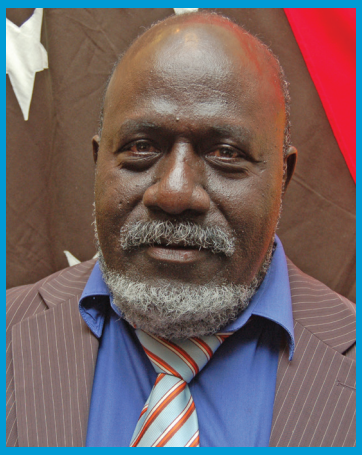
Cybercrime Policy

July 2014

Table of Contents



FOREWORD BY THE MINISTER

The National ICT Policy, 2008 makes a passing mention of cybercrime not being permitted in Papua New Guinea.

While this brief mention of cybercrime is acknowledged, the Government intends to do a lot more than just make a fleeting mention of an issue that is becoming more prevalent, particularly when information and communication technologies (ICT) are also becoming increasingly prominent both at work and in the workplace.

It therefore gives me much pleasure, as the Minister responsible for ICT, to introduce a standalone cybercrime policy for the country. The Papua New Guinea Cybercrime Policy was formally endorsed by Cabinet through NEC Decision No. 219/2014. Cybercrime refers to offences committed using electronic devices, systems and/or networks.

This important National Cybercrime Policy just didn't happen overnight.

The Government had earlier formed a Core Working Group (CWG), comprising officers from my Department, the National Information & Communication Technology Authority (NICTA), and the Department of Justice & Attorney General. Since 2010, the CWG has been working progressively to develop our own Cybercrime Policy.

The CWG attended several lead up cybercrime workshops with their Pacific Island colleagues, through funding and technical support from the International Telecommunications Union (ITU). The workshops were held in the Republic of Vanuatu, Samoa, and the Kingdom of Tonga respectively.

From these workshops, Pacific Island countries developed country-specific policy templates for their respective countries, drawing inspiration from the Commonwealth Model or the Budapest Convention on Cybercrime. At that time, the Kingdom of Tonga was the only Pacific Island country that had adopted its own Cybercrime Policy.

I commend the work of the CWG highly while the ongoing participation and guidance of Cybercrime Expert, Dr Marco Gerke, through the joint efforts of the PNG Government and ITU is also acknowledged.

Generally, the PNG Cybercrime Policy highlights the need to develop a legal framework that criminalises cybercrime in the country, while also calling for the strengthening of our collaboration and partnership with specialised regional and international agencies and governments on cybercrime.

It also calls for increased levels of awareness on threats and consequences of cybercrime on our people, with a particular focus on our children. It also promotes the importance of developing and strengthening the capacity and capabilities of State institutions like the police, judges, and other court officials to effectively deal with cybercrimes.

I encourage you all to read and familiarise yourselves with the ensuing pages of this crucial Policy.

It is incumbent on every citizen, the Internet service providers, the wider business community, the media, and government and other non-government actors to work together to minimise the real and serious threat that cybercrime possess, particularly with the increasing presence of ICT and the borderless environment they operate in. Let's make it our collective business to tackle cybercrime in Papua New Guinea.

I commend the National Cybercrime Policy to you all.

Hon. Jimmy Miringtoro, OBE, MP
Minister for Communication & Information Technology

ABBREVIATIONS

ICT	Information & Communication Technology
ITU	International Telecommunication Union
NICTA	National Information and Communication Technology Authority
PM&NEC	Department of Prime Minister and National Executive Council
DCI	Department of Communication and Information

PART ONE: INTRODUCTION

1. Background

The Government of Papua New Guinea ("the Government"), as with many countries worldwide, has recognized the social and economic benefits to be derived from Information Communication Technologies (ICTs). Properly utilised, ICTs can be a significant tool in our country's development, and the realisation of the National Goals and Directive Principles (NGDPs).

Concurrently, the Government is mindful that the use of ICTs inevitably introduces correlative security concerns for individuals, businesses, and the public sector that need to be addressed. Malicious software that affects millions of electronic devices, systems and networks, and causes significant damage are only examples of the much broader problem of Cybercrime.

Cybercrime and Cybersecurity issues present major concerns for law enforcement agencies around the world. This has generated intensive debate where various solutions have been discussed to address the issue of criminal abuse of electronic devices, systems and networks. Evolving technological advances have also meant that Cybercrime and Cybersecurity are high on the agenda of governments, and regional and international organisations.

Therefore, to address this challenge a National Policy response is required.

2. Vision Statement

The socio-economic development of Papua New Guinea is becoming increasingly dependent on the use of ICT services and applications. However, the Government acknