, 1995, p. 398), cyber-enabled crime (Roycroft, 2016, p. 66), network crime (Akhgar et al., 2016, p. 301), hi-tech crime (Alkaabi et al., 2011, p. 1). However, cybercrime is the commonly used term employed to explain actions where a computer or computer system is a tool, or a target, or a place of criminal activity (Newman, 2009, p. 551).

1.1 CATEGORIES OF CYBERCRIME

Hargreaves and Prince (2013, p. 3) believed that there are two fundamental categories of cybercrime: computer enabled and computer dependent crime. The Royal Canadian Mounted Police divided cybercrime into two categories; traditional crimes, or crimes committed with the aid of a computer or computer system (technology-as-instrument) such as online fraud, identity theft, money laundering, drug and human trafficking, child pornography or cyber bullying. Secondly, technology-as-target where other information technologies or computers are the target of criminal offences such as crimes that involves unauthorised use of computers, or hacking, and computer viruses, and damages to data (RCMP, 2014, p. 3). According to the Government of Canada (2010, p. 5), cybercrimes are more complicated when organised criminals recruit skilled cyber criminals to committing traditional criminal activities for them such as identity theft, money laundering, and so on.

Traditional crimes are the type of crimes exist in the real world however, their horizon and reach have been expanded due to today’s technological advancement. Information and Communication Technologies provided more opportunities for traditional crimes such as stalking, fraud, phreaking. Traditional “classic” crimes such as money laundering, and hacking. The difference is, the risks are lower (Jahankhani, Al-Nemrat & Hosseinian-Far, 2014, p. 150). Moreover, the Council of Europe Convention on Cybercrime outlined offences against the confidentiality, integrity and availability (CIA) of information and computer system

for instance, fraud and forgery. In addition, using of remote computers or electronic devices to launch an attack such as distributed denial of service (DDoS), infringements of copyright and related rights, viruses and large-scale fraud, spam and scams (Alkaabi et al., 2011, p. 3).

Terrorists have also found new opportunities in cyberspace that is effective with abusive abilities. For instance, DDoS where the attacker uses a number of remote computers, also referred to as "zombie" computers to launch the attack (Platt, 2012, p. 157). According to Rao et al. (2020, p. 2), there is a rapid growth in the number of DDoS attacks on critical infrastructure (CI) networks. This technique works by inserting a malicious code (Trojan horse) and infect a large number of devices such as computers. In order to gain unauthorised access and exploit these computers, the attack can send the malicious software attached to an e-mail, installed in a free game, or other media (Aborujilah et al., 2020, p. 790).

For instance, in 2007 a series of DDoS attacks were launched targeting several services in the Republic of Estonia. This includes crashing several banks' websites and newspapers' websites. Compromising the government communication systems, and the websites for Estonia's parliament and various government ministries (Shackelford, 2009, p. 1). According to Traynor (2007), the attacks were launched from thousands of zombie computers around the world.

1.2 CHALLENGES IN DEVELOPING A CYBER LAW

It is evident in the literature that the main challenges in developing cyber law is that the crimes together with the techniques and methods utilised to commit the crimes changes rapidly as technologies change (Shakeel, Tanha & Broujerdi, 2010, p. 149). For instance, cyberization is the new term used to describe diversity in the fields including embedded computing, ubiquitous and pervasive computing, green computing and communications, Internet of Things (IoT), cyber-physical, social networks, wearable technologies, smart city, cyber security, cloud computing, big data, artificial intelligence, and robot technology (Ma, 2016, p. 85).

Crimes committed in the above-mentioned environments, most are considered as traditional crimes that is, crimes reliant computers or other form of electronic devices to conduct and increase their boundaries (Payne et al., 2020, p.

1). Such as computer software piracy, and credit card forgery and fraud, online scams, drug trafficking, trafficking corporate secrets, identity theft, and money laundering (Choo & Smith, 2008, p. 39). Usually, the common law can be used to prosecute crimes such as hacking particularly if unauthorised access involves. Nevertheless, with technology advancement, some crimes evolve accordingly, neither common law nor criminal law can be applied. For instance, if a legitimate user of an information system gained access to another information system that he/she not supposed to without knowing as a result of a man-in-the-middle attack or being re-directed by a hacker, neither the common law nor the criminal law can be applied to deal with (Shakeel et al., 2010, p. 149).

According to KPMG International, a large amount of the public still not aware that there is a lack of laws or acts to protect personal data (Forensic, 2004, p. 378). The lack of expertise among the personnel to develop and implement legal measures such as legislations, regulations to rule, manage, and control cybercrime in the Economic Community of West African States (ECOWAS) and its member states (Jerome Orji, 2019, p. 14). This issue has pushed countries to rely heavily on technical solutions developed by various international organisations.

Cloud technologies such as cloud storage on the other hand, presented law enforcement agencies and digital forensic practitioners with issues such as accessing and collecting data (Quick & Choo, 2013, p. 266). Cloud robotic is a product of ICT technology advancements. Regardless of all the benefits and advantages it may bring, it also presents issues and challenges. Fosch-Villaronga and Millard (2019, p. 86) cloud robotics contributes substantial amount of data including personal data to big data issue and raises the question of how to protect personal data. Nonetheless, the present legal framework for cloud robotics contains general concepts, definitions, and regulations. Yet it does not specify how it can be applied to new technologies.

Privacy and personal online safety are a major issue highlighted in a campaign to create awareness with regards to cyberbullying among Internet users in Qatar (Foody et al., 2017, p. 48). As our society becomes more and more dependent on electronic devices and web-based services, criminals have found a way to take advantage of ICT's advancement. Making available the right but

rigorous legislative framework is a vital part of any government's response to cybercrime (Barclay, 2017, p. 77).

1.3 RESEARCH GOAL & QUESTIONS

The goal of this study is to determine whether the legislative framework in the Kingdom of Tonga is ready to criminalise and prosecute crimes committed in cyberspace. In order to achieve the primary goal of this study, four neighbouring countries of Tonga were selected, that is Kiribati, Samoa, and Fiji. The reasoning behind the selection of these three south pacific countries is that they have some similarities with Tonga in culture and tradition. In addition, these countries are still developing in terms of economy, politic, education, Information & Communication Technologies (ICT), Critical Infrastructures (CI). The outcome will then be compared with the cybercrime related legislations of a well-developed country in the south pacific such as New Zealand.

Seeing that this study is designed to review the legislative frameworks of five countries, Doctrinal Research Methodology (DRM) is the chosen methodology to guide this study. Doctrinal research is regarded as the study of legal texts. Also, can be employed as a standard for argument, description, and interpretation that provide insights which formulate clear circumstances when comparing to other legal systems (Chynoweth, 2008, p. 29). Accordingly, the researcher proposes and recommends the required changes - law reform.

At the end, this study will answer the question: *"What can be done to ensure the readiness of Tonga's legislative framework to combat cybercrime?"*

In order to further understand and maximise the outcome of this study - the design, data analysis, findings; three sub-questions were also developed to help brings out the best solution that meets the objective of this study.

SubQ 1 – What are the weaknesses of the current cybercrime legislation in Tonga?

SubQ 2 – What are the advantages of having a cyber-specific legislation?

SubQ 3 – Is the legal system in Tonga ready for cybercrime?

These questions will be answered at the end of this study along with relevant recommendations will be provided. Such information can be vital to law makers in

any developing countries in the south pacific to criminalise and prosecute criminals of cyberspace.

1.4 THESIS STRUCTURE

This thesis is divided into six main chapters. The first chapter is intended to provide an overview of this study and highlight the purpose of the study. Chapter two provides a theoretical review of Tonga's current cybercrime legislation. This review will mainly focus around the part 2 of the Tonga *Computer Crimes Act 2016* which is the offences that criminalise by the *Computer Crimes Act*. Furthermore, the reader needs to aware of the style of writing employed by this study. This study will take relevant literature found in the body of knowledge and use it in the analysis. The analysis will be accompanied by critique, and followed by comparisons and discussions.

Chapter three outlines the design of the study and describe the research methodology chosen to guide the study. Chapter three will also discuss the main research question and the sub-questions derived from the literature which will be answered at the conclusion of this study. Chapter four is designed to analyse the cybercrime related legislations of Kiribati, Fiji, and Samoa. The outcome will then be compared with the outcome of the analysis conducted in chapter two.

Chapter five on the other hand is designed to provide an analysis of New Zealand's cybercrime related legislation. Chapter six will take the outcome of the comparison conducted in chapter four. This will be used to compare with the New Zealand's cybercrime related legislation. Chapter six is also designed to draw the conclusion for the study, and provide the answers for the research questions. Also, offer recommendations for law makers, which can play a vital role in fighting cybercrime.

Chapter 2

The Cybercrime Legislation in Tonga

2.0 INTRODUCTION

The previous chapter (chapter 1) provides an overview of various methodologies employed in the field of research. Chapter 1 also showed doctrinal research as the chosen research methodology to guide this study. It also provides a detailed explanation of the research design for the study including the main research question and sub-questions. As mentioned in earlier chapters, this study is designed to evaluate the legal readiness and capacity of developing countries in the South Pacific to criminalise various types of cyber-related activities.

Analysing the Tonga's current legal framework to determine its current state, and comparing it to those Pacific countries such as PNG, Kiribati, Fiji and Samoa for context will reveal how the framework works in the Pacific countries. Analysing New Zealand's legal framework, as a developed country to inform what changes could be made to improve Tonga's current legal framework.

2.1 THE DEVELOPMENT OF THE COMPUTER CRIMES ACT

The legislation to criminalise cybercrime in Tonga is the Computer Crimes Act, and it sets the structure for cybercrime legislation in Tonga. The *Tonga Computer Crimes Act 2003* is the first legislation to criminalise computer misuse in Tonga, particularly crimes involving the use of Information and Communication Technologies. The *Tonga Computer Crimes Act 2003* comprises of three parts - part I - Preliminary, part II - Offences, and part III - Procedural Powers.

Part I of the Act deals with initial information including clarifying and defining technical terms such as "computer", "computer data", "computer data storage medium", "computer system", "hinder", "seize", "service provider", and "traffic data". Part II of the Act is concerned with defining offences that criminalise by the Act, and Part III clarifies and explains procedural powers provided by the 2003 Act. As explain in chapter 1, the style of writing employed, the analysis will be accompanied by a critique, and followed by comparisons and discussions.

According to the former Solicitor General, Kefu (2011, p. 1), the Computer Crimes Act was developed based on the Commonwealth Model Law. Nonetheless, there is also the Cyber Legislation: Model Law for the South Pacific.

Part II – Offences, sections 4 to 8. Section 4 of the Act is concerned with "Illegal Access". Section 4(1)(2)(3)(4) were from section 7(1)(2)(3)(4) of the Model Law for the South Pacific. Section 5 of the was also taken from the section 8 of the Model Law for the South Pacific. Section 6 of the Tonga Computer Crimes Act is new in the 2016 revision, and was taken from section 7(1) of the Commonwealth Model Law, and also section 9 of the Model Law for the South Pacific (Scott, 2007, p. 107-109).

Section 7 of the Tonga Computer Crimes Act 2016 revision was taken from section 10 of the Model Law for the South Pacific. Section 8(1) and (2) of the Tonga Computer Crimes Act 2016 revision on Illegal devices was taken from section 11 of the Model Law for the South Pacific (Scott, 2007, p. 109). There are other sections in both the Commonwealth Model Law and the Model Law for the South Pacific, that the law makers in Tonga did not consider including in the Tonga Computer Crimes Act. Such as the child pornography from the Commonwealth Model Law.

Part II – defining 5 provisions on "offences" that criminalises cyber wrongdoings. Such as Illegal access, a person gained access to a computer system without lawful excuse, aiming to commit an offence. Section 5 is concerned with criminalising Interfering with data. This provision is designed to criminalise someone who wilfully destroys data, renders data useless, or interferes with lawful use of data, and so on. Section 6 concerns with someone who unlawfully interfere with computer system. This provision is to criminalise a person who wilfully interferes with the functioning of a computer system.

Section 7 was designed to penalise the intercepting data illegally such as intercepting data that are transmitting to and from within a computer system. Final section of Part II is concerned with penalising Illegal devices that a person may use without any lawful excuse to imports, exports, distributes or makes available a computer password, access code or similar data. The Tonga Computer Crimes Act

establishes the structure for the cybercrime legislation in Tonga. The Electronic Crimes: Knowledge-based Report stated that Tonga has a comprehensive approach. As a result, the format, definitions, and explanations are taken directly from both the Commonwealth Model Law and the Cyber Legislation: Model Law for the South Pacific. The Tonga Computer Crimes Act 2003 has been revised in 2016.

2.2 CRIMINAL BEHAVIOR UNDER THE ACT

There are legal statutes in Tonga to criminalise computer and computer related misuse such as the Criminal Offences Act, the Copyright Act, the Communication Act, and the Computer Crimes Act. The *Tonga Computer Crimes Act 2016* revision is the principal legal tool to fight cybercrime.

2.2.1 Illegal Access

Section 4 of the *Tonga Computer Crimes Act 2016* is the provision designed to criminalise access offences. Section 4(1) explained the purpose of the section which is the security of a protected computer and its program and data. Section 4(1) sub-paragraphs (a, b, c, d) outlined the types of program and data that is used directly in connection with or necessary for (a) the security, defence or international relations of the Kingdom. (b) the existence or identity of a confidential source of information relating to the enforcement of a criminal law. (c) the provision of services directly related to communications infrastructure, banking and financial services, public utilities, public transportation or public key infrastructure. Or (d) the protection of public safety including systems related to essential emergency services.

There are technical terms which are the key elements of this provision such as “protected computer”, “computer”, “computer data”, “computer system”, and “public key infrastructure”.

1) Protected computer is defined as:

the term ‘‘protected computer’’ means a computer -

(A) *exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct*

constituting the offense affects that use by or for the financial institution or the Government; or

(B) *which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States* (GPO, 2010, p. 298).

The Tonga Computer Crimes Act uses the term "protected computer" in Part II section 4(1) of the Act however, does not provide a definition for it. The definition provided in this chapter was taken directly from the "Title 18 – Crimes and Criminal Procedure" a publication published by the U.S. Government Publishing Office (GPO). In the light of this definition, the term "protected computer" refers to computers used exclusively in financial institutions and the Government of Tonga.

2) Computer is defined as:

an electronic, magnetic, optical, electrochemical, or other data processing device, or a group of such interconnected or related devices, performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device or group of such interconnected or related devices, but does not include —

a) an automated typewriter or typesetter;
b) a portable hand-held calculator; or
c) a similar device which is non-programmable or which does not contain any data storage facility;

The former attorney general of Tonga claims that the Tonga Computer Crimes Act was developed based on the Commonwealth Model Law. Nonetheless, the model law does not provide a definition for the term "Computer". However, this definition is very similar to the definition provided by the Computer Crime and Intellectual Property section of the Cybercrime Laws of the United States (Rees, 2006, pp.12). The definition provided in the Tonga Computer Crimes Act was taken directly from Model Law for the South Pacific. The definition is in two folds, the definition of the term "computer" and the second part outlines what is not.

3) Computer data is defined as:

any representation of facts, information or concepts in a form suitable for processing in a computer system, including a programme suitable to cause a computer system to perform a function.

This definition was taken from the Computer and Computer Related Crime, the Commonwealth model law. This definition is identical to the one used by the Cyber Legislation: A Model Law for the South Pacific. This definition is two-fold, first part is concerned with the data/information and second part, focuses on the programmes that are used to capture and process the data in a computer system.

4) Computer system is defined as:

a device or a group of inter-connected or related devices, including the Internet, one or more of which, pursuant to a programme, performs automatic processing of data or any other function.

Similar to the definition provided for the term "computer data", the definition was taken from both the Computer and Computer Related Crime, the Commonwealth model law. Not only that but also the Cyber Legislation: A Model Law for the South Pacific definition.

5) Public Key Infrastructure (PKI) is defined as:

a system of policies, procedures, people, hardware, software and services that support the use of public cryptography to obtain secure communication (Albarqi et al., 2015, p. 32).

According to the National Institute of Standards and Technology (NIST), PKI defines technologies involved and how the PKI systems provide security (Kuhn, Hu, Polk & Chang, 2001, p. 5).

The aim of PKI is to increase the number of e-services of Government and Private entities to empower the e-Government Transformation as PKI provides:

- Electronic transactions protection against identity fraud
- Data integrity, data confidentiality, strong authentication, and non-repudiation

- Trust, confidence and easiness to use online services for citizens and residents (RSA Data Security, 1999, p. 2).

Same as the "Protected Computer" term, the Tonga Computer Crimes Act did not provide any definition for it. Therefore, the definitions and explanations given were obtained from reputable sources such as NIST, RSA Data Security, and ITU.

2.2.2 Cyber-Enabled Crimes

Tonry (2014, p.9) reported a long-term decrease in the occurrences of traditional crimes yet, cybercrime rate continues to climb. According to the New Zealand Police, Cyber-enabled crimes are traditional crimes that utilised Information Communication Technologies (ICT) or the Internet to expand its boundaries and scale (New Zealand Police, 2020). The NZ Police also gave a list of Cyber-Enabled Crimes for instance online scams, threats to life or public safety, and possessing or distributing objectionable material such as child pornography.

2.2.2.1 Computer Enabled Online Scams

There are various known types of online scams including romance scams, cold calling scams, business email compromise, employment or work-at-home scams, and also the investment opportunity scams. Cyber enabled is very dangerous due to its pervasive nature and intelligence. As a result, it is vital to study potential risks, threats, and technologies in order to develop effective approach and control (Ma et al., 2016, p. 7).

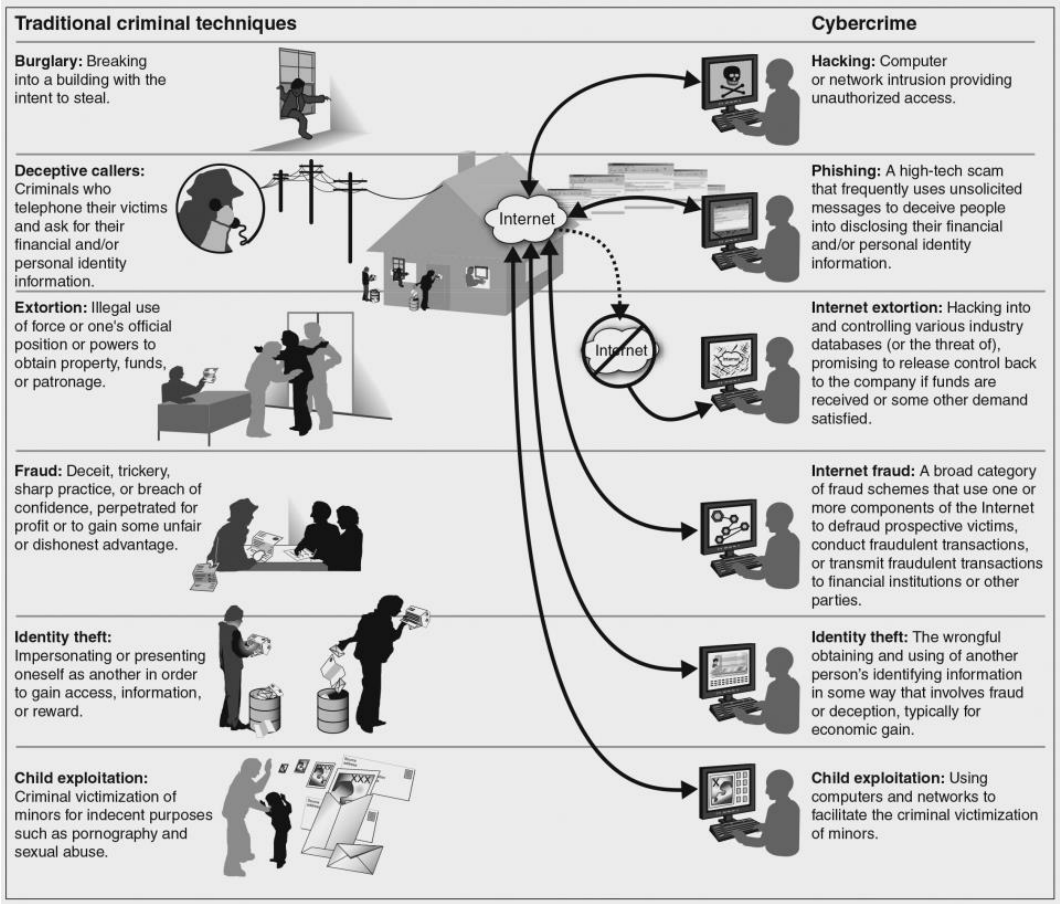

Figure 2.1: Traditional crime and Cybercrime (Thompson & Smith, 2007, p. 6).

The Tonga Computer Crimes Act does not have any provision to criminalise online scams. As mentioned earlier in section 2.1, the former Solicitor General of the Kingdom of Tonga explained that the Computer Crimes Act was developed based on the Commonwealth Model Law. However, it is evident that most of the Computer Crimes Act is identical with the sections, sub-sections of the Cyber Legislation: Model Law for the South Pacific. Nonetheless, the two model laws also have no provisions to deal with computer enabled online scams. Therefore, the Tonga Criminal Offence Act was looked at and examined to see if it has any provision to criminalise scams, frauds and forgeries. Figure 2.1 illustrated an example some of the crimes can be committed utilising traditional techniques and cybercrimes.

Section 154 of the Tonga Criminal Offence Act is the provision to criminalise "Robbery". This deals with the taking of anything capable of being stolen by using violence or threats of injury to the owner. Section 156 deals with

Extortion meaning, every person who gain anything from anyone accuses or threatens to accuse of a criminal offence. Section 158 deals with embezzlement and that is, fraudulently converting anything received on behalf of his/her master or employer for his/her own use or benefit. Sections 159 to 169 deal with various types falsifications and frauds.

For instance, falsification of accounts, fraudulent conversion of property, obtaining by false pretences, obtaining credit by false pretences, and false pretences as to documents. Lastly, section 170 deals with forgery meaning, making any false document with intent to defraud or deceive anybody. All the sections of the Tonga Criminal Offence Act mentioned in this section can be applied directly to criminalise cyber enabled online scams, fraudulent acts, and robbery. Not only that but there is no provision in the offences section of the Tonga Computer Crimes Act either.

2.2.2.2 Child-Pornography Related Offences

The growth and advancement of ICT technologies and Internet have played a role in the increase of child pornography issues. That is in terms of producing, collecting, and distributing of child pornography materials (Catudal, 1999, p. 82; Akdeniz, 2016, p. 1). In the United States of America, Congress introduced the *Child Pornography Prevention Act (CPPA) 1996* as their response to the advancement on ICT technologies and the growth Internet. In addition to the CPPA 1996, a database of known to be real children images was developed by the Federal Bureau of Investigation (FBI) (Chawki et al., 2015, p. 82).

However, in *Ashcroft vs. Free Speech Coalition* 2002, the U.S. Supreme Court found the CCPA to be very broad, ambiguous, unconstitutional. Moreover, the CPPA violates the free-speech protection in the first amendment of the U.S. constitution (Mota, 2002, p. 86). This application requirements will be varied depending from country to country as a result, model laws were developed to combat cybercrimes.

Section 10 of the Commonwealth Model Law on Computer and Computer Related Crime is the provision to criminalise child pornography related offences. Types of related offences are explained in sub-sections (1) it refers to (a) *"a person who, intentionally, does any of the following acts".* (b) *"produces child*

pornography for the purpose of its publication through a computer system" or (c) *"possesses child pornography in a computer system or on a computer data storage medium".*

Section (3) expands the definition and types of child pornography further to include provisions for material that visually depicts (a) *"a minor engaged in sexually explicit conduct"* (b) *"a person who appears to be a minor engaged in sexually explicit conduct"* or (c) *"realistic images representing a minor engaged in sexually explicit conduct".*

Section (3) uses the word "minor" in sub-sections (a), (b), and (c). As a result, this part of the section (a) defines the word "minor" as *"a person under the age of [x] years".* The word "publish" includes: (a) *"distribute, transmit, disseminate, circulate, deliver, exhibit, lend for gain, exchange, barter, sell or offer for sale, let on hire or offer to let on hire, offer in any other way, or make available in any way"* (b) *"have in possession or custody, or under control, for the purpose of doing an act referred to in paragraph (a)"* or (c) *"print, photograph, copy or make in any other manner (whether of the same or of a different kind or nature) for the purpose of doing an act referred to in paragraph (a)".*

The Cyber Legislation: Model Law for the South Pacific does not have any provision to criminalise "child pornography" as does the Tonga Computer Crimes Act. Nevertheless, Tonga has a specific Law on pornography known as the Pornography Control Act, and currently is the 2016 Revised Edition. Sections 4 and 5 of the Act defines the offences and what is included.

Section 4 criminalises the ***"Production of pornographic material prohibited".*** The definition and fine provided by this provision is *"Any person who deals in or carries out any activity pertaining to the production of pornographic material or is otherwise concerned in the production of pornographic material commits an offence and shall be liable upon conviction to a fine not exceeding $10,000 or 3 years imprisonment or both."*

Section 5 criminalises the ***"Sale or hire of pornographic material prohibited"*** and the definition provided is *"Any person who sells or hires out or knowingly allows any other person to sell or hire out pornographic material commits an offence."* These two provisions criminalise production, sale, and hire

of pornographic materials. This does not include child pornography, copy, transmit, transfer, exchange, barter, circulate, have in possession, etc. The main issue is that, the provisions provided by the Tonga Pornography Control Act may not be enough to prosecute computer/digital related pornography.

2.2.2.3 Copyright and Related Rights Infringement Offences

Both the Commonwealth Secretariat Model Law on Computer and Computer Related Crime, and the Cyber Legislation: A Model Law for the South Pacific do not have a provision to prosecute copyright and related rights infringement offences. Therefore, it is no surprise that the Tonga Computer Crimes Act also has no provision for copyright and related rights infringement offences. Nonetheless, Tonga has a specific Act for copyright known as the Tonga Copyright Act 2002.

In order to regulate the computer related copyright infringements, the Copyright Act 2002 provides the following clauses. Part 1 is Copyright and section 3 outlines the Works protected under the copyright provisions. Sub-sections (1)(a), *"Literary and artistic works are original intellectual creations including - ... computer programs ..."*. Section 6(1)(e) on Economic rights *"... a computer program, a database or a musical work in the form of notation, irrespective of the ownership of the original or copy concerned".*

Also, section 8(2)(d) with regards to - Private reproduction for personal purposes *"of a computer program, except as provided in section 14".* However, section 14 particularly focusses on computer related infringements but mainly dealing with - *"Reproduction and adaptation of computer programs".* It is clear that the Tonga Copyright Act 2002 is primarily concerned with the protection of a computer program.

In 2017, Tonga joined the Budapest Convention on Cybercrime, this makes Tonga the first country from the Pacific Island region to be conceded to the Budapest Convention (Radio & TV Tonga, 2017). *Article 10* of the Budapest Convention on Cybercrime is about *Offences related to infringements of copyright and related rights.* The Budapest Convention pointed out that such legislation is required to prosecute violation of the copyright Act. For instance, any violation of trade-related aspects of Intellectual Property Rights, Literary and Artistic Works, by means of a computer system. Section (10)(2) concerns with the Protection of

Performers, Producers of Phonograms and Broadcasting Organisations (Clough, 2014, p. 7).

Looking back over the past two decades of Tonga Law Reports, a direct case on copyright violations cannot be found. However, the first Copyright Act was the 1988 Edition, Chapter 121. Section 2 describes that the primary objective of the Act is to protect the moral and economic interests of authors relating to their works (Copyright Act 1988). This is done to acknowledge author's rights and regulate access to their work. Field of application defined in section 3. Sub-sections (1)(a) & (b) are the provisions to protect authors residence of Tonga or works first published in Tonga.

Section 3 and sub-sections (2)(a) & (b) are the provisions to protect unpublished works and works first published in a foreign country provided they offer similar protection to residents of Tonga for their unpublished works and works first published in Tonga. Not only that but the works to be protected in Tonga according with the International conventions. In the Copyright Act 2002, sections are more organised and divided into four major parts. Section 14 is the provision to protect "*reproduction and adaptation of computer programs"* is a new addition to the Part 1 of the Copyright Act 2002.

2.3 DISCUSSION

Ministry of Information and Communications. (2013, p. 2) in Tonga conducted a workshop sponsored by the ITU and the European Union. The purpose is to strengthen the capacities of local authorities, so they can deal with cybercrime, identify key issues, and raise awareness. In this workshop, the main cyber-related crimes in Tonga and neighbouring countries in the Pacific were online scams, lottery scams, sphere phishing, and cyber bullying.

The Internet and the advancement in ICT technologies make it all possible to collect millions of e-mail addresses from personal computers and web-servers around the world for their scams (Newman, 2009, p. 559). However, in terms of bullying, the relationship between suicide and bullying in the literature is quite clear. According to Hinduja and Patchin (2010, p. 207), young people who were bullied are at risk of having either suicidal thoughts, attempts, or completed

suicides. The Tonga *Computer Crimes Act* consists of three main parts. Part 1 comprises of the title, interpretation, and jurisdiction. Part 2 covers all the offences considered a violation of the Act. Part 3 comprises all the procedural powers of the Act. This carries the structure similar to what is employed by legislators around the globe.

The Act criminalises five offences; illegal access, interfering with data, interfering with computer system, illegal interception of data, and illegal devices. The illegal access refers to unlawful access, unauthorised access, or access without lawful excuse. The illegal access provision in the *Computer Crimes Act* focusses on illegal access to protected computers and computer system. It is evident that the provision in section 4 of the *Computer Crimes Act* only applies to protected computers and computer systems.

The provision in section 4 does not include illegal access to any other computer or computer system that is not used in relation to the security, defence, services directly related to communications infrastructure, banking and financial services, public utilities, public transportation, protection of public safety including systems related to essential emergency services in the Kingdom of Tonga. In addition, this provision requires physical contact with a protected computer or computer systems only, however, it does not include illegal remote access.

For instance, *United States v. Morris* where a malicious software was launched to gather usernames and passwords in order to gain access to 600 e-mail accounts collecting personal information, photos, and videos (Kittichaisaree, 2017, p. 271). Nonetheless, it is clear from this case that an amendment is required, sentencing needs to be allocated according to the damages caused by the criminal (Daly, 1993, p. 465).

Section 5 is the provision to criminalise Interfering with data. Part 2 section 6 of the Commonwealth Model Law on Computer and Computer Related Crime has a provision to criminalise interfering with data. It refers to intentionally destroying, rendering data useless, interfering with legitimate use of data, and/or denies access to legitimate users of data (Commonwealth Secretariat, 2017, p. 7). The Model Policy Guidelines & Legislative Text suggests that countries and

governments may choose to deal with the "interfering with data" offence differently.

Some countries may decide not to include the unlawful access provision as they have other solutions available (HIPCAR, 2012, p. 19). In terms of the "interfering with data" offence, it is evident that the Tonga *Computer Crimes Act* aligns with international best practices and guidelines such as the Commonwealth Model Law, the HIPCAR Model Legislative Text, the Cyber Legislation: The Model Law for the South Pacific.

Section 6 is designed to criminalise "interfering with computer system" and prosecute someone who interferes with the normal operation of a computer system or interferes with someone who is a legitimate user of a computer system. According to chapter 2, section 1 article 5 of the *Convention on Cybercrime, Nov, 23, 2001, E.T.S. 185, Budapest, 25* on system interference, each country should have a provision to regulate such an action when committed intentionally and interferes with the normal function of a computer system.

On this provision, the Tonga *Computer Crimes Act* shows evidence that it aligns with international legislations that regulate cybercrimes. Similar to that provided by the *HIPCAR* and the *Commonwealth Model Law*, all provisions follow international best practices. The ITU explained in its 2016 Cybercrime Legislation Resources that the financial damages of an attack on a computer system is often high. However, the legal system may find attacks such as online scams, or remote access triggered attacks such as DDoS more challenging because the attack may be launched from different jurisdiction or jurisdictions (Gercke, 2016, p. 55).

Due to the pervasive nature of mobile smart devices, they transmit both private and non-private data over public and non-public communication networks. The goal is to prevent any type of attacks in order to protect the Confidentiality, Integrity and Availability (CIA) of the data (Rocchetto, Ferrari & Senni, 2019, p. 30). In addition, similar concerns exist with regards to threats against computer systems with illegal interception of data. Despite the significance of the matter, there are still countries with no provisions to criminalise such a criminal act. For instance, the Electronic Government for Regional Integration Project (EGRIP) *Data Protection Bill 2011* does not criminalise illegal interception of data.

Section 7 of the Tonga *Computer Crimes Act* on the other hand is concerned with "illegal interception of data". That is, criminalising intentional, without lawful excuse, use of technical means to intercept data. Whether in storage or in transmission to, from or within the computer or Information Systems. Similar provisions have been provided by both the *Commonwealth* and the *HIPCAR Model Laws* however, they criminalise unlawful interception of data transmitting over non-public networks only. Therefore, they cannot be used to prosecute illegal interception of data transmitting over the public network. The Tonga *Computer Crimes Act* is different in this matter as it can be used to prosecute illegal interception of data regardless of the transmission media used.

The final provision in the offences section of the Tonga *Computer Crimes Act* is to criminalise "illegal devices". That is, prosecuting anybody who unlawfully produces and/or distributes a device or a tool, including a computer program that is designed to use to commit a crime. Furthermore, distribute or make available password or access code that allows access to a computer system. Similar to the *HIPCAR* and the *Commonwealth Model Law,* all follows the international best practices in terms of criminalising "illegal devices".

According to the Commonwealth Secretariat (2002, p. 5), the wordings of the provision is going to be difficult to distinguish the use of import, export, produce, sell, and so on for lawful purposes. On the contrary, cyber security experts use devices like these to break into computer systems for testing purposes. These tests are called penetration testing, also known as pen testing or ethical hacking. Pen test is an authorised attack performed to evaluate the security status of a computer system.

The Budapest Convention on Cybercrime 2001 excludes this provision in cases where the application of such device and software is for the purpose of authorised testing on computer systems. Nonetheless, it is evident that the Tonga *Computer Crimes Act* is not sufficient to regulate all types of electronic crimes. Tonga needs an electronic transactions law to regulate the use of emails or any other writings in electronic form which will eliminate current uncertainties in this area (Blythe, 2006, p. 2).

2.4 CONCLUSION

This chapter focusses on the evaluating the Cybercrime Legislation in Tonga. It is evident that the Kingdom of Tonga has been trying to align its legislative framework with the International standards and best practices. Tonga has joined the Budapest Convention on Cybercrime and become the first to join from the pacific region. They also developed their Cybercrime legislation based on the Commonwealth Model Law on Computer and Computer Related Crime and the Cyber Legislation: A Model Law for the South Pacific.

It is also evident that there are some differences in the structure of the Act such as, the Commonwealth Model Law on Computer and Computer Related Crime. The Cyber Legislation: A Model Law for the South Pacific does not have that provision however; Tonga has a specific Law on pornography known as the Pornography Control Act. Both of the Model Laws used by Tonga legislature to develop its Computer Crimes Act do not contain any provisions for Copyright and so as the Tonga Computer Crimes Act. Nonetheless, Tonga has a specific Act to criminalise Copyright and Related Rights Infringement Offences known as the Tonga Copyright Act.

Chapter 3

Research Methodology

3.0 INTRODUCTION

The previous chapter (chapter 1) provides an overview of the purposes of the study. This chapter, chapter three offers a description of the methodology employed to guide this study. This chapter is organised into five main sections (3.0 – 3.4) which starts off with an introduction to the chapter. This is followed by section 3.1 which provides a discussion on the philosophy behind research. The fundamental anticipations of research are also discussed and that leads up to a discussion on the methodology used in legal research. This is followed by section 3.2 which discusses the research method employed by this study. Section 3.3 is designed to discuss the data requirements of this study while section 3.2.1 defines how the data is going to be processed and 3.2.2 discusses how the data will be analysed. Finally, section 3.4 concludes the chapter.

3.1 METHODOLGY/RESEARCH METHODS

Research is understood as a process of thinking, critically assessing various stand points of your profession, understanding and articulating guiding principles that administer certain method (Kumar, 1998, p. 1). Since research is understood as a process of thinking, it requires a method. Method is a logical course of action to accomplishing the objective. Methodology on the other hand, is a structure of methods and philosophies for undertaking something such as teaching or conducting research (Collins, 2020, p. 1).

Deb et al. (2019) elaborated that, research implies thorough, precise, unbiased, methodical way of searching for knowledge. This involves clear definition and formulation of research questions, sub-questions, and hypotheses (p. 1). Even though that a methodology may not define or express particular approaches however, it is regarded as a highly intellectual human activity used in the investigation of nature and matter and deals specifically with the manner in which data is collected, analysed and interpreted (Pattron, 2009, p. 1). At the end,

exploring and investigating to identify and determine the best and most favourable solution (Chen, 2014, p. 11).

As a result, a researcher in the legal domain will have to determine on the type of research to be conducted. Chynoweth (2008) suggested that even though theoretical studies has become normal practice now in the legal domain but then again, the type of legal studies is lack in the theoretical literature (p. 28). As a result, this study is designed to examine the types of interpretative research methods applied by researchers in the field (Knight & Ruddock, 2009, p. 2). At the end, most appropriate method will be chosen to guide this study.

Figure 3.1 illustrates three main approaches to research - qualitative, quantitative, and mixed methods (Newman, Benz & Ridenour, 1998, p. 2). Even though the processes of qualitative and quantitative methods are similar however, qualitative approaches have distinctive technique for data analysis and dependent on text and image data (Creswell & Creswell, 2017, p. 153).

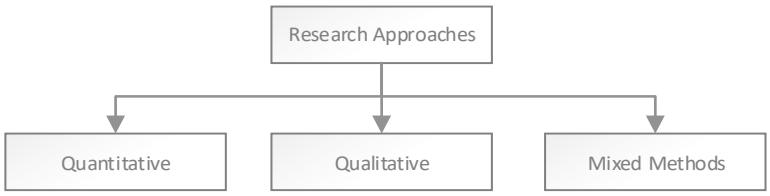

Figure 3.1: Research approaches (Creswell & Creswell, 2017, p. 25).

Quantitative method on the other hand deals with studies that focus on "counting things and the patterns that emerge from those counts" (Brown, 2011, p. 192). This involves collecting, analysing, and interpreting quantitative data and reporting the findings of the study. Collecting quantitative data mainly by way of survey, experiment, and so on (Creswell & Creswell, 2017, p. 18). The next section (2.2) is designed to discuss the chosen methodology to guide this study.

3.2 RESEARCH METHODOLOGY EMPLOYED

Methodology is recognised as the path to follow in order to answer the research question or questions (Van Gestel et al., 2012, p. 1). This path metaphor comes from the origin of the word "method" which is the Greek word "meta-hobos", meta means "after" and hodos means "way" (Sowa, 2011, p. 1). In most research arena,

the following the path metaphor always associate with the fundamental expectations however, in the legal domain, it has become an issue.

According to Van Gestel et al. (2012, p. 1), the word methodology in the legal research domain has a different meaning. It can be used to refer to the way a judge took to arrive on a decision for a case. Not only that but occasionally methodology and method appear to convey different things. In spite of this, Verma and Wani (2015, p. 3) believed that the study of law is closely associated with legal research. This is vital in order to provide directions. Paul Chynoweth reported in his book what is known as the "taxonomy of legal research styles" proposed by Henry Arthurs in 1983.

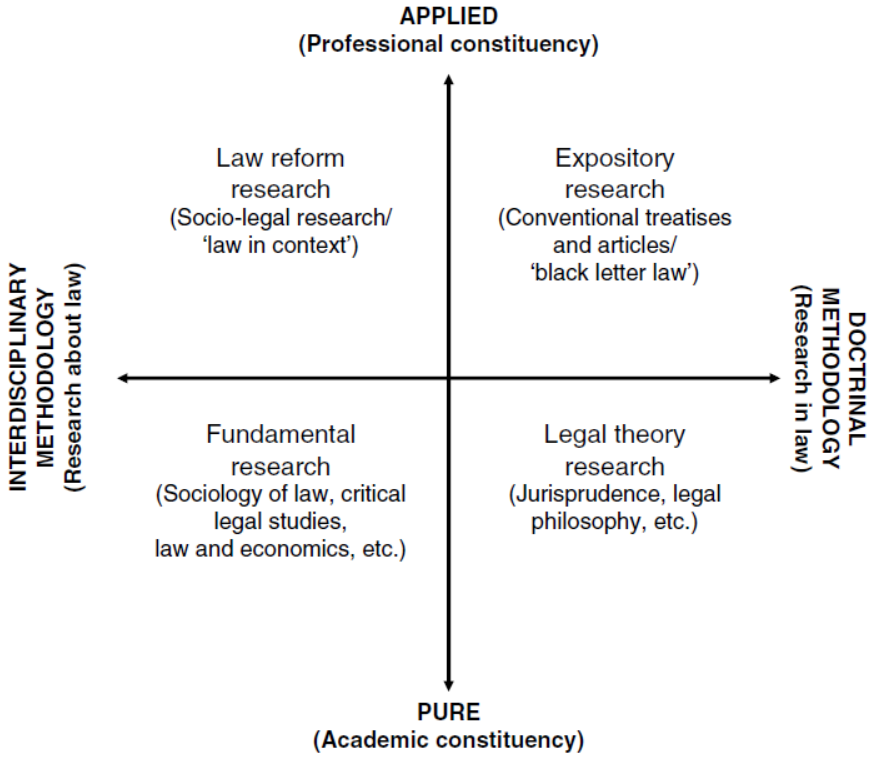

Figure 3.2: Legal research styles (as cited in Chynoweth, 2008, p. 29).

The vertical axis in figure 3.2 illustrates the distinguishing features between "pure research" – academically focused – and "applied work" – professionally focused. Nonetheless, the interest leans towards the horizontal axis. This highlights the differences between doctrinal and interdisciplinary research. McConville (2017, p. 4) explained that there are three main types in the legal research domain. The empirical legal research, international and comparative legal research, and doctrinal

research. In view of that, the doctrinal methodology focusses on researches in law whereas interdisciplinary methodology emphasises research about law. The next section is designed to define the chosen methodology to guide this study.

3.2.1 The Guiding Methodology

As it explained in the previous section, this study is designed to review the legislative frameworks of Tonga, Kiribati, Fiji, and Samoa (TKFS) in relation to Cybercrime. The outcome will then be compared with the legislative framework of a well-developed country in the Pacific such as New Zealand. Since the main objective of the study is to analyse and compare the legislative frameworks of five countries, Doctrinal Research Methodology (DRM) is the chosen methodology to guide this study.

The word doctrine originated from "doctrina" a Latin word means instruction, knowledge, or learning. This consist of notions, philosophies, and standards including cases, statutes, and rules (Hutchinson & Duncan, 2012, p. 84). Doctrinal research methodology is referred to as the method for research at the foundation of the proceeding.

Doctrinal research is defined as research which asks what the law is in a specific area. Therefore, the researcher will need to collect and analyse data from any relevant legislation within the concerned legal framework (Dobinson & Johns, 2017, p. 19). This will make clear any uncertainty with the law and their relationships within the legal framework. According to Chynoweth (2008, p. 29), doctrinal research is regarded as the study of legal texts. DRM is mainly used when the study is aimed to, investigate and analyse the fundamental principle of a body of law, and the related legislation (Wang, 2016, p. 25).

DRM provides a benchmark for argument, description, and interpretation that adds informative insights which helps with formulating certain occurrences when comparing to others and the legal system as a whole (Taekema, 2020, p. 13). Dobinson and Johns (2017, p. 20) explained that at this time, doctrinal, problem, policy, and law reform are the main four categories of research. This means that the study will begin by identifying and determining a specific area of the law - doctrinal. Thereupon, the problems with the existing legislative framework/law and

the supporting policies will be identified. Consequently, the researcher proposes and recommends the required changes - law reform.

Kharel (2018, p. 4) reaffirmed that initiating a doctrinal research starts by establishing the position of the law in respect to a particular issue and develop legal proposition. Not only that but the authorities on the primary and secondary data analysis to test the proposition. Queen's University gives explanation of the phases of researching into a specific issue within the legal regime as illustrated in figure 3.3.

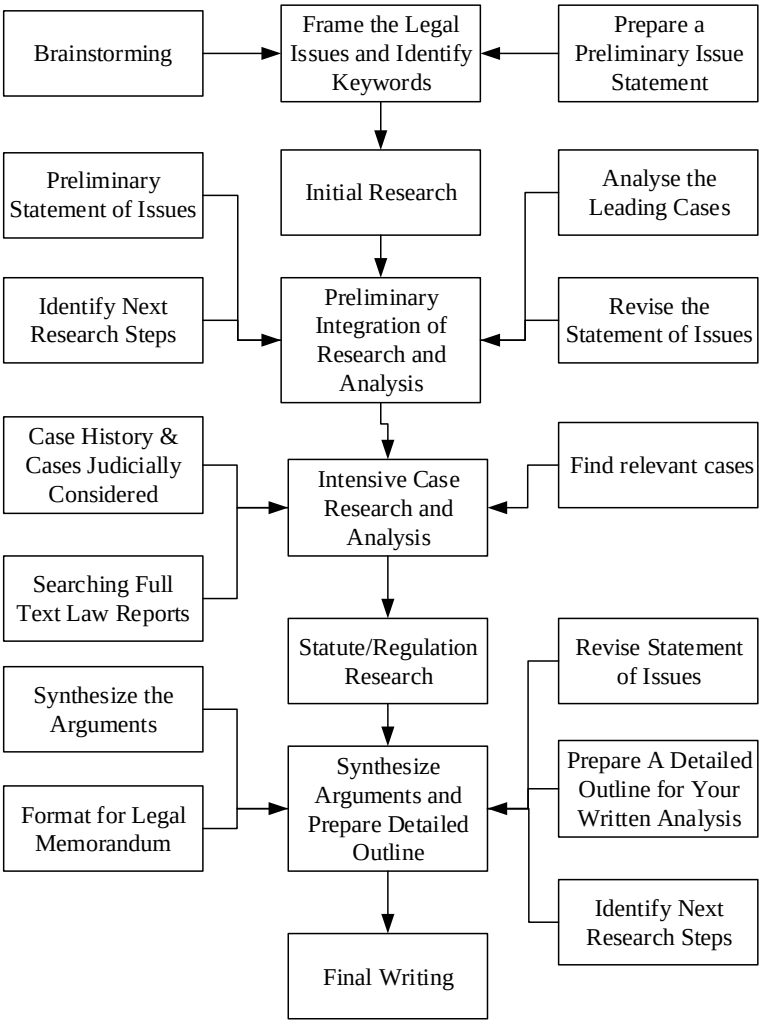

Figure 3.3: Phases of legal research (adopted from Queen's University, 2020, p. 3).

Table 3.1 outlined some of the main purposes of doctrinal legal research, and it explains why doctrinal method is important in the field of law. It is to enhance the

significant part of the law which may result in accomplishing comprehensive objective of the law.

Table 3.1: Purposes of doctrinal research (Kharel, 2018, p. 7).

	Doctrinal Research Main Purposes
I.	Develop new legal theories, principles and doctrines.
II.	Maintain continuity, consistency, and certainty
III.	Sort out daily client concerns
IV.	• Provide counsel to courts/clients on application of legal doctrine. • Examine the legal judgements to avoid conflicts in decisions from various courts
V.	Provide tools to enable judges/lawyers to well informed decision
VI.	Identify and acquire theory to explain how areas of the law fits together

According to Kharel (2018, p. 7), the critical mission of the law is justice. Doctrinal method is mostly theoretical in character. Nonetheless, it is always utilised in order to improve the content, develop principles, new knowledge, coding, and interpretation of the law. Gawas (2017, p. 129) rightly stated that, legal concepts and principles of all types' cases, statute and rules are used in the doctrinal legal research. Research and legal analysis are not only vital components but are connected and must work alongside each other.

3.2.2 Design of Study

According to Hevner et al. (2004, p. 88), the word design - is a search process to accomplish the most appropriate solution to a problem. The design of the study is created based on the Doctrinal Research which is the adopted methodology to guide the study. Figure 3.3 shows the design which specifies the major processes of the study – the input, process, and the output. The "input" involves reviewing of the existing relevant literature in the body of knowledge. The idea is to verify what is already known and its limitations. This helps to conceptualise the design and identify the research problem.

The second major process is the "process" which involves analysing the legislative frameworks of four selected countries in the South Pacific – Tonga,

Kiribati, Fiji, and Samoa (TKFS). The outcome will then be compared with the legislative framework of a well-developed country such as New Zealand. The purpose of this process to determine the readiness of Tonga's legislative framework to criminalise Cybercrimes. The third major process of this study is "output" and it refers to the final deliverable, the outcome of this study.

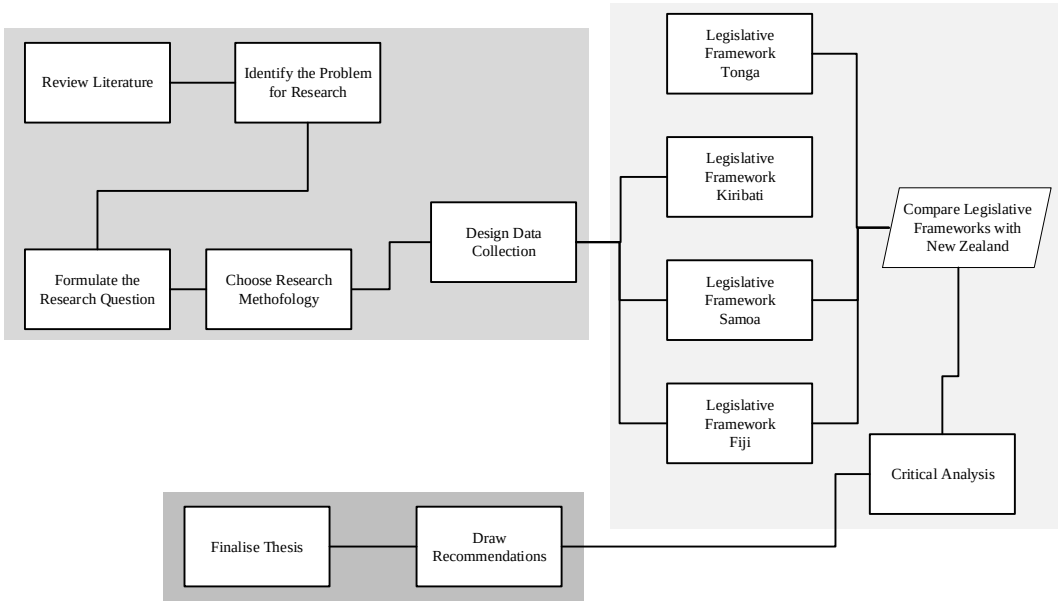

Figure 3.3: Design of the study.

As mentioned earlier, the objective of this study is to determine the readiness of the Tonga legislative framework to criminalise Cybercrimes. Accordingly, the processes are structured to aid in maximising the development of the artefact, the final product of the study. The results of the comparison with the New Zealand's legislative framework will be used to draw recommendations to inform the law makers of Tonga. Not only that but all together will answer the main research question and sub-questions and finalise and complete this thesis. The next section is to define and explain the research questions.

3.2.3 The Research Question

This study is designed to review the existing relevant literature in the body of knowledge, and answer the question *"What can be done to ensure the readiness of Tonga's legislative framework to combat cybercrime?"* In order to optimise the output of this study - the design, data analysis, findings; three sub-questions were

also developed to help brings out the best solution that meets the objective of this study.

SubQ 1 – What are the weaknesses of the current cybercrime legislation in Tonga?

SubQ 2 – What are the advantages of having a cyber-specific legislation?

SubQ 3 – Is the legal system in Tonga ready for cybercrime?

The three sub-questions are to be answered by evaluating the legislative frameworks of four selected countries in the pacific – Tonga, Kiribati, Fiji, and Samoa (TKFS). The results are vital in identifying the current standing of Tonga legislative framework amongst the south pacific islands. The outcome will then be compared with the legislative framework of a well-developed neighbouring country such as New Zealand. The final outcome is crucial to answer the research questions and the development of the recommendations for the Tonga law makers.

3.3 CONCLUSION

An analysis of relevant literature in the body of knowledge is provided in chapter 1. This chapter (chapter) was designed to define and identify the most appropriate approach and methodology to guide the study. A design for the study was also developed based on the chosen methodology. The design highlighted the input, process, and the output as in figure 3.3. Section 3.2.3 outlined the main research question and sub-questions that will be answered at the completion of this study.

In the next chapter, chapter 4, the chosen methodology is put into action. Doctrinal Research methodology is used to guide the evaluation of legislative frameworks of three selected countries in the pacific - Kiribati, Fiji, Samoa and also compare with Tonga's cybercrime legislation.

Chapter 4

Tonga and the Three Selected Countries

4.0 INTRODUCTION

This chapter is designed to provide an overview and a review of the legislative framework of Tonga, Kiribati, Samoa, and Fiji. The Pacific islands are referred to as the Pacific microstates as they are very small, internationally recognised sovereign states. A "Microstate" is defined by the United Nations as a state with one million or less population and with limited natural and human resources (Stringer, 2006, p. 548).

However, the rapid growth of Information & Communication Technology has reached the Pacific microstates regardless their lack of natural and human resources. These developments have positively effect lifestyles across the area. The Kingdom of Tonga for instance, in August 2013, had the first submarine cable (fibre optic) installed which connect it to the outside world. (Matangi Tonga, 2013). Therefore, more places are now available with open wireless hotspot such as pizzerias, hotels, cafes, pubs, and restaurants (Lutui, Tete'imoana & Maeakafa, 2017, p. 1). At the same time, this advancement also brings opportunities for various types of Cyber-attacks.

As mentioned earlier, this chapter will review the legislative frameworks of Tonga, Kiribati, Samoa, and Fiji in relation to Cybercrime. This review will then compare to the legislative framework to New Zealand, a well-developed country in the region. This comparison will be based on Cybercrime categorisations found in the literature. According to Ngo & Jaishankar (2017, p. 2), there are thirty different types of Cybercrimes found in the literature including: cyber bullying, harassment and stalking, and distributed denial of service attacks, online fraud, credit card fraud, spamming, email spoofing, hacking, malware and identity theft.

We are living in a digital age where governments, businesses, and individuals are entirely dependent on information and communication technologies to conduct their daily business and it critical to safeguard cyberspace from cybercrime (Watney, 2012, p. 71). According to Arief and Adzmi (2015, p. 84), the

security of cyberspace is more and more vulnerable to cyberattacks. Wall (2015, p. 1) stated that cyber criminals have made the Internet a channel for criminal activities.

Cybercrime has been defined in various ways and is seen as a combination of crime and cyberspace (Arief, Adzmi & Gross, 2015, p. 71). There is no formal definition for the word cybercrime. However, it is use to define a vast range of criminal offences against computers, computer-related and other electronic devices, information technology networks, or traditional crimes (Donalds & Osei-Bryson, 2019, p. 403). Cybercrimes are regard as an international crime, no boundaries which raise an issue in terms of jurisdiction (Tsakalidis et al., 2019, p. 22).

Barn & Barn (2016, p. 2) explain that Cybercrimes can be divided into three main categories: 1. Crimes that relies on the use of technology. 2. Publishing of illegal contents via Cyber-space. 3. Crime occurs in scientific forums. Alternatively, McGuire & Dowling (2013, p. 2) explained that Cybercrime categorisation is in two-fold: "Cyber-dependent and Cyber-enabled" crimes. Cyber-dependent refers to new crimes such as malware, hacking, and viruses that made possible by technology. Cyber-enabled crimes refer to old crimes including theft, fraud, and harassment but committed using computers or other electronic devices.

Gordon & Ford (2006, p. 13) argued that Cybercrimes are divided into two types – Type 1 is "techno-centric" and Type 2 is "people-centric". It is evident however, that Gordon & Ford's Type 1 cybercrime is aligned with "Cyber-dependent" crimes whereas the Type 2 crimes includes social engineering. Nevertheless, the advancement of Information and Communication Technologies (ICT) and the rise in Cybercrime produced or generated a new major challenges and issues for law enforcement agencies around the world. This gives computer scientists, Cyber-security experts, and researchers in the field around the world a significant task of finding a way to prevent, defend, and protect information assets.

Information assurance is a major issue in the field of Computer Science. Information assurance encompasses the foundations of Information Security which are confidentiality, integrity, and availability. This provides defensive mechanisms for information and data while in process, storage, and in transmission (Schou &

Trimmer, 2004, p. 1). Confidentiality provides an assurance that information is not accessible to unauthorised persons or devices. Integrity provides assurances that the quality of information will always remain uncontaminated, and availability makes sure that information will be available for use by authenticated users (Elmaghraby & Losavio, 2014, p. 493).

Will Davis and Chi (2011, p. 354) believed that there are five principles in terms of protecting and defending information, and they are confidentiality, integrity, authentication, availability, and non-repudiation. Non-repudiation is concerned with ensuring that no one can deny something. For instance, if information is exchanged between two parties, correct evidence data if vital to non-repudiation. Therefore, proof of origin will not allow the originator to deny association, same goes to the receiver (Standard Standardisation of ITU, 2008, p. 2).

The other four principles already mentioned earlier by Elmaghraby and Losavio but they group Integrity and authenticity together. Nevertheless, Information and Communication Technology has become part of our daily lives these days, applied in different ways from healthcare to smart cities. The pervasiveness of these devices makes them vulnerable to various cyber threats (Kettani & Cannistra, 2018, p. 184). According to the latest report from European Union Agency for Network and Information Security, the top fifteen cyber threats are showing in table 4.1 below.

Table 4.1: The current threat landscape (ENISA, 2019, p. 9).

Ranks	2017	2018
1	Malware	Malware
2	Web Based Attacks	Web Based Attacks
3	Web Application Attacks	Web Application Attacks
4	Phishing	Phishing
5	Spam	Denial of Service
6	Denial of Service	Spam
7	Ransomware	Botnets
8	Botnets	Data Breaches

9	Insider Threat	Insider Threat
10	Physical manipulation/ damage/ theft/loss	Physical manipulation/ damage/ theft/loss
11	Data Breaches	Information Leakage
12	Identity Theft	Identity Theft
13	Information Leakage	Cryptojacking
14	Exploit Kits	Ransomware
15	Cyber Espionage	Cyber Espionage

Table 4.1 shows a very interesting new development. Ransomware was number 7 in 2017 but a new related threat Crytojacking (a/k/a Cryptomining) emerged as a new threat in 2018. Threat actors moved from ransomware to Cryptojacking because the risk is low while the profit is high. Cryptomining uses the processing power of the victim's computer to mine cryptocurrencies without the victim's knowledge (ENISA, 2019, p. 82).

4.1 THE CYBERCRIME NOTIONS

Given that we are living in a digital age where governments, businesses, and individuals are entirely dependent on information and communication technologies to conduct their daily business. It is now critical and very important for everyone to come together and safeguard cyberspace from cybercrime (Watney, 2012, p. 71). According to Arief and Adzmi (2015, p. 84), the security of cyberspace is more and more vulnerable to cyberattacks. Wall (2015, p. 1) stated that cyber criminals have made the Internet a channel for criminal activities.

Cybercrime is seen as a combination of crime and cyberspace (Arief, Adzmi & Gross, 2015, p. 71). There is no formal definition for the word cybercrime. However, it is use to define a vast range of criminal offences against computers, computer-related and other electronic devices, information technology networks, or traditional crimes (Donalds & Osei-Bryson, 2019, p. 403). Cybercrimes are regard as an international crime, no boundaries which raise an issue in terms of jurisdiction (Tsakalidis et al., 2019, p. 22).

4.2 LEGISLATIVE FRAMEWORK OF TONGA

Small, untouched but widely spread out islands in the South Pacific have become the Kingdom of Tonga. Tonga is a constitutional monarchy. The head of state is the King and the head of government is the Prime Minister, The Monarch supported by a privy council consisting of ministers and governors from the islands of Ha'apai and Vava'u. In Tonga, the responsibility of Government administration lies in the Prime Minster and the Cabinet which control, except in instances of minority government, a majority of the votes in the "Falealea" the unicameral parliament.

The Falealea consists of 26 members, 17 representatives from the 17 electoral constituencies of the country, and 9 representing the nobles of the five main islands of Tonga. The 26 members of the Falealea then elect the Prime Minister. The Prime Minister will then recommend the members of the Cabinet from among elected members of the Falealea. The Prime Minister has a constitutional right to nominate up to four cabinet unelected members. Tradition and culture are important and still very strong in the Kingdom of Tonga (Tonga Tourism Authority, 2018, p. 1).

4.2.1 Cybercrime Main Legislation

In the Kingdom, the Computer Crimes Act 2003 revision sets out the structure of cybercrime legislation. According to the Solicitor General, Kefu (2011, p. 1), the Computer Crimes Act was based on the Commonwealth Model Law. The Model Law was aimed to put a legal framework in place criminalising computer and computer related crimes, particularly for Commonwealth countries (Commonwealth Secretariat, 2017, p.1).

Without a doubt, cybercrime brings unique challenges with regards to legislation, law enforcement, and policy-making. According to the Commonwealth Secretariat 2017, Cybercrime is not a defined legal category. However, it includes offences aimed at computers, or communication systems, their users or the data they contain. Not only that but when these systems involved in committing more traditional offences.

Tonga has a number of legal statutes that can be applied to computer, information system or cyber related crimes. This includes the Tonga *Computer*

Crimes Act; the *Evidence Act* – for some evidential provisions; *Criminal Offences Act*; *Pornography Control Act*; *Communications Act 2000*; Mutual Assistance in *Criminal Matters Act*; and *Extradition Act*. In the midst of all these Acts, the Tonga *Computer Crimes Act* is the primary Act for prosecuting computer, information system and/or cyber related crimes as well as to provide for the collection and use of electronic evidence.

Section 4 of the Tonga *Computer Crimes Act 2016* chapter 10.06 is designed to criminalise offences related to: Illegal access, interfering with data, Interfering with computer system, Illegal interception of data, and Illegal devices. Section 4 is the provision which criminalises illegal access, that is, someone who intentionally accesses a computer system with no lawful justification. Interfering with data applies to someone who intentionally with no lawful justification destroys or manipulates data, causes data to be meaningless or useless, interferes with the lawful use of data, or denies access to authenticated users. Interfering with computer system means, someone who intentionally without any lawful justification interferes with the normal operations of a computer system, or interferes with authenticated users.

Illegal interception of data refers to someone who intentionally with no lawful justification intercepts any transmission of data from a computer system. Illegal devices refer to, a person who intentionally without any lawful justification produces, sells, obtains or distributes a device, computer program, password, access code with the intent that it be used for the purpose of committing an offence under sections 4, 5, 6, or 7 of the Tonga *Computer Crimes Acts*. In order to understand this section (4) of the act, there are five elements that need to be analysed including, computer, computer data, computer data storage medium, computer system, and traffic data. These terms are defined in section 2 of the Act. According to the section 2 of the Tonga *Computer Crimes Act 2016*,

1) Computer

"computer" is defined as;

"an electronic, magnetic, optical, electrochemical, or other data processing device, or a group of such interconnected or related devices, performing logical, arithmetic, or storage functions, and includes any data storage facility or

communications facility directly related to or operating in conjunction with such device or group of such interconnected or related devices" but does not include –

a) an automated typewriter or typesetter;
b) a portable hand held calculator; or
c) a similar device which is non-programmable or which does not contain any data storage facility;
d) such other device as the Minister may, by notification in the Gazette, prescribe;

This definition in section 2 of the Act departs from the Commonwealth Model Law which does not provide a definition for the term "Computer". The English Law Commission stated that the UK Acts did not use this kind of definition. It noted that that such legislative definition may be unnecessary and undesirable (Christopher Lee, 1993, p. 267). Nevertheless, the Tongan definition is very similar to the definition provided by the Computer Crime and Intellectual Property section of the Cybercrime Laws of the United States. The definition is in twofold, providing for the definition of the term "computer" while also outlining what is not a computer in the second part. (Rees, 2006, p. 12). unsurprising

In the New Zealand Law Commission Report 54 on Computer Misuse, section 2, sub-section 15, The commissioners observed that the Attorney-General's Department of Australia, the Law Commission of England and Wales, and the Scottish Law Commission do not recommend defining the term "computer". Two reasons provided were 1) the rapid growth and advancement of computer technology will render and definition obsolete quickly; and two a legal definition of the term "computer" can be very complex and may generate considerable argument regarding the meaning of the term which can detract from enforcement efforts. Based on those reasons, the law commissioners believed that it is best not to provide a definition for the term "computer" (Justice Baragwanath et al., 1999, p. 8).

Nonetheless, looking at the definition of the term "computer" provided by the Tonga Computer Crimes Act, the National Institute of Standards and Technology (NIST) from the United States defined the term as, "computer" as *"a device that accepts digital data and manipulates the information based on a*

program or sequence of instructions for how data is to be processed" their Special Publication 800-34 (Swanson, et al., 2010, p. 1). The Israeli Computer legislation adopted this definition (Deutch, 1995, p. 2).

Although Samoa does not have a specific Act for cybercrimes or computer related crimes but in the Part XVIII of the *Samoa Crimes Act 2013* "Crimes Involving Electronic Systems" section 205, a definition is provided for the term "device". *A "device" includes the following:*

(a) components of electronic systems such as computer, mobile phones, graphic cards, memory, chips;

(b) storage components such as hard drives, memory cards, compact discs, tapes;

(c) input devices such as keyboards, mouse, track pad, scanner, digital cameras;

(d) output devices such as printer, screens.

Papua New Guinea on the other hand in the southwestern Pacific, has a Cybercrime Code Act 2016. Section 2 of the Act provided a definition for the term "computer". *"A "computer" means an electronic, magnetic, optical, electrochemical, or other data processing device, or a group of such interconnected or related devices, performing logical, arithmetic, storage and display functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device or group of such interconnected or related devices, but does not include an automated typewriter or typesetter, or a portable hand held calculator or other similar device which is non-programmable or which does not contain any data storage facility".*

The definition for the term "computer" provided in the PNG Cybercrime Code Act is very similar to the definition in the Part XVIII "Crimes Involving Electronic Systems" of the Samoa Crimes Act 2013 for the term "device". However, the PNG Cybercrime Code Act definition is the same as the definition provided by the Tonga Computer Crimes Act except it does not include the sub-section (d) of the Tonga Computer Crimes Act that states *"such other device as the Minister may, by notification in the Gazette, prescribe".*

2) Computer data

> ***"computer data** means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function"*

This definition was taken from the "Model Law on Computer and Computer Related Crime". The definition is in two-fold, first the data/information and the second, the programmes that are used to capture and process the data in a computer system. This definition is very similar to how the New Zealand Law Commission defined "computer data". In Report 54 on Computer Misuse, section 2, sub-section 14 the Commission defines data as "*intended to include all types of information stored on a computer, including the programmes which run the computer as well as personal information"* (Justice Baragwanath et al.,1999, p. 8).

The Samoa Crimes Act 2013 Part 18 on Crimes Involving Electronic Systems provides a definition on "electronic data" as; *"electronic data means any representation of facts, concepts, information (either texts, sounds or images), or machine-readable code or instructions, in a form suitable for processing in an electronic system, including a program suitable to cause an electronic system to perform a function".* This definition is also very similar to the Tonga Computer Crimes Act definition, except that the Samoa Crimes Act definition defined provides additional terns noting the electronic data includes *"any representation of facts, concepts, information"* as either in the forms of *"texts, sounds or images or machine-readable code or instructions".*

The PNG Cybercrime Code Act defined the term "data" as *""data" means any representation of facts, concepts information (being either text, audio, video, audiovisual or images) machine readable code or instructions, in a form suitable for processing in an electronic system or device, including a program suitable to cause an electronic system or device to perform a function".* This definition is very similar to the Samoa Crimes Act definition however, the PNG Cybercrime Code Act definition expand the *"representation of facts, concepts information"* to include *"audiovisual".*

Section 2 of the Singapore Computer Misuse Act, Revised Edition 2007 provided a definition for "data" as; *"data means representations of information or*

of concepts that are being prepared or have been prepared in a form suitable for use in a computer (p.4). This definition is similar to the first half of the definition provided in the Tonga Computer Crimes Act. However, the Singapore Computer Misuse Act's definition does not include the programmes that capture and process the data.

3) Computer data storage medium

> ***"computer data storage medium*** *means any article or material such as a disk, from which information is capable of being reproduced, with or without the aid of any other article or device"*

This definition obviously adopted from the Model Law on Computer and Computer Related Crime definition. This definition focusses on the component or media that is used to store the data. It is clear that this definition is very general, unlike the definition provided in the Samoa Crimes Act. The definition is provided as part of the definition of the term "device" as *"storage components such as hard drives, memory cards, compact discs, tapes"*. The PNG Cybercrime Code Act also did not provide a specific definition for the *"computer data storage medium"* however, same as the Samoa Crimes Act, provide the same definition as part of the definition provided for the term "device".

4) Computer system

> *"**"computer system"** means a device or a group of inter-connected or related devices, including the Internet, one or more of which, pursuant to a program, performs automatic processing of data or any other function"*

As mentioned earlier in section 4.1.1, the Tonga Computer Crimes Act was based on the Commonwealth Model Law. The definition given for the term "Computer system" was taken from the Commonwealth Model Law. In the New Zealand Law Commissioners Report 54, a definition for the term "Computer Network" is provided. The definition divided "Computer Network" into two main areas. One focusses remote access connection and two, interconnection of 2 or more computers.

The Samoa Crimes Act combines the two definitions (Model law and the NZ Report) when defining the term "Electronic system." This definition concerns with one or more inter-connected devices with a program that can automatically process data or perform any other function. Also, a computer, two or more inter-connected electronic systems, remote access communication, and two or more inter-connected electronic systems including remote accessing or any other device.

The PNG Cybercrime code act on the other hand, summarises the definition given in the Samoa crimes act for the term "electronic system". The PNG Cybercrime code act stated that an "electronic system means a system consisting of hardware or software, or a group of interconnected or related systems or devices, one or more of which, under a program, performs automatic processing, generating, sending, receiving, or storing of data and includes, but is not limited to, electronic devices, the Internet, input, output and storage facilities". The PNG Cybercrime code act also highlighted what it meant *"performs automatic processing" as "without direct human intervention".*

5) Traffic data

*"**"traffic data"** means computer data that relates to a communication by means of a computer system; and is generated by a computer system that is part of the chain of communication, and shows the communication's origin, destination, route, time, date, size, duration or the type of underlying services".*

This definition also was adopted from the Commonwealth model legislation. The Samoa Crime Act 2013 does not contain a provision for dealing with crimes related to traffic data. The Papua New Guinea Cybercrime Code Act 2016 contains a provision for dealing with acts related to "data traffic". The definition provided in the section 2 of the Act is *"**"data traffic"** means any electronic data relating to a communication by means of an electronic system or device, generated by an electronic system or device 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".*

The definition of the term "traffic data" in the Tonga Computer Crimes Act is similar to the definition provided in the Commonwealth model legislation. It is very specific to data in communication by means of a computer system only. However, Part 1 section 2 of the Tonga Computer Crimes Act provides a definition for the term "computer system". This definition states that *"**computer system"** means a device or a group of inter-connected or related devices, including the Internet, one or more of which, pursuant to a program, performs automatic processing of data or any other function"*. With this definition, it aligns the Tonga Computer Crimes Act definition with the definition provided in the PNG Cybercrime Code Act.

4.3 TONGA COMPUTER CRIMES ACT 2016

All types of attacks targeting electronic data, computers, and computer systems are an attack on the information security "CIA" triangle, Confidentiality, Integrity, and Availability (von Solms & van Niekerk, 2013, p. 98). These attacks are considered as cybercrime offences (Gřivna & Drápal, 2019, p. 1). Currently, much work focusses on creating legislation to criminalise cyber related offences. There are model laws created to assist governments in this important work to fight cybercrimes (Clough, 2014, p. 701). For instance, the Commonwealth Model Law on Computer and Computer Related Crime, the ETS 185 – Convention on Cybercrime, the ITU Model Legislation, the World Bank-OECS-EGRIP Model Law on Cybercrime (Jamil, 2014, p. 10).

The Kingdom of Tonga has signed the Budapest Convention on Cybercrime in 2017 and has become the first Pacific Island State to sign the Budapest Convention (MEIDECC, 2017, p. 1). The Convention is aimed at criminalising cyber related offences including illegal access, illegal interception, data interference, system interference, and misuse (Weber, 2012, p. 431). The Computer Crimes Act 2003 was the first Act enacted to combat computer crimes in the Kingdom. Also, it provides for the collection and use of electronic evidence. A revised edition of this Act was passed in 2016 and there has been not changes to the legislation since that time.

4.4 COMPUTER CRIME OFFENCES

Part II of the Tonga Computer Crimes Act highlighted five main types of computer crime offences - Illegal access, Interfering with data, Interfering with computer system, Illegal interception of data, and Illegal devices. The following sub-sections will outline and explain these offences.

4.4.1 Illegal Access

Section 4 of the Tonga Computer Crimes Act consists of main four sub-sections. Sub-section 1 defined the provision to criminalise *'illegal access'*, and sub-sections 2 and 3 outlines the penalties under this section. Sub-section 4 states the precondition for any prosecution under this section. This specified that for any prosecution under this section, it will be presumed that the accused has the knowledge with regards to computer, program or data. Not only that but the essential knowledge that unauthorised access to that computer, program or data is an offence.

Sub-section 1 states the for the purpose of this section, a computer shall be treated as a *"protected computer"*. The term *"protected computer"*, neither section 2 nor anywhere in the Tonga Computer Crimes Act provide a definition or mention the term but section 1. Even though the Tonga Computer Crimes Act adopted the Commonwealth Model Law but for this particular offence is different. The definition provided in the Commonwealth Model Law is very simple and did not include provision for the term *"protected computer"*.

Part XVIII of the Samoa Crimes Act does not include *"illegal access"* however, section 208 outlined the penalties and provide the definition for *"Illegal remaining in an electronic system"*. This section criminalises a person who logs into an electronic system with no justification or excuse and remain logged in. Although this section covers illegal access to a computer system but it did not use the term *"protected computer"*.

The PNG Cybercrime Code Act uses the term *"Unauthorised Access or Hacking"* to criminalise this type of offence. The definition adopted by the PNG Act is very similar to that of the Commonwealth Model Law. However, the PNG Act is in two-fold. Section 6 sub-section 1 focuses on the unauthorised access side

of the offence. That action alone is guilty of a misdemeanour and the penalty is imprisonment with a maximum five years or a fine not exceeding 7,000 Kina (PNG currency) or both. The second part (sub-section 2) focuses on the damages or losses as a result of the unauthorised access. The penalty is imprisonment with a maximum of 15 years or a fine not exceeding 25,000 Kina or both.

Even though that it stated in the Section 4 sub-section 1 of the Tonga Computer Crimes Act that a computer "shall" be treated as a protected computer, the Act penalises the offender differently. Sub-section 2 penalises illegal access to any computer system with a fine not exceeding TOP$10,000, or maximum 2 years imprisonment or both. Illegal access to any protected computer on the other hand will be liable upon conviction to a fine not exceeding TOP$100,000 or 20 years maximum imprisonment or both. Following is the provision to criminalise *"illegal access"* in the Tonga Computer Crimes Act 2016.

"For the purposes of this section, a computer shall be treated as a "protected computer" if the person committing the offence knew, or ought reasonably to have known, that the computer or program or data is used directly in connection with or necessary for —

a) the security, defence or international relations of the Kingdom;

b) the existence or identity of a confidential source of information relating to the enforcement of a criminal law;

c) the provision of services directly related to communications infrastructure, banking and financial services, public utilities, public transportation or public key infrastructure; or

d) the protection of public safety including systems related to essential emergency services".

However, the term *"protected computer"* is defined in the Title 18 of the United States Code – Crimes and Criminal Procedure, Section 1030(e)(2) as a computer –

a) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or

b) which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States.

The ICB4PAC (2013) argued that, the provision in the section 4 of the Tonga Computer Crimes Act is complicated. This is due to the general and broad nature of the definition also, the specific provision to criminalise illegal access to protected computer systems (p.42).

4.4.2 Interfering with Data

Section 5 states the provision to criminalise *"interfering with data"* offences. The provision highlighted five various types that criminalise under this section. That is – a person who wilfully without lawful excuse - destroys or alters data; renders data meaningless, useless or ineffective; obstructs, interrupts or interferes with the lawful use of data; obstructs, interrupts or interferes with any person in the lawful use of data; or denies access to data to any person entitled to it, The penalty for this type of offences under this section 5 a fine not exceeding $10,000 or imprisonment for a period not exceeding 2 years or to both. This provision was adopted from the section 6(1) of the Commonwealth Model Law (Commonwealth Secretariat, 2017, p.7).

The PNG Cybercrime Code has a very similar provision in section 8 *"data interference"* of their act. Types of offences is very similar to that provided in the Tonga Computer Crimes Act except they added - damages or deteriorates data; deletes data. In terms of penalties, there are two different penalties under the section 8 of the PNG Cybercrime Code Act. If the accused is a natural person, the fine not exceeding K20,000.00 (Kina – PNG currency), or imprisonment for a term not exceeding 10 years, or both. In the case of a body corporate, a fine not exceeding Kl00,000.00 (Cybercrime Code Act, 2016, p.7).

The Samoa Crimes Act 2013, Part XVIII, section 210 on *"damaging or interfering with electronic data"* is very similar to the section 8 provision for *"data interference"* on the PNG Cybercrime Code from sub-section (a) to (g). The difference is how section 8 penalises someone who is found guilty under the

provision. There is monetary fine however, a person will be liable to not more than 7 years imprisonment if found guilty.

Information assets are the most critical assets for many organisations including government. ICT infrastructures are used to conduct business today and critical information assets are at risk. The security requirements focus on the confidentiality, integrity, and availability of the information (Alberts & Dorofee, 2002, p.113). As a result, various organisations and governments around the globe are implementing laws on cybercrime as mean of protecting and preventing interference with these vital assets such as deleting, modifying, manipulating, obstructing and denying access (Reddy & Reddy, 2014, p.1).

4.4.3 Interfering with Computer System

Section 6 of the Tonga Computer Crimes Act is a provision to criminalise *"interfering with computer system".* The provision is divided into two different sub-sections. Sub-section (a) deals with hindering and interfering with the functioning of a computer system. Sub-section (b) deals hindering and interfering with a user who is lawfully using the computer system. The penalty under this provision is a fine not exceeding TOP$5,000 or not more than 1-year imprisonment or both (Computer Crimes Act, 2016, p.8).

Sub-sections (a) and (b) are similar to the provision shown in section 7(1) of the Commonwealth Model Law section 6. However, the Commonwealth Model Law defines the term *"hinder"* stated in 6(a) and 6(b) as - (a) cutting the electricity supply to a computer system; (b) causing electromagnetic interference to a computer system; (c) corrupting a computer system by any means; and (d) inputting, deleting or altering computer data (Commonwealth Secretariat, 2017, p.7).

Section 212 of the Samoa Crimes Act deals with Illegal system interference. The provision is two-fold. Sub-section 1(a) and 1(b) are very similar to section 6(a) and 6(b) of the Tonga Computer Crimes Act. However, sub-section 1(c) focusses on electronic system that is used in critical infrastructure operations. Section 212(2) defines sub-section 1(c) "critical infrastructure" as, *electronic systems, devices, networks, electronic programs, and electronic data, that are so vital to the country*

that the incapacity or destruction of or interference with such systems and assets would have a debilitating impact on security, national or economic security, national public health and safety, or any combination of those matters (Crimes Act, 2013, p.99). The penalty for crimes committed under this provision is imprisonment not exceeding 7 years.

System Interference is the criminalised under the section 9 of the *PNG Cybercrime Code Act 2016.* The provision is in two-fold and very similar to the Samoa Crimes Act where, sub-section (1)(a) deals with the normal functioning of the electronic system and sub-section; and (1)(b) deals with interfering with legitimate user of the electronic system. The penalty under sub-section (1)(a) in the case of a natural person is a fine not exceeding K10,000 or imprisonment not more than 10 years or both. In a case of a body corporate, it is a fine of not more than K100,000 (Cybercrime Code Act, 2016, p.7).

Sub-section (2)(a) and (2)(b) of section 9 is concerned with system interference against operation of electronic system or devices exclusively for used in critical infrastructure. The penalty in the case of a natural person is a fine not exceeding K100,000 or imprisonment for not more than 25 years or both. In the case of a body corporate, is a fine not exceeding K1,000,000 and K25,000 for each subsequent day the critical infrastructure remains inoperable.

4.4.4 Illegal Interception of Data

Section 7 of the Tonga *Computer Crimes Act* is the provision for "illegal interception of data". This provision criminalises the unlawful application of any technical method to intercept data while in transmission or via an electromagnetic emission. Section 209 of the *Samoa Crimes Act* deals with "illegal interception", the description is very similar to that of the Tonga *Computer Crimes Act* but with few variations. The *Samoa Crimes Act* added intentional interception of data that is not intended to available to public. Also, section 211 of the Samoan Act is concerned with "Illegal acquisition of electronic data" which criminalises intentional acquisition of data without authorisation or lawful justification particularly, if they are classified as a protected computer or protected computer system.

Fiji Cybercrime Bill 2020 section 6 is concerned with *"unauthorised interception of computer data or computer systems"* which means, "intentional and unauthorised interception of any computer data." Such activity is an offence under this provision. Section 6(2) broadens the methods of interception to include listening to, recording or acquiring the substance. Part 7 of the Kiribati *Telecommunications Act 2004* are the provisions for Computer Misuse in Kiribati. Section 68 is concerned with *"unauthorised use or interception of computer service"* and 68(2) is particularly designed to focus on criminalising knowingly unauthorised interception computer program or data.

The Article 3 of the Budapest Convention on Cybercrime (2001, p. 4) is concerned with illegal interception of data. The Convention suggested that each country should adopt legislation to criminalise intentional and unauthorised interception of data. As mentioned earlier, the design of the Tonga *Computer Crimes Act* was informed by the Commonwealth Model Law on Computer and Computer Related Crime. With regards to illegal interception of data, section 8 of the Commonwealth model law is identical to section 7 of the Tonga *Computer Crimes Act.* Among the four chosen Pacific island countries mentioned in this paper, they all have provisions to criminalise illegal interception of data with small variations based on each country's requirement.

4.4.5 Illegal Devices

Article 6 of the Budapest Convention on Cybercrime provides suggestions in regard to the term "misuse of devices."; that is, each country should enact legislation along with other measures to make the "misuse of devices" a criminal offence. This would encompass actions such as producing, selling, procuring, importing, and distributing a device including a computer program that are designed for the purpose of committing crimes.

As mentioned earlier, the Tonga *Computer Crimes Act* was based on the *Commonwealth Model Law*. As a result, the descriptions provided in these provisions on "illegal devices" are identical. The provision criminalises producing, distributing, and selling, importing and exporting of a device including computer programs without authorisation. This includes access to credentials such as a

username, password, or access code specifically for the use to commit a crime. Section 213 of the *Samoa Crimes Act* has the same provision with similar descriptions.

Section 8(1) and 8(2) of the *Fiji Cybercrime Bill 2020* is concerned with the "unlawful supply or possession of computer system or other device, or computer data". The *Fiji Cybercrime Bill 2020* does not include a specific provision for "illegal devices" however, section 8 has similar provisions. Section 8(1) is concerned with intentional manufacturing, selling, distributing, procuring, importing of any device, computer system, computer data, or computer program designed on purpose to use to commit a criminal offence. Section 8(2) on the other hand is concerned with the possession of any computer system, device, program or data designed primarily to aid with conducting a criminal offence.

4.5 COMPARISON

After going through this review, it is evident that Tonga, Fiji, Samoa, Papua New Guinea, and Kiribati have made an effort to keep up with the international guidelines and best practices when it comes to legal matters. Particularly, when it comes to dealing with cyber criminals. There is no doubt that we are living in the digital age and the advancement and growth of technology is faster than first anticipated (Li, 2011, p. 264; Yao & Liu, 2011, p. 1068; Sultana & Turkina, 2020, p. 2).

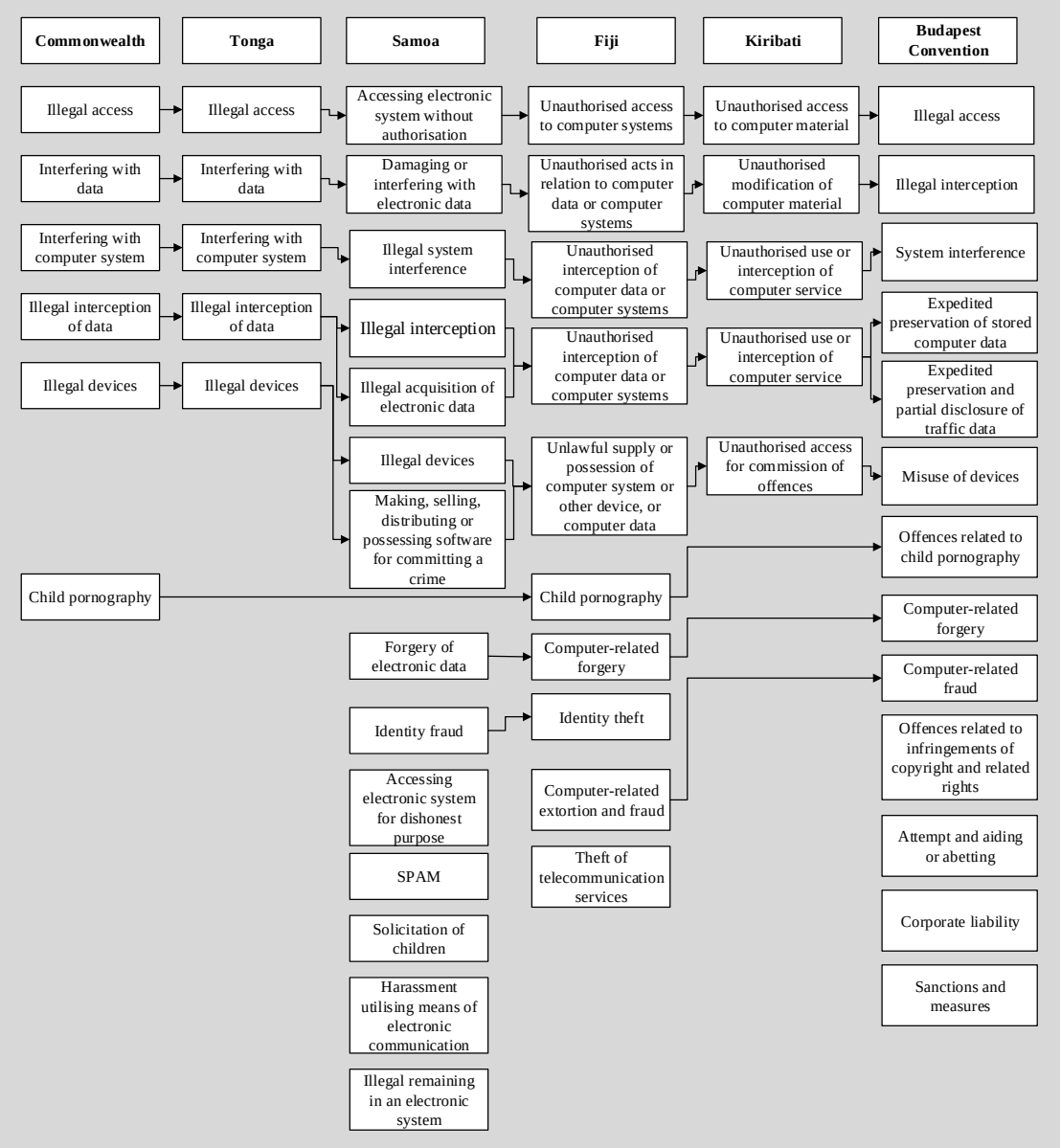

Figure 4.1: The Mapping of the Chosen Pacific Countries

Figure 4.1 illustrates the full mapping of the computer and computer related Acts in South Pacific countries. This shows their similarities and differences and how they compare to the Commonwealth Model Law on Computer and Computer Related Crime and the Budapest Convention on Cybercrime. Table 4.1 shows each party involved in this study and the number of provisions they offer. The Tonga *Computer Crimes Act* and the *Computer Misuse* – part 7 of the Kiribati *Telecommunications Act 2004;* both offer 5 provisions each to criminalise computer and computer related criminal offences.

The Tonga *Computer Crimes Act* is concerned with offences such as "illegal access" however, a computer is assumed to always be a "protected computer" in this provision. As such, a violation of this section is when a computer, program, or data that is in connection or necessary for the function of "security, defence, or international relations of the Kingdom". This includes essential services (i.e., banking, communication infrastructures, etc) and extends to systems used for the "protection of public safety".

The *Kiribati Computer Misuse* legislation on the other hand stated in section 65 that "unauthorised access to computer material" refers to the use of a computer to access programs and data knowingly without permission to do so. However, the difference is that section 65 of the *Kiribati Computer Misuse* does not extend to include computer program, data, or any program and data within that computer. The Tonga *Computer Crimes Act* recognises wilful interference with data, destruction or alteration of data in a way that results in its reliability being rendered useless. The *Kiribati Computer Misuse* has a provision in section 67 that explains in its provision for "unauthorised modification of computer material" as a person who changes the content on a computer.

Table 4.1: Each Party with Number of Provisions

Each Party and Number of Provisions					
Budapest Convention on Cybercrime	**Commonwealth** Model Law on Computer and Computer Related Crime	**Tonga** Computer Crimes Act	**Samoa** Crimes Involving Electronic Systems	**Fiji** Cybercrime Bill 2020	**Kiribati** Computer Misuse
13	6	5	14	11	5

In any case, section 4.1 of this chapter on computer crime offences, has provided a detailed review of the offences criminalised by the provisions provided by the parties involved in this study. Figure 4.1 has mapped out the provisions that relates to the five provisions defined by the offences section of the Tonga *Computer Crimes Act*. However, the Commonwealth Model Law has one extra provision on "child pornography". The provision to criminalise the intentional use of any computer system to publish, produce, or store any child pornography materials.

Out of the countries involved, only the *Fiji Cybercrime Bill* has a provision to criminalise child pornography. This provision is very similar to the Commonwealth Model Law provision with several differences. The Fiji provision does not include hiring or renting of child pornography materials, lending for gain, bartering, offering in any other way, or making available in any way. Article 9 of the Budapest Convention suggested that each country should establish legislation to make child pornography as a criminal offence. The Budapest Convention recommends adding computer related forgery and so far, only Fiji and Samoa included a provision to criminalise such an offence. That is the intentional and without lawful justification of input, alteration, deletion, or suppression computer data, resulting in in inauthentic data.

In terms of "identity theft" and "identity fraud", both the Commonwealth model law and the Budapest convention does not recommend the inclusion of such provision. Nonetheless, Fiji and Samoa included a provision to criminalise obtaining, transferring or possessing someone else's identity information with intention to commit an offence. The Budapest Convention suggests the adoption of a provision to establish "computer-related fraud" as a criminal offence. Thus, criminalising an offence that results in the loss of property to someone else by intentionally - without lawful excuse - altering, deleting and suppressing computer data, or interference with a computer system.

"Offences related to infringements of copyright and related rights", "attempt and aiding or abetting", "corporate liability", "sanctions and measures", were all suggested by the *Budapest Convention on Cybercrime.* As shown in Table 4.1, Samoa *Crimes Involving Electronic Systems* has 14 main provisions, the highest among the parties involved in this study. As shown in Figure 4.1, all provisions were compared including the Budapest Convention and the Commonwealth Model Law. As a result, the Samoa *Crimes Involving Electronic Systems* has 5 standalone provisions. These were implemented and put in place to deal with "accessing electronic system for dishonest purpose". "Dishonest purpose" means accessing and obtaining "property, privilege, service, pecuniary advantage, benefit, or valuable consideration" which results in a loss for another person. With this offence, the attempt is included.

Section 217 is the provision designed to criminalise "SPAM" and its function. SPAM refers to sending multiple messages using an electronic system to deceive targeted users. The electronic system the provision is referring to is the use of a "protected electronic system" to relay these electronic messages in an effort mislead users regarding its origin. SPAM under the Act refers to the use of "multiple electronic message", (eg E-Mails and instant messages), that are sent to more than 1,000 users.

Section 218 draws attention towards the "solicitation of children" in committing a crime. This occurs when a person uses technology to entice a child to meet them with the intention to commit an offence. Moreover, it includes the events that led up to the actual meeting. Section 219 considers the "harassment utilising means of electronic communication" which is the intentional persuasion and harassment of a person that results in emotional distress and intimidation. As the title states, this refers to using electronic communications to commit this specific offence.

Section 208(1) goes further into the issue by explaining that even if one gains unauthorised access into an electronic system, continuous access or remaining logged into the electronic system is considered an offence. Similar to the previous sections, section 208(2) states that this will not apply to those who have authority to gain access or have been lawfully granted access to the electronic system. There is only one standalone provision in the *Fiji Cybercrime Bill 2020* – section 13 "Theft of telecommunication services". This provision is designed to criminalise unauthorised access and intentional use of a computer to transfer, possess or use the telecommunication services of another person with the intent to commit or to aid and abet, or in connection with any criminal activity.

4.6 CONCLUSION

In conclusion, this chapter reviewed that computer and computer related crime laws implemented by countries in the South Pacific. Three countries were selected, Kiribati, Fiji, and Samoa to review and then compare with the cybercrime's law of Tonga. Section 4.2 detailed the comparison and Figure 4.1 outlined each countries'

provisions, including suggestions taken from the Budapest Convention on Cybercrime and also the Commonwealth Model Law.

According to Table 4.1, Samoa has the most provisions while Tonga and the Kiribati has the least. The review also showed that Tonga and Fiji both have Acts dedicated to computer and computer related crimes also known as cybercrime. Samoa's provisions for cybercrime is included in the *Samoa Crimes Act 2013* and, Kiribati's provisions for *Computer Misuse* are included in its *Telecommunications Act 2004.*

It is evident that the selected countries' cybercrime laws all align with international best practices and guidelines however, some countries' provisions are broad which will be hard to interpret. Cybercrime continues to adjust as technology continues to change and legal frameworks are required to adapt accordingly.

Chapter 5

The Cybercrime Legislation in New Zealand

5.0 INTRODUCTION

Chapter 4 provides an evaluation of Cyber Legislation in Tonga. This chapter (5) is designed to evaluate the current status of Cyber Legislation in New Zealand, a more-developed country. The outcome of the evaluation will be used to compare with Tonga in order to determine the readiness of the legislative framework in Tonga and its approach to prosecute Cybercrime and Cyber related crimes.

The New Zealand Cybercrime and Cyber related crimes is included in the New Zealand Crimes Act 1961. Sections 248 to 254, Part 10 of the Crimes Act contains the provisions to prosecute *"Crimes involving computers"*. Section 248 provides the Interpretation of the terms used in the crimes involving computers section. Section 249 contains the provisions to criminalise *"accessing computer system for dishonest purpose"*. *"Damaging or interfering with computer system"* is the provision provided in the section 250.

Section 251 is the provision to prosecute crimes involving *"making, selling, or distributing or possessing software for committing crime".* Section 252 is the provision to prosecute crimes that involves *"accessing computer system without authorisation".* Sections 253 and 254 outline the provisions to criminalise crimes involving *"qualified exemption to access without authorisation offence for New Zealand Security Intelligence Service"* and *"Qualified exemption to access without authorisation offence for Government Communications Security Bureau"* however, they are both marked as being *"Repealed"*.

This chapter is designed to help take a closer look into how New Zealand deals with Cybercrime. All the sections and sub-sections in this chapter will cover and mainly focus on the Part 10 sections 248 to 254 of the New Zealand Crimes Act 1961. Therefore, the next section will start by looking into the development of the *"Crimes involving computers"* section of the Crimes Act.

5.1 THE CRIMES INVOLVING COMPUTERS

The New Zealand Crimes Act 1961 in particular has a long history which can be dated back to the Criminal Code 1893 (NZLII, 2020). As such, there is no specific Act for Cybercrime. Instead, a subsection named *Crimes involving computers* was developed and included as sections 248 to 254 of Part 10 of the Crimes Act. Consequently, there were several amendments nonetheless, three of those were in Part 10, sections 248 to 254.

According to the Crimes Act 1961 under the *Crimes involving computers* section it stated that, the heading replaced by section 15 of the Crimes Amendment Act 2003 (No 39) on the 1 October. This means that the principal Act has been amended by repealing Part 10. For instance, under section 248 – Interpretation for terms used in section and sections 249 to 252 has now become section and sections 249 and 250 under the Amendment Act 2003 (No 39).

Section 248 was again amended in 2011 by section 4(2) of the Crimes Amendment Act 2011 (No 29). Additionally, the interpretation for the term "authorisation" was inserted back into section 248 with the following definition - "***authorisation*** - includes an authorisation conferred on a person by or under an enactment or a rule of law, or by an order of a court or judicial process". Furthermore, sections 249 and 250 of the 2003 amendment were omitted and substituted by sections 249 to 252 in the 2011 amendment.

The following sections are designed to review the provisions offered by the New Zealand Crimes Act 1961 to criminalise cybercrime and cyber related crimes.

5.1.1 Section 248 - Interpretation

Sections 249 to 252 consist of the provisions to criminalise crimes involving computers. To better understand these provisions, section 248 defines the terms used.

a) Access

   Access is defined as -

   "in relation to any computer system, means instruct, communicate with, store data in, receive data from, or otherwise make use of any of the resources of the computer system"

The Commonwealth Model Law and the Model Law for the South Pacific, the model laws that were employed in the development of the Tonga Computer Crimes Act does not provide any definition for the term "Access". Instead, they both define the term "Illegal Access". The definition provided above mainly focuses on access to computer system in terms of communication such as receiving or transmitting data, storing data, or using any other resources of a computer system. Sub-section "C" of this section provides a definition for the term "Computer system".

b) Authorisation

Authorisation is defined as -

"includes an authorisation conferred on a person by or under an enactment or a rule of law, or by an order of a court or judicial process"

The definition provided for "authorisation" is very broad and unclear. Assuming that this definition is to clarify and aid with criminalising a person accessing a computer or computer system without authorisation. It is evident that the main issue is to understand the term "authorisation". According to one of the Department of Justice's publications, there is always a distinction to be made between insider and outsider access. *"Insider"* can be referred to an employee. An employee has provided with access credentials such as username and password. Insiders usually get prosecuted for exceeding their access rights while outsiders get prosecuted for unauthorised or illegal access (Jarrett et al., 2010, p. 6).

c) Computer system

A computer system is defined in two parts, first part concerns with the meaning of the term computer system. Second part deals with what parts to include in the items defined in the first part.

1. means -
    i. a computer; or
    ii. 2 or more interconnected computers; or
    iii. any communication links between computers or to remote terminals or another device; or

iv. 2 or more interconnected computers combined with any communication links between computers or to remote terminals or any other device; and

2. includes any part of the items described in paragraph (a) and all related input, output, processing, storage, software, or communication facilities, and stored data.

The New Zealand Crimes Act definition is different from the definition provided by the Model Laws adopted by countries in the pacific to develop their cybercrime statutes as it is showing in table 5.1.

Table 5.1: Four Cybercrime related Model Laws

Commonwealth Model Law on Computer and Computer Related Crime	Cyber Legislation: A Model Law for the South Pacific	HIPCAR Model Legislative Text on Cybercrime	4th Draft EGRIP Electronic Crimes Bill
"computer system" means a device or a group of inter-connected or related devices, including the internet, one or more of which, pursuant to a program, performs automatic processing of data or any other function;	"computer system" means a device or a group of inter-connected or related devices, including the Internet, one or more of which, pursuant to a programme, performs automatic processing of data or any other function;	Computer system (or information system) means a device or a group of inter-connected or related devices, including the Internet, one or more of which, pursuant to a program, performs automatic processing of data or any other function.	"electronic system" means an electronic device or a group of interconnected or related devices, one or more of which, pursuant to an electronic program, performs automatic processing of data and includes an electronic storage medium;

The four model laws shown in table 5.1 are very similar with very minor variances however, not included in table 5.1 is how the Convention on Cybercrime (CoC) define the term "Computer System". Chapter I, Article 1(a) defines the term "computer system" as, *any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data.* This definition highlights its objective which is to protect a computer system or related devices that have capabilities of processing data.

According to the New Zealand Law Commission Report 54 on Computer Misuse, the Crimes Bill 1989 provided definitions for the following terms – Access, Computer, Computer network, Computer programme, Computer software,

Computer system (Baragwanath et al., 1999, p. 25). It seems that the Part 10 sections 248 of the Crimes Act have omitted most of the terms from its definition. The Crimes Bill defined the term "Computer system" as *a set of related computer equipment, devices, and software, whether connected or unconnected to one another.* The Crimes Act always make reference to these terms such as Computer, Computer program, Computer devices, and it is very important to clearly define these terms in the Act.

5.1.2 Section 249 - Accessing Computer System for Dishonest Purpose

Section 249(1) outlined the penalties applied to any offences defined in this section. Anyone who directly or indirectly access a computer system for dishonest purpose is liable to a term not exceeding 7 years imprisonment. These criminal acts are mostly financially driven or other forms of revenue, and section 249 of the NZ Crimes Act is designed to prosecute them. Types of criminal activities include stalking, spamming, identity theft, phishing, online extortion, fraud, just to name a few.

For an example, an unhappy employee that is looking to take revenge on his/her employer deletes some files from the organisation's computer system. Obviously, the employee can do that but only to the files allowed by his access permission. If this is the case then, the employee will most likely to be liable for a simple loss of those files under this provision as intentions cannot be proven. Unless, the loss of those files results in the loss of reputation, business, money, etc for the employer, this provision does not prosecute. In addition, if the employee must access those files outside his/her authority and without authorisation then it is likely that the employee will be found guilty in court (Trenwith, 2004, p. 101).

Section 249(2) outlines the penalties applied to someone who accesses a computer system with intent and/or without claim of right, meaning no lawful justification and if found guilty, then liable for imprisonment for a period of not more than 5 years. This penalty applies to the use of a computer system without authorisation to obtain any service or privilege, to obtain any property, gain monetary advantage or benefit.

This section is also designed to prosecute someone who uses a computer system to cause any kind of loss to any other person. It is designed to include coverage of more traditional crimes which can also be committed in the cyber world by using electronic devices such as a computer for instance, burglary, breaking into a property, and so on (Hilbert, 2013, p. 15). According to the New Zealand Police, cyber-enabled crimes may include online scams, threats to the life or public safety, and possessing or distributing objectionable material such as child pornography (New Zealand Police, 2020).

5.1.3 Section 250 - Damaging or Interfering with Computer System

Section 250 is designed to prosecute someone who damages or interferes with a computer system. According to Section 250(1), if found guilty under this provision, the penalty is imprisonment for a term not exceeding 10 years. This penalty applies to anyone who intentionally or recklessly destroys, damages, or alters any computer system. Under Section 250(2), the penalty is imprisonment for a term not exceeding 7 years for someone who acts intentionally or recklessly without authorisation. As a result, the action damages, deletes, modifies, interferes with or ruins any data or program and/or deny service to legitimate users.

Provisions provided under section 250 were designed to protect the access of legitimate users and criminalise any intentional obstruction of legitimate users of a computer system. Additionally, the provision will protect the integrity of the computer system as well (ICB4PAC, 2013, p. 35).

The Article 5 of the Budapest Convention on Cybercrime focusses on system interference. Article 5 recommends that member parties should implement all necessary legislation to ascertain criminal offences committed intentionally such as obstructing a computer system's functions without lawful authorisation by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data (Convention on Cybercrime, 2001, p. 5). The criminal's lack of access rights or authorisation is a significant component of this offence (Watson, 2015, p. 6).

However, the motive is also attached to the unlawful access in this provision whether the action was intentional or reckless. According to the New Zealand

Police website, regardless of the criminal's objective or reason, it may include computer intrusion, attack on a computer system, and malicious software (New Zealand Police, 2020). The computer systems provide cyber criminals with a more complex opportunities to commit traditional crimes in a non-traditional way (Manual, 2001, p. 5).

The philosophies of illegal and dishonest intentions, authorisations, highlight the fact that it is important for the criminal law to be able to prosecute cybercrimes. In addition, it must be able to differentiate between intentional and non-intentional misuse of a computer system, careless and intentional misuse of a computer system, unauthorised or illegal access to a computer system. Nonetheless, the United Nations acknowledged that the criminal justice systems and laws cannot keep up with technological changes (Manual, 2001, p. 3).

Section 9 of the Commonwealth Model Law on Computer and Computer Related Crime has a provision for *Interfering with computer system*. This provision is designed to criminalise a person who wilfully or recklessly (a) hinders or interferes with the functioning of a computer system or (b) hinders or interferes with legitimate user of the computer system. The penalty under this provision is a fine or a period not more than 1-year imprisonment or can be both (Commonwealth Secretariat, 2017, p. 7).

Similarly, the provisions defined in the section 7(1) of the Cyber Legislation: A Model Law for the South Pacific are very similar to the section 9 of the Commonwealth Model Law on Computer and Computer Related Crime. In fact, the only difference is in the penalties, The Commonwealth model law defines a 1-year imprisonment while the Model Law for the South Pacific allows each party to define their own imprisonment period (Scott, 2007, p. 7).

5.1.4 Section 251

Making, selling, or distributing or possessing software for committing crime

Section 251(1) stated that the penalty under this provision is imprisonment for a term not exceeding 2 years. The provision applies to anyone who offers, exposes, sells, supplies, possesses software or information that will allow someone to access a computer system without authorisation. For instance, an unlawful access to a

computer system and obtain confidential information such as a list of usernames and passwords.

Similar provision applied by the U.S. Department of Justice's criminal investigation in the 1999 prosecution of David Smith. In late March 1999, the Melissa virus infected millions of computers. Upon investigation, a call record obtained from the ISP showed that the virus was launched from David Smith's apartment (Turrini & Ghosh, 2011, p. 5). Nonetheless, some progress has been made in this area, and in this work, an attempt has also been made to separate the costs of cyber-enabled crimes. Turrini and Ghosh (2011) explained further that, the most challenging part of prosecuting David Smith is assessing and estimating the economic damage caused by the Melissa virus. This is a crucial part of the investigation because, the penalty needs to correspond with the damages (p. 3).

According to the Home Office Research Report 75, estimating the costs of cybercrime is challenging (McGuire & Dowling, 2013, p. 24). This is due to the nature of cybercrime, and there are various sources of data came from however, data is fragmented and available statistics are not enough. According to Anderson et al., (2013), cybercrime data and statistics seems to suffer from either under-reporting or over-reporting and that depends on who collected them and errors may be intentional or unintentional (p. 267).

Section 251(2) states that the penalty is imprisonment for a term not exceeding 2 years. This provision is designed to prosecute someone who obtains any software or information that will allow someone to access a computer system without authorisation. Furthermore, it will apply to someone who intends to use the software or that information to commit an offence. Section 251(2) is very similar to the provisions in 251(1). The difference is that unlike (2)(b), this provision criminalises the use of software or other information to commit an offence.

5.1.5 Section 252 - Accessing computer system without authorisation

Section 252(1) describes the penalty under this provision which is imprisonment for a term not exceeding 2 years. This penalty applies to someone who intentionally and knowingly accesses any computer system without authorisation, 252(2) is designed to help clarify 252(1). Sub-section (1) does not apply to a legitimate user

who accesses the computer system for a reason other than what he/she is authorised for. Section 252(3) repealed, on 13 July 2011, by section 5 of the Crimes Amendment Act 2011 (2011 No 29).

The Commonwealth Model Law on Computer and Computer Related Crime section 5 has a very simple provision on *"Illegal access"*. Section 5 criminalises illegal access to a computer system. This applies to accesses with no lawful excuses or justifications to commit an offence, and upon conviction, the penalty is imprisonment or a fine or both. According to the Title 1 of the Convention on Cybercrime 2001 suggests that, offences against the confidentiality, integrity and availability of computer data and systems, everyone should adopt such legislative as it is essential to criminalise illegal access to a computer system or computer networks.

The model policy guidelines & legislative texts point out that the current technical solutions to prevent illegal access to a computer system such as firewalls and solutions such as encryptions to be enough to prevent illegal interception of communications. However, experience has shown that legislative measures are also essential and required (HIPCAR, 2012, p. 8).

Section 7 of the Cyber Legislation – A Model Law for the South Pacific describes the provisions to criminalise Illegal access. Section 7(1) explains that a computer is to be treated as a protected computer. This is designed to prosecute someone who commits an offence knowing that the computer system is connected to the security, defence or international relations. Not only that but in connection with identity of a confidential source of information relating to the enforcement of a criminal law. Also, in connection with the critical infrastructure, public safety including essential emergency services.

Section 7(2) describes the penalties that apply to someone who unlawfully accesses a computer system and commits an offence, will be liable upon conviction to imprisonment for a period not exceeding 2 years or monetary fine or both. Penalties under section 7(3) on the other hand applies to someone who accesses a protected computer illegally and commits an offence will be liable upon conviction to imprisonment for a period not exceeding 20 years or monetary fine or both.

The New Zealand Crimes Act does not use the term "protected computer". The term applies to computers used in relations with interstate or foreign commerce and federal government and financial institutions (Jarrett et al., 2010, p. 4). The term protected computer is defined in Section 1030(e)(2) a computer -

> *exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or which is used in or affecting interstate or foreign commerce or communication.*

According to Wang (2016), the term "protected computer" was introduced in the National Information Infrastructure Protection Act (NIIPA) of 1996 to replace the term "federal interest computer". The NIIPA was introduced into law in October 1996 and it was a major revision of the USA's computer crimes law to deal with a wide range of criminal offences that involves a computer or an electronic device (HG.org, 2020).

5.2 CYBER-ENABLED CRIMES

Information and Communication Technologies (ITC) has changed the world we are living in, and the people communicate and conduct daily businesses. Even though ICT technologies make it more effective and efficient but, it also brings new threats and opportunities for criminal activities (Sallavaci, 2017, p. 54). In the process of fighting cybercrime, the government should prioritise having the necessary legal framework in place that fit the purpose (Cornish, Hughes & Livingstone, 2009, p. 13).

The term cybercrime comes into the scene in the late twentieth century and it is used to describe crimes committed in cyberspace (Newman, 2009, p. 551). There are two basic types of cybercrimes: cyber-dependent and cyber-enabled crimes. Cyber-enabled crimes refer to traditional crimes such as fraud, data theft, etc. Cyber-enabled crime employs ICT technologies to maximise its reach and

increase its scale. Cyber-dependent crimes on the other hand, also known as computer related crimes such as distributed denial of service (DDoS) attacks, spreading malicious software, hacking and so on. These types of crimes can only be committed by using ICT technologies (McGuire & Dowling, 2013b, p. 4).

5.2.1 Computer Enabled Online Scams

The crimes involving computers section of the New Zealand Crimes Act did not have a provision to criminalise computer enabled online scams. The London Police and the National Fraud Intelligence Bureau established a national reporting centre known as the Action Fraud (Action Fraud, 2020, p. 1). People can report information regarding frauds and cyber related crimes to the Centre. The Action Fraud Centre reports a number of frauds and that includes account takeover, advance fee frauds, bank card and cheque fraud, charity donation fraud, clairvoyant or psychic scams, click fraud, domain name scams, government agency scams, identity fraud, inheritance fraud, Internet auction fraud, Internet dialler scam, loan scams, mass marketing fraud, online shopping fraud, plastic card, fraud, vehicle matching scams, West African or 419 scam, and work from home scams. These are some of the frauds reported to the centre but not all (Owen, Noble & Speed, 2017, p. 214).

According to Pouryousefi and Frooman (2019, p. 3), terms such as fraud, con, and swindle are often used interchangeably. This includes product scams and lottery draw frauds to fraudulent auction sites. It is evident that the Internet auction houses have done nothing to stop Internet auction fraud. Chua and Wareham (2008, p. 306) suggest that governments should regulate auction sites to help reduce Internet auction frauds.

The crimes involving computers section does not have any provisions to criminalise computer enabled online scams. However, sections 255 to 265 of the NZ Crimes Act have a comprehensive and detailed provisions to criminalise forgery and counterfeiting.

5.2.2 Section 255 – Interpretation

Section 255 runs through the definition of terms used in sections 256 and 263. There are only two terms defined in section 255 – bank note and false document. Bank note refers to any negotiable instrument used as currency issued by the Reserve Bank of New Zealand or any bank in other countries or other authority authorised by law to issue notes.

False document means a document made by a fictitious person, claims to be made on behalf of a person either without authorisation or a fictitious person. Or, altered in any way and claims to have done on behalf of someone with his/her authorisation or on behalf of a fictitious person. Or, reproduce any document and then claim to have been made on behalf of a person who did not make it or authorise its making. Or, made by a person or to have authorised by that person with the intention to pass as being made by someone else and not the person who made it.

5.2.3 Section 256 – Forgery

Sub-section 1 is designed to criminalise and prosecute a person who makes a false document intending to gain something from monetary benefits to any property or privilege and service. The punishment that applies to someone who is liable for such criminal actions is imprisonment for a term not exceeding 10 years. Imprisonment for a term not exceeding 3 years defined in sub-section 2 applies to a person who is liable for making dales document knowingly with intention to use in New Zealand or somewhere else.

Sub-section 3 and 4 defines the conditions as in (3), the forgery is complete the time the forged document is made with the intent. Sub-section (4) explains that forgery is complete regardless if the forged document is complete or claim it to be binding or legally sufficient and intended to be genuine. Not more than three years imprisonment for someone who without reasonable excuse or distribute false document knowingly and with intentions to use in New Zealand or elsewhere and genuine.

5.2.4 Sections on Forged Documents

This provision is concerned with the use of forged documents to gain monetary benefits, properties, privileges or services. Or use the forged documents or cause someone to act upon it as if it were genuine. Upon conviction, the person is liable for a maximum of not more than 10 years imprisonment. Sub-section 2 is concerned with forged documents made outside New Zealand is to be seen and treated as if it was made in New Zealand.

Section 258 is designed to deal with altering, concealing, destroying, or reproducing documents with intent to deceive. Imprisonment for a maximum of 10 years for someone who is liable for obtaining by fraudulence property, monetary advantage, or cause damage to someone else. Sub-section (1)(a) concerns the destruction of documents, altering and concealing; (1)(b) causing a document to be made or reproducing any other document.

Sub-section (2) is concerned with an offence against sub-section (1). According to sub-section (2), the offence is complete when the alteration is made or the document is made or destroyed. Sub-section (3) defines a penalty of imprisonment of not more than three years upon conviction for whoever sells, distributes any documents (a) that has been altered, concealed or been reproduced. (b) the document was dealt with in the manner specified in paragraph (a) with intent to gain monetary benefit, service, privilege, or cause loss to someone else.

Sub-section 259 is designed to criminalise the intentional use of altered or reproduced document to deceive. Paragraph 1 defined the penalty applied under this provision, upon conviction, imprisonment for not more than 10 years for someone who is aware of any document to have been made or altered with the intent as it is referred to in section 258.

Sub-section 260 is designed to prosecute false accounting. The penalty is imprisonment for a term not exceeding 10 years for someone who intentionally obtains, by way of deceiving, any privilege, property, monetary advantage, or to deceive or cause loss to someone else. Paragraph (a) criminalises the make or causes the make, or in agreement in the making of, any false entry or use for accounting purposes. Paragraph (b) criminalises the omission or in agreement to omit particular information from such book or account. Paragraph (c) criminalises the making of

any transfer of any interest in a stock, debenture, or debt in someone else's name other than the owner of that interest.

5.2.5 Sections on Counterfeiting

Section 261 criminalises counterfeiting public seals and upon conviction, the penalty is imprisonment for a term not more than 10 years. This applies to someone who (a) unlawfully making or counterfeiting any seal, or stamp, or impressions of a seal or stamp in use in New Zealand or any other country knowing it is a counterfeit. Section 262 criminalises counterfeiting of corporate seals and upon conviction, the penalty is imprisonment for a term not exceeding five years.

This provision applies to unlawfully making and counterfeiting of any seal or stamp; or impressions of any such seal or stamp; knowingly uses of any such seal, stamp or such impressions to be counterfeit in New Zealand or any other country by any corporate body or company other than those mentioned in section 261. Section 263 criminalises the possession of forged bank notes. This applies to someone who knowingly purchases, or receives, or is in possession of, or in control of any forged bank note to be forged. Upon conviction, the penalty is imprisonment for a term not exceeding seven years.

Section 264 - paper or implements for forgery. This provision is designed to prosecute someone who is intentionally in possession or in control of anything that can create forged documents. The penalty upon conviction under this provision is imprisonment for a term not exceeding ten years. Sub-section 265 is the provision to criminalise imitating authorised or customary marks. Under sub-section 265, there are two paragraphs (1) and (2), and paragraph (1) contains two sub-paragraphs (a) and (b).

Paragraph (1) defines the penalty which is imprisonment for a term not exceeding five years for someone who fraudulently counterfeits or copies any mark, word, or description. That is, impressing or making, writing upon or attaching to an item of property, a mark or a word, or a description that has been recognised, examined and certified to be of a particular quality by any particular officer. Sub-section (2) applies if the officer referred to in sub-section (1) is authorised by law or not.

Even though sections 249 to 252 on “crimes involving computers” do not include provisions for fraudulent act. Nonetheless, sections 256 to 263 of the *New Zealand Crimes Act* describe the provisions to criminalise forgery and counterfeiting. Although those provisions do not specify involvement of computer or other electronic devices but those fraudulent acts can be committed by computers.

The Commonwealth Model Law on Computer and Computer Related Crime sections 5 to 10 consists of practical criminal law. Offences such as illegal access, interfering with a computer system, and illegal interception of data even, child pornography using a computer system. Yet, the Model Law does not cover computer-related forgery or fraud.

Article 7 of the Budapest Convention on Cybercrime defines the convention’s suggestion in relation to computer-related forgery. The convention suggests that each country should adopt such legislative necessary to establish as criminal offences when committed intentionally and without authorisation, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data. It requires intent to defraud before criminal liability attaches (Convention on Cybercrime, 2001, p. 6).

5.3 DISCUSSION

There is no specific Act designed to criminalise and prosecute cyber and computer related crimes in New Zealand. Sections 249 to 252 of Part 10 of the *New Zealand Crime Act 1961* outlined the provisions to criminalise computer related offences. Section 249 is concerned with “accessing computer system for dishonest purpose” offence. It is going to be a challenge to try to determine the scope of section 249 (Mayhew & Reilly, 2007, p. 18). The Privacy Commissioner (2000, p. 10) explained that access, with or without authorisation, does not really matter but the intention counts.

An access can be authorised or unauthorised however, accessing a computer system - or part of - with intention to commit a crime is punishable under section 249 and 252. Unauthorised access is commonly referred to as “hacking”, a method used by an outsider to work around the security control put in place to gain access to a computer system. There are also the authorised access users, these are known

as an insider attack, and it is a significant threat to the confidentiality, integrity, and availability of the data. According to the U.S. Secret Service report, 34% are insider attacks while 37% are outsider attacks (Mathew et al., 2010, p. 383). Insider threats are especially hard to detect and prevent since they have authorised access to the computer system (Kammüller, Nurse & Probst, 2016, p. 234).

Damaging or interfering with computer system is the provision to criminalise intentional damaging, altering of any computer system knowing that it may result in a danger to life according to the *NZ Crimes Act, part 10 section 250*. Furthermore, deleting, damaging, modifying both data and software in any computer system is included. Section 251 is concerned with the "making, selling, or distributing or possessing software for committing crime" *NZ Crimes Act, part 10 section 251.* The provision can be used to prosecute anyone who supplies, distributes, and/or possesses any software or information that would enable someone to access a computer system without authorisation.

Baragwanath et al., (1999, p. 11) pointed out that the legislation deals with four various types of unauthorised conducts;

- unauthorised access and use of a computer system for dishonest purpose
- unauthorised and intentionally damaging, deleting, modifying, or interfering with data or computer systems
- unauthorised making, selling, or distributing or possessing software for committing crime
- unauthorised access to a computer system

Looking at the New Zealand context, the question is whether the current legislation is enough, and the answer is simple, "No". There is a real need for a cyber-specific law to create consistency, harmony, and confidence among all legislators and legal experts in dealing with cyber criminals.

The current provisions are focussing on unauthorised access and intentional actions to cause damage or for personal gain. These are very broad and can be confusing, for instance, in a criminal investigation, the unauthorised access will have to be established and proved first then, prove the intention and finally prove the damages. When it comes to "unauthorised access", there can be a lot to take into

consideration such as, the approach employed, communication media, data location, user access privilege, and so on.

These provisions also included actions that interfere or interrupt with normal operations of computers, computer programs, computer systems, and computer networks. In terms of damages, there are various ways that can cause damage to the information systems. For instance, there are different types of malware that can be used to destroy or modify the data remotely and can cause damages as well to either or both information and communication system resources, program, and/or data.

5.4 CONCLUSION

This chapter focusses on reviewing the New Zealand legal provisions to criminalise criminal acts in relation to computers and computer related offences. It is evident that the provisions described in this chapter are not sufficient to prosecute all computer related offences. Crimes involving computers consists of only four provisions, sections 249 to 252.

Section 249 is concerned with accessing a computer system for dishonest purpose. Section 250 is concerned with damaging or interfering with computer system. Section 251 is concerned with making, selling, or distributing, or possessing software for committing crime. Section 252 is concerned with unauthorised access to a computer system.

Part 2 of the Commonwealth model law on computer and computer related crime has six provisions yet none on computer related forgery or fraud. This chapter includes suggestion found in article 7 of the Budapest convention on cybercrime in relation to computer related forgery. The convention suggested that for each party to adopt such legislative as it is necessary to build a criminal offence.

Chapter 6

Comparison and Conclusion

6.0 INTRODUCTION

The previous chapters were designed to analyse and review first; the relevant literature available in the body of knowledge; second, analyse and compare Tonga's legislative framework of Kiribati, Fiji, and Samoa in relation to cybercrime. In this chapter, the outcome of the Tonga, Kiribati, Fiji, and Samoa (TKFS) comparison conducted in chapter 4 will be referred to as "TKFS". This chapter aims to take the TKFS outcome from previous chapters and compare with the New Zealand's legislative framework for cybercrime. At the end of this chapter, the main research question and sub-questions will be answered.

Furthermore, based on the comparison, there are four aspects to consider based on the viewpoints of the research questions. These viewpoints are:

a) the readiness of Tonga's legislative framework to combat cybercrime.
b) the weaknesses of the current legal system in Tonga.

6.1 THE COMPARISON

This study is based only on a few pre-selected legal systems - Tonga, Kiribati, Fiji, Samoa, and New Zealand. The four neighbouring countries in the south pacific were chosen because, they are still in their developing stages in terms of information communication technologies. The New Zealand legal system, a more developed country, is taken as the most suitable model for comparison. The objective of the study is to determine the readiness of Tonga's legal framework to combat cybercrime and identify area for improvements.

6.1.1 Cybercrime Definition Issues

A workshop dedicated to the issues of crimes related to computer systems in the United Nation's 10th Congress on the Prevention of Crime and Treatment of Offenders divided cybercrime into the following two categories:

(a) computer crime means unlawful acts using an electronic device targeting the security of a computer system and the data processed by it (United Nation, 2014).
(b) in a more comprehensive sense – computer related crime means, any unlawful act by way of, or in relation to a computer system including illegal possession, or distributing information using a computer system (United Nation, 2014).

Kshetri (2006, p. 33) provided a broad approach to the definition of the term "cybercrime" as a crime that uses a computer network to commit an offence such as an attack on critical infrastructure, or online fraud, or online money laundering, including the use of Internet communication technologies to further traditional crimes, and cyberextortions. The most distinguished features of cybercrime include novelty, technology and knowledge intensive, and rapid proliferation (Kshetri, 2009, p. 141).

Cybercrime is also known by various other terms such as technology enabled crime, electronic crime or e-crime, or online crime. According to New Zealand Police (2020), cybercrime is a criminal act committed by using Information Communication Technologies where the computer or computer network is the target of the offence such as computer intrusion, attack on a computer system, or malicious software (Gercke, 2016, p. 28).

It is evident in the literature that cybercrime is currently an umbrella term used to cover a wide variety of computer related criminal actions and it is too complicated to develop a typology or classification system for cybercrime (Gercke, 2016, p. 29). However, according to Gordon and Ford (2006, p. 13), there is no single universal term to apply to the tools and software that are utilised in committing computer related crimes.

The Council of Europe's Convention on Cybercrime listed a number of various offences that are referred to by the term "cybercrime". This ranges from offences targeting the confidentiality, integrity and availability of computer data to, copyright and right related violations (Weber, 2012, p. 431). There are several aspects to cybercrime that are very similar to traditional crimes. Krone (2005, p. 2) pointed out that the current definitions of the term "cybercrime" are changing according to experiences and observations of observers and the victims.

Nonetheless, it is believed that the existing definitions of cybercrime can be problematic, it tends to be explanatory and not grounded on a theoretical framework. A theoretical framework will help to define the key concepts of cybercrime and provide common descriptions of their relationships. Dealing with criminals in cyberspace and crimes committed in various jurisdictions is still a major issue to consider. The framework can also aid legislators and policy makers to develop a legal definition which is meaningful at least from the technical viewpoint (Gordon & Ford, 2006, p. 14).

6.2 THE SCOPE OF CYBERCRIME OFFENCES

The cyber and computer related legislations of the chosen countries are all different in terms of the targeted offences. However, it is evident that they are aiming to prevent attacks, an intrusion, interference, damages, illegal use, unauthorised access, and illegal interception (Guo, 2018, p. 141). All to protect the confidentiality, integrity, and availability of information (Jianglan, 2008, p. 9). Information and data are the most important and critical asset to any organisation, including governments. ICT infrastructures are used to conduct business today and critical information assets are at risk. As a result, the security requirements focus on the confidentiality, integrity, and availability of the information (Alberts & Dorofee, 2002, p. 113).

As a result, legislators for various governments around the world are implementing laws on cybercrime as part of an effort to protect and prevent vital and critical assets from criminal acts such as deleting, modifying, manipulating, obstructing and denying access to legitimate users (Reddy & Reddy, 2014, p. 1). A clear statutory guiding principle is crucial, also simplify international relations and be able to protect, prevent and prosecute cybercrime (Yilma, 2017, p. 254). The application of law is an important requirement in the design of a legal framework. In addition, it is also a critical feature of legal philosophy and that will help in identifying the value, function, and nature of each legislation.

The purpose of this study as mentioned earlier in the previous chapters, is to review cybercrime laws or computer related crime laws of chosen countries in

the South Pacific. This part of the study has been done in chapter 4 which identified similarities and differences in their cybercrime legislations. Figure 6.1 is showing

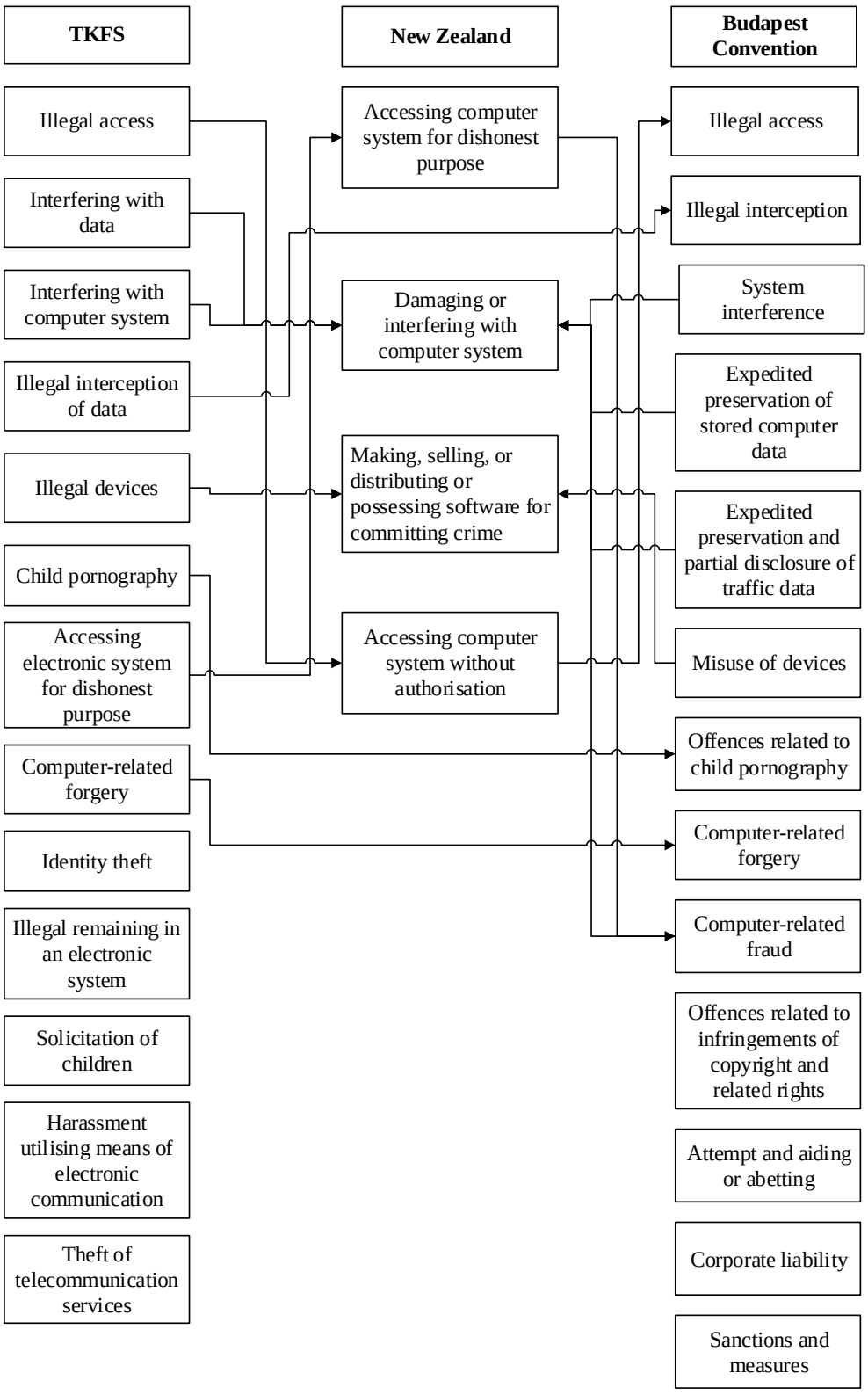

Figure 6.1: Comparing 3 Countries, NZ & CoC

the TKFS reviews and comparisons. New Zealand is considered a well-developed country in the South Pacific. Figure 6.1 is taking the TKFS and comparing it with the cybercrime legislation in New Zealand. According to the New Zealand Government (2020, p. 1), the New Zealand Government is considering joining the Budapest Convention on Cybercrime.

Therefore, the provisions provided by the articles in the *Convention on Cybercrime, Nov, 23, 2001, E.T.S. 185, Budapest, 25* is included in this comparison as shown in Figure 6.1. The New Zealand *Crimes Involving Computers* is a section of the *Part 10 - Crimes against rights of property* of the New Zealand *Crime Act 1961* that contains the provisions to criminalise cybercrimes in New Zealand. The New Zealand *Crimes Involving Computers* consists of 7 sections – 248 to 254. Section 248 provides interpretations of the technical terms used by the *Crimes Involving Computers* however, sections 253 and 254 had been repealed. Therefore, only sections 249 to 252 carry the provisions to criminalise cybercrimes in New Zealand.

Figure 6.1 shows the TKFS in comparison against the sections 249 to 252 of the New Zealand *Crimes Involving Computers* and also the *Convention on Cybercrime, Nov, 23, 2001, E.T.S. 185, Budapest, 25*. Table 6.1 shows the number of provisions provided for by each partakers.

Table 6.1: Number of offences from each partakers

TKFS	New Zealand	Budapest CoC
13	4	13

The 13 offences criminalised by the TKFS is a result of the comparisons in chapter 4, the similarities and differences were combined into the TKFS. Five of the TKFS 13 provisions mapped out to the New Zealand 4 provisions. The New Zealand *Crimes Involving Computers* combines interferences or damages to computer systems and interferences or damages to computer data offences into a single provision. The TKFS divided the same provision into 2, “interfering with data” and “interfering with computer system”.

However, the Budapest Convention believed that in order to successfully combat cybercrimes, it is vital for the legislative framework to be specific. For that

reason, the Budapest Convention suggested that such provision be divided into 4 different offences "system interference", "computer-related fraud", "expedited preservation of stored computer data", and "expedited preservation and partial disclosure of traffic data". Figure 6.1 also showed that both the TKFS and the Budapest CoC has a provision for "illegal interception of data" while the NZ *Crimes Involving Computers* does not.

Part 9A of the New Zealand *Crime Act 1961* is for "crimes against personal privacy". Part 9A has provisions to criminalise the use of interception devices, the disclosure of private communications that was intercepted unlawfully as well as the supply and distribution of interception devices. It is evident that Part 9A focusses on prohibiting the use of interception device to illegally intercept private communications. In addition, it also prohibits disclosing the intercepted communication or part of it.

New Zealand has a very comprehensive cybersecurity strategy published in 2015. This indicates the government's commitment to make sure that its citizens are safe, resilient and prosperous online. Figure 6.2 shows 4 interconnecting goals of the New Zealand cybersecurity strategy to set up a secure, resilient and prosperous cyberspace for New Zealand.

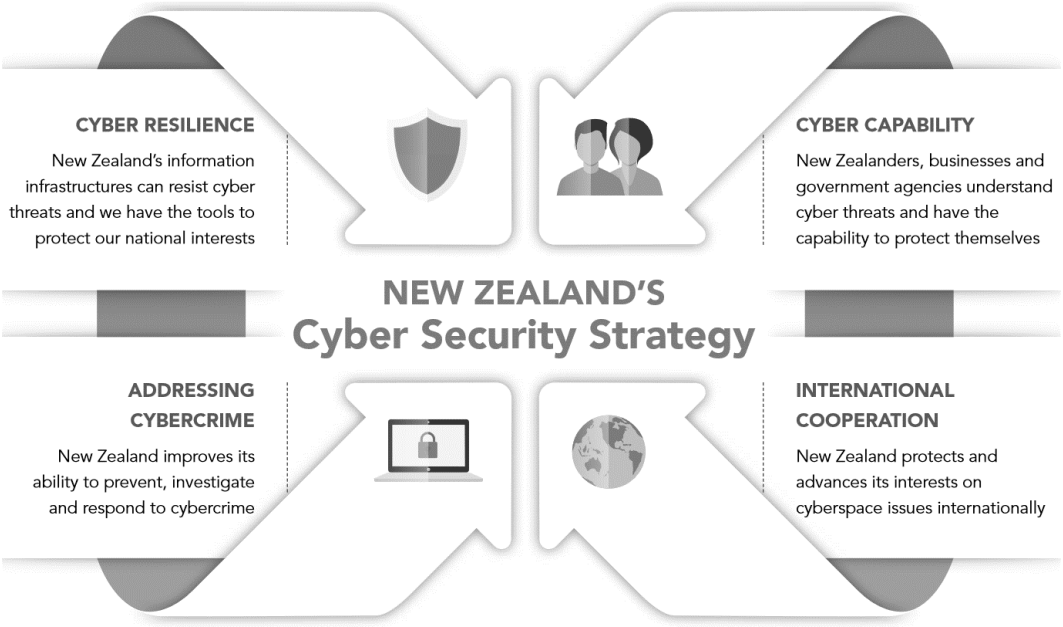

Figure 6.2: NZ Cyber Security Strategy (NZ Government, 2015, p. 3).

The NZ Cyber Security Strategy helps the government familiarise themselves with issues, challenges, values, and philosophies of cybercrime. This approach is vital and essential in developing the most appropriate response to cybercrime. Additionally, it will help to facilitate preventative measures and minimise risks and provide New Zealanders with means to protect themselves in cyberspace. According to the NZ Government (2015, p. 5), 83% of the people in NZ has encountered some form of cybercrime.

There are various ways that cybercrime affected its victims, including emotionally and economically. It is quite a challenge to deal and manage cybercrime because of its borderless nature and the unknown character of the Internet. With NZ joining the Budapest CoC, that is going to help in terms of dealing with those challenges more effectively. Not only that but it will help law enforcement agencies in working together with their international counterparts.

6.3 CONCLUSION

This study is designed to review and compare the cybercrime legislations in Tonga and the selected neighbouring countries in the South Pacific – Kiribati, Fiji, and Samoa. As mentioned in section 6.2, the outcome of this review is referred to as TKFS. The TKFS will be taken and compared with the cybercrime related legislation in New Zealand. However, in these reviews and comparisons, the Budapest CoC is also included in the comparison as a reference model. Tonga has signed the CoC and now New Zealand is now considering joining the Budapest CoC. Nonetheless, Fiji and Samoa are not a member, nor have they considered joining. The outcome of this comparison will be used to answer the research questions and inform the recommendation section.

6.3.1 The Research Questions Answered

The main research question for this study is –

"What can be done to ensure the readiness of Tonga's legislative framework to combat cybercrime?"

As mentioned in earlier chapters, the development of the Tonga *Computer Crimes Act* was informed by the Commonwealth Model Law on Computer and Computer

Related Crime. The illustration in figure 4.1 clearly showed that the five offences criminalised by the Tonga *Computer Crimes Act* mapped perfectly to the Commonwealth *Model Law on Computer and Computer Related Crime*.

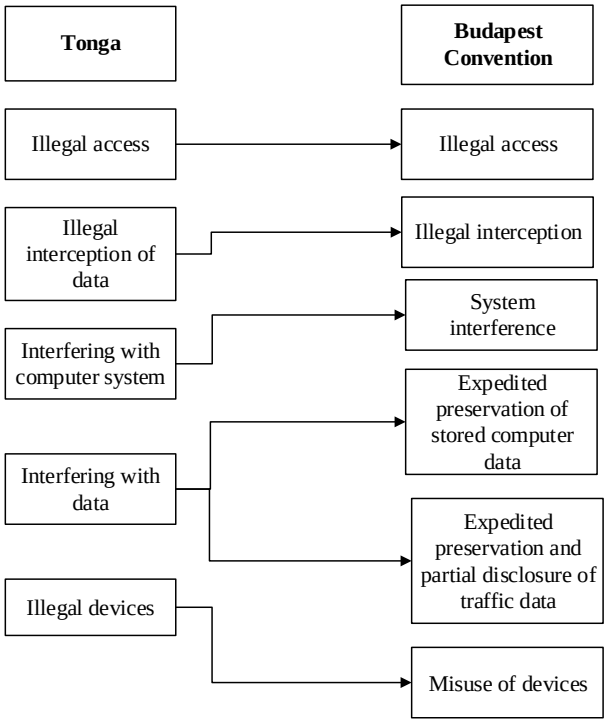

Figure 6.3: Tonga & Budapest CoC Comparison

Figure 6.3 shows the comparison of the Tonga cybercrime legislation and the Budapest CoC. The 5 offences criminalised by the Tonga *Computer Crimes Act* can be mapped to 6 of the Budapest CoC.

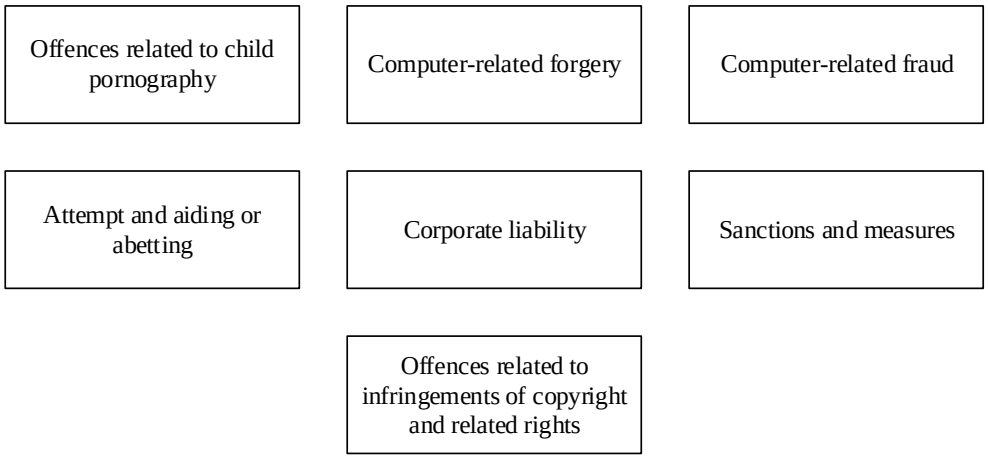

Figure 6.4: Remaining provisions of the Budapest CoC

Figure 6.4 shows the remaining 7 provisions from the Budapest CoC after comparing with the 5 offences in the Tonga *Computer Crimes Act.* To answer the

question - ***What can be done to ensure the readiness of Tonga's legislative framework to combat cybercrime?***

It is evident that the Tonga legislature has done a good enough job so far in terms of aligning itself with the international standard practices and guidelines. It is clear from the TKFS reviews including the *PNG Cybercrime Code Act 2016,* and the comparisons that Tonga's cybercrime legislation is consistent with the Budapest CoC. There are benefits that Tonga will gain from the convention for instance, the convention regularly updated their provisions which will help Tonga legislature to keep up-to-dated with international guidelines. Not only that, but it can also extend and further promote international collaboration. The convention is also capable of assisting Tonga in meeting the requirements for double criminality. Furthermore, the convention can help consolidate and strengthen the domestic legal system and assist as a legal foundation for international collaboration.

Figure 6.4 illustrated the differences and dissimilarities between the Tonga *Computer Crimes Act 2016* and the Budapest CoC. This may be explained due to the differences in economy, culture, tradition, politics, and legal system. The cybercrime legislation in Tonga is very basic however, technological advancement is growing fast. Therefore, the legal measures should be able to adapt accordingly in order to safeguard and protect Tongans while in cyberspace. In addition, the local cyber investigations are based on such legislation. Based on that, the answer to the second half of the main question is a "NO", Tonga's legislative framework is not ready to combat cybercrime.

To answer sub-question 1 - ***What are the weaknesses of the current cybercrime legislation in Tonga?***

The *Computer Crimes Act 2016* is the current cybercrime legislation in Tonga at the time of writing of this document. In addition to the weaknesses outlined and discussed in the previous section, the main weakness is clear, the Tonga *Computer Crimes Act* was developed based on one model law, the Commonwealth Model Law on Computer and Computer Related Crime. Apart from the fact that the offences criminalised by the Commonwealth Model Law are limited, there have been no amendments since 2003. Technology has changed a lot since 2003 therefore, more ways to commit a crime using technology has also changed a lot.

This is clear in the TKFS comparison, Fiji has released a new *Cybercrime Bill 2020* to update its legal defence against cybercrime. Samoa has 14 offences in its *Crimes Involving Electronic Systems*, the Budapest Convention on Cybercrime has 13 offences while, Tonga has only 5 in its *Computer Crimes Act 2016.* It is clear that Tonga needs an amendment to update its *Computer Crimes Act.*

To answer sub-question 2 - *What are the advantages of having a cyber-specific legislation?*

It is clear in the literature that some scholars and researchers in the legal research field argued against implementing cyber-specific laws. Main reason being a cyber-specific law won't be able to keep up with the growth and rapid technology changes. However, cybercrimes are fundamentally different from traditional crimes. They comprise of new classification of crimes or criminal conducts. For that reason, traditional crime law will be inadequate to prosecute cybercrime, more reason to need a cyber-specific legislation to criminalise cyber wrongdoings.

Computer crimes in New Zealand is responsible for a huge financial loss to individuals, businesses, and government. According to CERT NZ, cybercrimes cost 1.7 million dollars from January to March, and up to 6.5 million from April to June 2019 (Pope, 2019, p. 1). As a result, an involuntary cost is taken up by the victims in terms of buying new and updating security measures in order to safeguard themselves and protect their assets from cyber-attacks. Additionally, any attacks on privacy and security of their online activities can also have an impact on reputation, identity, and finances.

The main challenge with cybercrime is that it can be committed across international boundaries, this can be easily managed and controlled by legislation (Tarter, 2017, p. 215). As a result, a good and comprehensive national legislation will help reduce cybercrimes and cut expenses at the same time. International body such as Budapest Convention is referred to as the cornerstone of international legal framework for combating cybercrime.

In the discussion provided in pages 75 & 76 highlighted the importance of having a cyber-specific legislation. The New Zealand Crimes Involving Computers is only a part of the New Zealand *Crime Act 1961*. It combines interferences or damages to computer systems and interferences or damages to computer data

offences into a single provision. There is a real need for a cyber-specific law to create consistency, harmony, and confidence among all legislators and legal experts in dealing with cyber criminals. On page 79, the Budapest Convention believed that in order to successfully combat cybercrimes, it is vital for the legislative framework to be specific.

There are four various categories of offences that the Budapest Convention provides. That is; offences against the confidentiality, integrity and availability of computer data and systems; computer-related offences; content-related offences; and criminal copyright infringement (Luong, 2019, p. 702). The main purpose of cybercrime legislation is to offer similar legal protection to computer data and computer systems (Schjolberg & Hubbard, 2005, p. 12).

To answer sub-question 3 - *Is the legal system in Tonga ready for cybercrime?*

The legal system of Tonga originated from the Constitution approved by His Majesty King George Tupou I on November 4th, 1875. The Constitution also pointed out that the common law in England can be applied in Tonga when no Tongan statute applies. This part is also acknowledged in the Constitution.

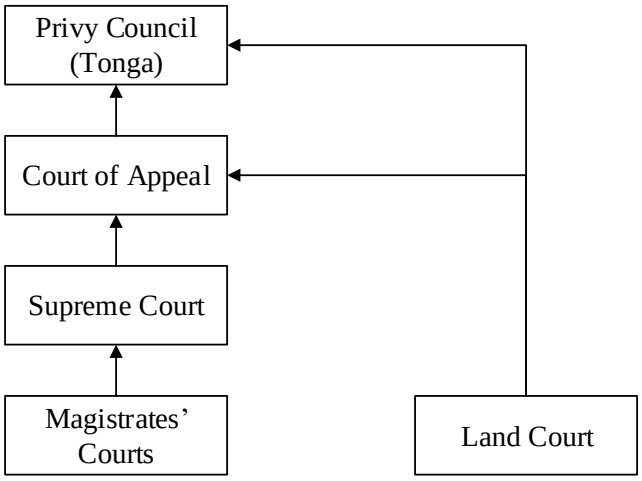

Figure 6.5: Tonga Courts System

As mentioned above, the foundation of the legal system in Tonga is the Common law. The British has an influenced in Tonga since the 19th century, around the same time the Wesleyan missionaries arrived in Tonga. Legal systems that are based on the Common law, their heritage rooted in Britain. According to Jaeger and Hök

(2010, p. 1) this is different from a legal system based in Civil law however, with time, the two legal systems have developed their own customs and characters.

Security in cyberspace has always been the main concern amongst the security experts and researchers around the world. Cybercrimes are criminal offences committed in cyberspace with the help of computers, computer systems, and other electronic devices. According to Li (2008, p. 53), this begins to raise questions whether the existing legal system is capable of preventing and dissuading cybercrimes.

According to the NZ Government (2015, p. 5), as technology rapidly changes, the risks and threat level grows accordingly. A better understanding of what is necessary to allow the system to deal effectively with cybercrime. With regards to the readiness of the legal system of Tonga to combat cybercrime, the answer is "NO". The legal system in Tonga required legislative reforms and further amendments to the existing *Computer Crimes Act 2016* to ensure that the legal framework enables the necessary and effective response to cybercrime.

6.3.2 Recommendations

The following are recommended to the Kingdom of Tonga to start the thinking process on how to improve the cybercrime legislation to increase the effectiveness of their cybercrime defensive measures. The following recommendations were informed by the lessons learned from the reviews and the comparisons in this study. Moreover, the conclusion drawn in section 6.3, and answers given in section 6.3.1 to the research questions.

The recommendations are:

a) Launch a campaign to raise awareness of cybercrime and also the offences criminalise by the *Computer Crimes Act.*
b) Provide training sessions for law enforcement officers in cyber investigation and also how to deal with, and handle digital evidence.
c) Provide training for law enforcement officers also on procedural requirements under the *Computer Crimes Act.*

d) Provide training sessions as well for the Judges and other officers of the courts including solicitors and attorneys. The goal is to familiarise themselves with the technical terms related or associated with cybercrime.
e) Tonga should consider adopting a more systematic approach such as the Budapest Convention's approach, and keep Tonga legislation on cybercrime up to date with international standards.
f) Make the distinction between cyber-dependent offences and cyber-enabled offences clear

6.4 FINAL COMMENTS

It is clear in from the findings of this study that Tonga is new to this whole cybercrime philosophy, and the experiences is still emerging in Tonga. In section 6.3.2, the study provides recommendations and in sub-section (a), (b), (c), and (d), that it is important to make the citizens and users of the Internet in Tonga aware of cybercrime and the offences that criminalise by the Computer Crimes Act. Also, the study believed that equally important to provide training to law enforcement officials, lawyers, and judges.

Cybercrime legislation defines standards of appropriate conducts for users of the Internet, Computers, Computer Networks, and other electronic devices. Cybercrime legislation protects ICT authorised users, and that includes the information system itself – the infrastructure, the services it provides, and the data it collects and processes. Cybercrime legislation also provides standards for the use of Internet and all electronic devices, actions of the users including government and private enterprises. In addition, cybercrime legislation includes applicable, procedural and preventive laws.

This study is designed aiming to review and compare cybercrime legislations of Tonga, Kiribati, Fiji, and Samoa. This is done with the hope to better the standards of cybercrime defensive and protective measures in the South Pacific. There's no doubt that we are living in a digital age, connected, and with the ICT technologies brings everyone closer and together. Cyber criminals have also taken advantage the technology to expand the boundaries of their criminal activities, faster and reach more people than ever before.

It is the hope of this study that the findings can be of use to find the appropriate methods to deter and combat cybercrime in the South Pacific. Given the fact that cybercrime is on the rise, complex, cutting-edge, with new methods of committing it. This study believes that with the conclusions drawn, and the recommendations made can be helpful to improve the current status in terms of legal mechanism to criminalise new crimes committed in cyberspace.

REFERENCES

Aborujilah, A., Nassr, R. M., Al-Hadhrami, T., Husen, M. N., Ali, N. A., Al-Othmani, A., Syahela, N., Ochiai, H. (2020). Security Assessment Model to Analysis DOS Attacks in WSN *Proceedings of the International Conference of Reliable Information and Communication Technology on Emerging Trends in Intelligent Computing and Informatics* (pp. 789-800). Cham: Springer International Publishing.

Action Fraud. (2020). *Cyber fraud*. Retrieved September 18, 2020, from https://www.actionfraud.police.uk/a-z-of-fraud-category/cyber-fraud

Akdeniz, Y. (2016). *Internet Child Pornography and the Law: National and International Responses*: Routledge.

Akhgar, B., Chorań, M., Brewster, B., Bosco, F., Vermeersch, E., Luda, V., Puchalski, D., Wells, D. (2016). Consolidated Taxonomy and Research Roadmap for Cybercrime and Cyberterrorism. In B. Akhgar & B. Brewster (Eds.), *Combatting Cybercrime and Cyberterrorism: Challenges, Trends and Priorities* (pp. 295-321). Cham: Springer International Publishing.

Albarqi, A., Alzaid, E., Alghamdi, F., Asiri, S., & Kar, J. (2015). Public Key Infrastructure: A Survey. *Journal of Information Security, 06*, 31-37.

Alberts, C. J., & Dorofee, A. (2002). *Managing Information Security Risks: The Octave Approach*: Addison-Wesley Longman Publishing Co., Inc.

Alkaabi, A., Mohay, G., McCullagh, A., & Chantler, N. (2011). Dealing with the Problem of Cybercrime *Proceedings of the International Conference on Digital Forensics and Cyber Crime* (pp. 1-18). Berlin, Heidelberg: Springer.

Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M. J. G., Levi, M., Moore, T., Savage, S. (2013). Measuring the Cost of Cybercrime. In R. Böhme (Ed.), *The Economics of Information Security and Privacy* (pp. 265-300). Berlin, Heidelberg: Springer Berlin Heidelberg.

Arief, B., & Adzmi, M. A. B. (2015). Understanding Cybercrime from Its Stakeholders' Perspectives: Part 2--Defenders and Victims. *IEEE Security & Privacy, 13*(2), 84-88.

Arief, B., Adzmi, M. A. B., & Gross, T. (2015). Understanding Cybercrime from Its Stakeholders' Perspectives: Part 1--Attackers. *IEEE Security & Privacy, 13*(1), 71-76.

Arthurs, H. (1983). Law and learning: report to the Social Sciences and Humanities Research Council of Canada. *The Consultative Group on Research and Education in Law*.

Baragwanath, Lee, M., Dugdale, & Henare, D. (1999). *New Zealand Law Commission Report 54 - Computer Misuse*. Wellington, New Zealand.

Barclay, C. (2017). Cybercrime and legislation: a critical reflection on the Cybercrimes Act, 2015 of Jamaica. *Commonwealth Law Bulletin, 43*(1), 77-107.

Barn, R., & Barn, B. (2016). An ontological representation of a taxonomy for cybercrime. *Proceedings of the 24th European Conference on Information Systems (ECIS 2016)* (pp. 1-16). Istanbul, Turkey: Middlesex University.

Blythe, S. E. (2006). South pacific computer law: Promoting E-commerce in Vanuatu and fighting cyber-crime in Tonga. *Journal of South Pacific Law, 10*(1), 1-29.

Brown, J. D. (2011). Quantitative research in second language studies. *Handbook of research in second language teaching and learning, 2*, 190-206.

Catudal, J. N. (1999). Censorship, the Internet, and the child pornography law of 1996: A critique. *Ethics and Information Technology, 1*(2), 105-115.

Cave, D. (2012). Digital islands: How the Pacific's ICT revolution is transforming the region. *Lowy Institute for International Policy, 21*(1), 1-24.

Chawki, M., Darwish, A., Khan, M. A., & Tyagi, S. (2015). Online Obscenity and Child Sexual Abuse. In *Cybercrime, Digital Forensics and Jurisdiction* (pp. 81-94). Cham: Springer.

Chen, K. (2014). Research Methodology. In *Comparative Study of Child Soldiering on Myanmar-China Border: Evolutions, Challenges and Countermeasures* (pp. 11-16). Singapore: Springer Singapore.

Child Pornography Prevention Act 1996 (U.S.A).

Choi, Y., & Hong, S. (2020). Qualitative and quantitative analysis of patent data in nanomedicine for bridging the gap between research activities and practical applications. *World Patent Information, 60*, 101943.

Choo, K.-K. R., & Smith, R. G. (2008). Criminal Exploitation of Online Systems by Organised Crime Groups. *Asian Journal of Criminology, 3*(1), 37-59.

Christopher Lee, G.-M. (1994). Offences Created by the Computer Misuse Act 1993. *Singapore Journal of Legal Studies*, 263.

Chua, C. E. H., & Wareham, J. (2008). Parasitism and Internet auction fraud: An exploration. *Information and Organization, 18*(4), 303-333.

Chynoweth, P. (2008). Legal research. *Advanced research methods in the built environment*, 28-38.

Clough, J. (2014). A world of difference: the Budapest convention of cybercrime and the challenges of harmonisation. *Monash University Law Review, 40*(3), 698-736.

Collins. (2020). *Methodology*. HarperCollins Publishers. https://www.collinsdictionary.com/dictionary/english/methodology

Commonwealth Secretariat (2017). Model Law on Computer and Computer Related Crime. *Office of Civil and Criminal Justice Reform, 1*(1), 1-20.

Commonwealth Secretariat. (2002). Model Law on Computer and Computer Related Crime. *Report of 2nd Meeting of Expert Group on Computer and Computer Related Crime, 1*(1), 1-34.

Convention on Cybercrime, Nov, 23, 2001, E.T.S. 185, Budapest, 25

Cornish, P., Hughes, R., & Livingstone, D. (2009). Cyberspace and the National Security of the United Kingdom. *Threats and Responses. Chatham House, London, 1*(1), 1-46.

Creswell, J. W., & Creswell, J. D. (2017). *Research design: Qualitative, quantitative, and mixed methods approaches*: Sage publications.

Crimes Act 1961 (NZ)

Crimes Amendment Act 2003 No.39 (NZ)

Daly, J. P. (1993). The Computer Fraud and Abuse Act-A New Perspective: Let the Punishment Fit the Damage, 12 J. Marshall J. Computer & Info. L. 445 (1993). *The John Marshall Journal of Information Technology & Privacy Law, 12*(3), 445-465.

Deb, D., Dey, R., & Balas, V.E. (2019). Introduction: What Is Research? Engineering Research Methodology: A Practical Insight for Researchers. Singapore, Springer Singapore**:** 1-7.

Deutch, M. (1995). Computer legislation: Israel's new codified approach. *J. Marshall J. Computer & Info. L., 14*, 461.

Dobinson, I., & Johns, F. (2017). *Research methods for law*: Edinburgh University Press.

Donalds, C., & Osei-Bryson, K.-M. (2019). Toward a cybercrime classification ontology: A knowledge-based approach. *Computers in Human Behavior, 92*, 403-418.

Elmaghraby, A. S., & Losavio, M. M. (2014). Cyber security challenges in Smart Cities: Safety, security and privacy. *Journal of Advanced Research, 5*(4), 491-497.

ENISA. (2019). ENISA Threat Landscape Report 2018: 15 Top Cyberthreats and Trends. *ENISA Threat Landscape Report 2018, 1*(7), 1-139.

Finau, G., Curuki, J., & Prasad, A. (2013). Cybercrime and it's Implications to the Pacific. *The Journal of the Fiji Institute of Accountants, 1*(1), 15-18.

Foody, M., Samara, M., El Asam, A., Morsi, H., & Khattab, A. (2017). A review of cyberbullying legislation in Qatar: Considerations for policy makers and educators. *International Journal of Law and Psychiatry, 50*, 45-51.

Forensic, K. (2004). Fraud Survey 2004, KPMG International. *Lawrence, TB & Robinson, SL (2007). Aint Misbehavin: Workplace Deviance as Organizational Resistance. Journal of Management, 33*(3), 378-394.

Fosch-Villaronga, E., & Millard, C. (2019). Cloud robotics law and regulation: Challenges in the governance of complex and dynamic cyber–physical ecosystems. *Robotics and Autonomous Systems, 119*, 77-91.

Gawas, V. M. (2017). Doctrinal legal research method a guiding principle in reforming the law and legal system towards the research development.

Gercke, M. (2016). Understanding cybercrime: a guide for developing countries. *International Telecommunication Union Cybercrime Legislation Resources, 1*(2), 1-493.

Goel, A., Tyagi, A., & Agarwal, A. (2012). Smartphone forensic investigation process model. *International Journal of Computer Science & Security (IJCSS), 6*(5), 322-341.

Gordon, S. (1995). Technologically enabled crime: Shifting paradigms for the Year 2000. *Computers & Security, 14*(5), 391-402.

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *Journal in Computer Virology, 2*(1), 13-20.

Government of Canada. (2010). *Canada's Cyber Security Strategy: For a stronger and more prosperous Canada*. Canada: Government of Canada.

GPO. (2010). *Title 18 - Crimes and Criminal Procedure*. U.S.A: U.S. Government Publishing Office.

Grenada Telecommunications Act #31 of 2000

Gřivna, T., & Drápal, J. (2019). Attacks on the confidentiality, integrity and availability of data and computer systems in the criminal case law of the Czech Republic. *Digital Investigation, 28*, 1-13.

Guo, M. (2018). China's cybersecurity legislation, it's relevance to critical infrastructures and the challenges it faces. *International Journal of Critical Infrastructure Protection, 22*, 139-149.

Hargreaves, C., & Prince, D. (2013). *Understanding cyber criminals and measuring their future activity*: Lancaster University.

HG.org. (2020). *Computer Crime Law*. Retrieved August 27, 2020, from https://www.hg.org/computer-crime.html

Hilbert, E. J. (2013). Living with cybercrime. *Network Security, 2013*(11), 15-17.

Hinduja, S., & Patchin, J. W. (2010). Bullying, cyberbullying, and suicide. *Archives of suicide research, 14*(3), 206-221.

HIPCAR. (2012). Cybercrime/e-Crimes: Model Policy Guidelines & Legislative Texts. *Model Policy Guidelines & Legislative Text, 1*(1), 1-64.

Hutchinson, T., & Duncan, N. (2012). Defining and describing what we do: Doctrinal legal research. *Deakin L. Rev., 17*, 83.

ICB4PAC. (2013). *Establishment of Harmonized Policies for the ICT Market in the ACP Countries*. Geneva.

Jaeger, A.-V., & Hök, G.-S. (2010). Legal Systems. In *FIDIC - A Guide for Practitioners* (pp. 1-53). Berlin: Springer.

Jahankhani, H., Al-Nemrat, A., & Hosseinian-Far, A. (2014). Chapter 12 - Cybercrime classification and characteristics. In B. Akhgar, A. Staniforth, & F. Bosco (Eds.), *Cyber Crime and Cyber Terrorism Investigator's Handbook* (pp. 149-164): Syngress.

Jamil, Z. (2014). Cybercrime Model Laws. Discussion paper prepared for the Cybercrime Convention Committee (T-CY), 1(1), 1-38.

Jarrett, H. M., Bailie, M. W., Hagen, E., & Etringham, E. (2010). *Prosecuting computer crimes* (Vol. 27). Washington, DC 20530: Office of Legal Education Executive Office for United States Attorneys.

Jerome Orji, U. (2019). An inquiry into the legal status of the ECOWAS cybercrime directive and the implications of its obligations for member states. *Computer Law & Security Review, 35*(6), 1-16.

Jianglan, W. C. W. Y. C. (2008). Information Institute of Shanghai Academy of Social Sciences, Shanghai 200235; A Layered Framework of the Informatization in World Expo [J]. *Library and Information Service, 9*.

Joshi, R. C., & Pilli, E. S. (2016). Smartphone Forensics. In *Fundamentals of Network Forensics: A Research Perspective*. London: Springer London.

Justice Baragwanath., Lee, J. M., Dugdale, D., onzm, D. H., & ed, T. B. (1999). *New Zealand Law Commission Report 54 - Computer Misuse*. Wellington, New Zealand.

Kammüller, F., Nurse, J. R. C., & Probst, C. W. (2016). Attack Tree Analysis for Insider Threats on the IoT Using Isabelle. *Proceedings of the International Conference on Human Aspects of Information Security, Privacy, and Trust* (pp 234-246). Cham: Springer International.

Karnow, C. E. (1998). The State of the Law on Cyberjurisdiction and Cybercrime on the Internet. *Australian Institute of Criminology*, 1-31.

Kefu, A. (2011). Tonga's Cybercrime Legislation. *Proceedings of the 1*0th *Octopus Conference & Budapest Convention* (pp. 1-7). Strasbourg.

Kettani, H., & Cannistra, R. M. (2018). On Cyber Threats to Smart Digital Environments. *Proceedings of the 2nd International Conference on Smart Digital Environment* (pp. 183-188). Rabat, Morocco: ACM.

Kharel, A. (2018). Doctrinal Legal Research. *Available at SSRN 3130525, 1*(1), 1-16.

Kittichaisaree, K. (2017). Cyber Crimes. In *Public International Law of Cyberspace* (pp. 263-293). Cham: Springer.

Knight, A., & Ruddock, L. (2009). *Advanced research methods in the built environment*: John Wiley & Sons.

Krone, T. (2005). Hacking Motives: High Tech Crime Brief. *High Tech Crime Brief*, 1-2.

Kshetri, N. (2006). The simple economics of cybercrimes. *IEEE Security & Privacy*, *4*(1), 33-39.

Kshetri, N. (2009). Positive externality, increasing returns, and the rise in cybercrimes. *Communications of the ACM*, *52*(12), 141–144.

Kuhn, D. R., Hu, V. C., Polk, W. T., & Chang, S.-J. (2001). Introduction to Public Key Technology and the Federal PKI Infrastructure. *National Institute of Standards and Technology* (NIST SP 800-32), 1-54.

Kumar, R. (1998). *Research methodology: A step-by-step guide for beginners*. Melbourne: Addison Wesley Longman.

Leedy, PD, & Ormrod, JE (2015). Practical research. Planning and design. Boston, MA: Pearson. *Journal of Applied Learning and Teaching, 1*(2), 73-74.

Li, D. (2011). Impact of IT Industry on Chinese Technology Advancement Based on Panel Data Approach. In Y. Wu (Chair). *Proceedings of the International Conference on Information and Management Engineering: Computing and Intelligent Systems.* (pp. 263-267). Wuhan, China: Berlin, Heidelberg.

Li, X. (2008). *Cybercrime and deterrence: networking legal systems in the networked information society* (Dissertation). University of Turku, City in Finland.

Lunney Jr, G. S. (1995). Lotus v. Borland: Copyright and Computer Programs. *Tul. L. Rev., 70*, 2397.

Luong, H. T. (2019). Cybercrime in Legislative Perspectives: A Comparative Analysis between the Budapest Convention and Vietnam Regulations. *International Journal of Advanced Research in Computer Science, 10*(3), 1-13.

Lutui, P. R., Tete'imoana, O., & Maeakafa, G. (2017). An analysis of personal wireless network security in Tonga: A study of Nuku'alofa. *Proceedings of the 2017 27th International Telecommunication Networks and Applications Conference (ITNAC)* (pp. 1-4). Melbourne, VIC: IEEE.

Ma, J. (2016). Cybermatics for Cyberization towards Cyber-Enabled Hyper Worlds. *Proceedings of the 4th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud)* (pp. 85-86). Oxford, UK: IEEE.

Ma, J., Choo, K.-K. R., Hsu, H.-h., Jin, Q., Liu, W., Wang, K., Wang, Y. & Zhou, X. (2016). Perspectives on Cyber Science and Technology for Cyberization and Cyber-Enabled Worlds. *Proceedings of the 14th Intl Conf on Dependable, Autonomic and Secure Computing, 14th Intl Conf on Pervasive Intelligence and Computing, 2nd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress* (pp.1-9). IEEE: Auckland, NZ.

Manual, U. (2001). United Nations Manual on the Prevention and Control of Computer-Related Crime. *1*(1), 1-29.

Matangi Tonga. (2013). *Tonga's high speed internet goes live August 21*. Retrieved July 30, 2019, from http://matangitonga.to/2013/08/14/tonga%E2%80%99s-high-speedinternet-goes-live-august-21

Mathew, S., Petropoulos, M., Ngo, H. Q., & Upadhyaya, S. (2010). A Data-Centric Approach to Insider Attack Detection in Database Systems. *Proceedings of the International Symposium on Research in Attacks, Intrusions, and Defenses* (pp 382-401). Berlin: Springer.

Mayhew, P., & Reilly, J. (2007). The Experience of E-Crime: Findings from The New Zealand Crime & Safety Survey 2006. *Research, Evaluation and Modelling Unit, 1*(1), 1-40.

McConville, M. (2017). *Research methods for law*: Edinburgh University Press.

McGuire, M., & Dowling, S. (2013a). Cyber crime: A review of the evidence. *Summary of key findings and implications. Home Office Research report, 75*. 1-35

McGuire, M., & Dowling, S. (2013b). Chapter 2: Cyber-enabled crimes-fraud and theft. *Cyber crime: A review of the evidence Research Report 75*(Home Office Research Report 75), 1-27.

MEIDECC. (2017). *Tonga, the first Pacific island to be a party to the BUDAPEST Convention*. Retrieved October 16, 2019, from http://www.mic.gov.to/news-today/press-releases/6788-tonga-the-first-pacific-island-to-be-a-party-in-the-budapest-convention

Ministry of Information and Communications. (2013). *Tonga conducts Cybersecurity and Cybercrime workshops*. presented at the meeting of the Cybersecurity and Cybercrime workshops, Nuku'alofa, Tonga.

Mota, S. A. (2002). The US Supreme Court addresses the child pornography prevention act and child online protection act in Ashcroft v. Free Speech Coalition and Ashcroft v. American Civil Liberties Union. *Fed. Comm. LJ, 55*, 85.

Mylonas, A., Meletiadis, V., Tsoumas, B., Mitrou, L., & Gritzalis, D. (2012). Smartphone Forensics: A Proactive Investigation Scheme for Evidence Acquisition. *Proceedings of the IFIP International Information Security Conference on Information Security and Privacy Research* (pp. 249-260). Berlin, Heidelberg: Springer.

New Zealand Government. (2015). A secure, resilient and prosperous online New Zealand. *National Plan to Address Cybercrime 2015, 1*(1), 1-16.

New Zealand Government. (2020). Why is NZ considering joining the Budapest Convention? *New Zealand Government Cyber Security, 1*(1), 1-3.

New Zealand Police (2020). *Cybercrime*. Retrieved June 28, 2020, from https://www.police.govt.nz/advice-services/cybercrime-and-internet/cybercrime

Newman, G. R. (2009). Cybercrime. In M. D. Krohn, A. J. Lizotte, & G. P. Hall (Eds.), *Handbook on Crime and Deviance* (pp. 551-584). New York: Springer.

Newman, I., Benz, C. R., & Ridenour, C. S. (1998). *Qualitative-quantitative research methodology: Exploring the interactive continuum*: SIU Press.

Ngo, F., & Jaishankar, K. (2017). Commemorating a Decade in Existence of the International Journal of Cyber Criminology: A Research Agenda to Advance the Scholarship on Cyber Crime. *International Journal of Cyber Criminology, 11*(1), 1-9.

NZCCL. (2020). *Freedom of thought, expression, and action, and the protection of these rights from government interference or restriction.* Retrieved October 1, 2020, from https://nzccl.org.nz/

NZLII. (2020). *New Zealand acts as enacted*. Retrieved August 7, 2020, from http://www.nzlii.org/nz/legis/hist_act/cca189357v1893n56192/

Owen, T., Noble, W., & Speed, F. C. (2017). The Challenges Posed by Scammers to Online Support Groups: The 'Deserving' and the 'Undeserving' Victims of Scams. In *New Perspectives on Cybercrime* (pp. 213-240). Cham: Springer International Publishing.

Papua New Guinea Cybercrime Code Act 2016.

Payne, K., Maras, K. L., Russell, A. J., Brosnan, M. J., & Mills, R. (2020). Self-reported motivations for engaging or declining to engage in cyber-dependent offending and the role of autistic traits. *Research in Developmental Disabilities, 104*(1), 1-11.

Platt, V. (2012). Still the fire-proof house? An analysis of Canada's cyber security strategy. *International journal, 67*(1), 155-167.

Pope, R. (2019). *Cyber crime cost New Zealand $6.5 million in three months, stats show*. Retrieved October 1, 2020, from https://www.tvnz.co.nz/one-news/new-zealand/cyber-crime-cost-new-zealand-6-5-million-in-three-months-stats-show

Pouryousefi, S., & Frooman, J. (2019). The Consumer Scam: An Agency-Theoretic Approach. *Journal of Business Ethics, 154*(1), 1-12.

Privacy Commissioner. (2000). Crimes against personal privacy and crimes involving computers: Intercepting private communications and accessing computer systems without authorisation. *Report by the Privacy Commissioner to the Minister of Justice on Supplementary Order Paper No 85 to the Crimes Amendment Bill (No 6), 1*(1), 1-26.

Queen's University Library. (2020). Steps in Legal Research. *Legal Research Manual, 1*(1), 1-8.

Quick, D., & Choo, K.-K. R. (2013). Forensic collection of cloud storage data: Does the act of collection result in changes to the data or its metadata? *Digital Investigation, 10*(3), 266-277.

Radio & TV Tonga. (2017). *Tonga is first pacific country to join the Budapest convention on cybercrime*. Retrieved July 15, 2020, from http://www.tonga-broadcasting.net/?p=7430

Rao, Y. S., Keshri, A. K., Mishra, B. K., & Panda, T. C. (2020). Distributed denial of service attack on targeted resources in a computer network for critical infrastructure: A differential e-epidemic model. *Physica A: Statistical Mechanics and its Applications, 540*(1), 1-10.

RCMP. (2014). Cybercrime: An overview of incidents and issues in Canada. *Royal Canadian Mounted Police, 1*(1), 1-16.

Reddy, G. N., & Reddy, G. (2014). A Study of Cyber Security Challenges and its emerging trends on latest technologies. *International Journal of Engineering and Technology, 4*(1), 1-5.

Rees, A. (2006). Cybercrime Laws of the United States. *Computer Crime and Intellectual Property Section, 1*(1), 1-76.

Rocchetto, M., Ferrari, A., & Senni, V. (2019). Challenges and Opportunities for Model-Based Security Risk Assessment of Cyber-Physical Systems. In F. Flammini (Ed.), *Resilience of Cyber-Physical Systems: From Risk Modelling to Threat Counteraction* (pp. 25-47). Cham: Springer.

Roycroft, M. (2016). Crime and Terrorism. In *Police Chiefs in the UK: Politicians, HR Managers or Cops?* (pp. 61-86). Cham: Springer International Publishing.

RSA Data Security. (1999). Understanding Public Key Infrastructure (PKI). *An RSA Data Security White Paper, 1*(1), 1-7.

Sallavaci, O. (2017). Combating Cyber Dependent Crimes: The Legal Framework in the UK. In H. Jahankhani, A. Carlile, D. Emm, A. Hosseinian-Far, G. Brown, G. Sexton, & A. Jamal (Chair) (Eds), *Proceedings of the International Conference on Global Security, Safety, and Sustainability: Global Security, Safety and*

Sustainability - The Security Challenges of the Connected World (pp. 53-66). Cham: Springer International Publishing.

Samoa Crimes Act 2013.

Schjolberg, J. S., & Hubbard, A. M. (2005). Harmonizing National Legal Approaches on Cybercrime. *Proceedings of the ITU WSIS Thematic Meeting on Cybersecurity* (pp. 1-25). Geneva: ITU.

Schou, C. D., & Trimmer, K. J. (2004). Information assurance and security. *Journal of Organizational and End User Computing, 16*(3), 123-145.

Scott, N. (2007). Cyber Legislation: A Model Law for the South Pacific. *Proceeding of the APT/ITU/PITA/Workshop on Principles of Cyber Legislation for the Pacific Region Conference* (pp. 93-134). Auckland, NZ: Victoria University

Shackelford, S. (2009). Estonia two-and-a-half years later: a progress report on combating cyber attacks. *Journal of Internet Law, Forthcoming, 1*(1), 1-12.

Shakeel, I., Tanha, A. D., & Broujerdi, H. G. (2010). A Framework for Digital Law Enforcement in Maldives. *Proceedings of the 2010 Second International Conference on Computer Research and Development* (pp. 146-150). Kuala Lumpur: IEEE.

Singapore Computer Misuse Act, Revised Edition 2007.

Sowa, J. (2011). Music Theory for the Twentieth-First Century: James Tenney's Meta-Hodos. *Joseph Sowa Composer, 1*(1), 1-14.

Standard Standardisation of ITU (2008). Series X: Data Networks. Open System Communication and Security: Overview of Cyber Security. *Recommendation ITU-T X.1205 (04/2008), 10*(20-X), 49.

Stringer, K. D. (2006). Pacific Island Microstates: Pawns or Players in Pacific Rim Diplomacy? *Diplomacy & Statecraft, 17*(3), 547-577.

Sultana, N., & Turkina, E. (2020). Foreign direct investment, technological advancement, and absorptive capacity: A network analysis. *International Business Review, 29*(2), 1-13.

Swanson, M., Bowen, P., Phillips, A., Gallup, D., & Lynes, D. (2010). NIST Special Publication 800-34 Rev. 1 Contingency Planning Guide for Federal Information

Systems/M. *Swanson, P. Bowen, AW Phillips, D. Gallup, D. Lynes.–2010.–149 p*, *17*.

Taekema, S. (2020). Methodologies of Rule of Law Research: Why Legal Philosophy Needs Empirical and Doctrinal Scholarship. *Law and Philosophy, 1*(1), 1-34.

Tarter, A. (2017). Importance of Cyber Security. In P. S. Bayerl, R. Karlović, B. Akhgar, & G. Markarian (Eds.), *Community Policing - A European Perspective: Strategies, Best Practices and Guidelines* (pp. 213-230). Cham: Springer

Thompson, B. G., & Smith, L. S. (2007). Cybercrime: Public and Private Entities Face Challenges in Addressing Cyber Threats. *US Government Accountability Office, 1*(1), 1-59.

Tonga Computer Crimes Act 2016.

Tonga Copyright Act 1988.

Tonga Copyright Act 2002.

Tonga Tourism Authority. (2018). *The Kingdom of Tonga Today*. Retrieved August 7, 2019, from http://www.thekingdomoftonga.com/three-millennia-of-history/

Tonry, M. (2014). Why crime rates are falling throughout the Western world. *Crime and justice, 43*(1), 1-63.

Traynor, I. (2007). Russia accused of unleashing cyberwar to disable Estonia. *The Guardian, 17*(05).

Trenwith, A. (2004). A Patch on the System-E-Crime and the Crimes Amendment Act 2003. *Auckland UL Rev., 10*, 90.

Tsakalidis, G., Vergidis, K., Petridou, S., & Vlachopoulou, M. (2019). A cybercrime incident architecture with adaptive response policy. *Computers & Security, 83*, 22-37.

Turrini, E., & Ghosh, S. (2011). A Pragmatic, Experiential Definition of Computer Crimes. In S. Ghosh & E. Turrini (Eds.), *Cybercrimes: A Multidisciplinary Analysis* (pp. 3-23). Berlin, Heidelberg: Springer Berlin Heidelberg.

Uma, M., & Padmavathi, G. (2013). A Survey on Various Cyber Attacks and their Classification. *IJ Network Security, 15*(5), 390-396.

United Nation. (2014). *United Nations' Definition of Cybercrime*. Retrieved September 1, 2020, from https://idn-wi.com/united-nations-definition-cybercrime/

Van Gestel, R., Micklitz, H. W., & Maduro, M. P. (2012). Methodology in the new legal world. Italy: European University Institute.

Verma, S. K., & Wani, M. A. (2015). *Legal research and methodology*: Indian Law Institute, New Delhi.

von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. *Computers & Security, 38*, 97-102.

Wall, D. S. (2015). The Internet as a conduit for criminal activity. *Information technology and the criminal justice system, Pattavina, A., ed*, 77-98.

Wang, Q. (2016). A Comparative Study of Cybercrime in Criminal Law: China, US, England, Singapore and the Council of Europe.

Watney, M. (2012). Cybercrime regulation at a cross-road: State and transnational laws versus global laws. *Proceedings of the International Conference on Information Society* (pp. 71-75). London: IEEE.

Watson, D. J. (2015). *The mens rea of criminal attempt in the law of New Zealand* (Dissertation). University of Otago, New Zealand.

Weber, A. M. (2012). The Council of Europe's Convention on Cybercrime. *Berkeley Technology Law Journal: Annual Review of Law and Technology*, *18*(1), 425-446.

Will Davis, I., & Chi, H. (2011). Cyber threat analysis for university networks via virtual honeypots. *Proceedings of the 49th Annual Southeast Regional Conference* (pp. 354-355), Kennesaw, Georgia: ACM.

Yao, X., & Liu, J. (2011). The potential of economic growth and technology advancement in the BRICs. *Proceedings of the 2011 International Conference on Machine Learning and Cybernetics* (pp. 1067- 1071). Guilin, China: IEEE.

Yilma, K. M. (2017). Ethiopia's new cybercrime legislation: Some reflections. *Computer Law & Security Review, 33*(2), 250-255.

Zavrsnik, A. (2008). Cybercrime definitional challenges and criminological particularities. *Masaryk UJL & Tech.*, *2*(1), 1-29.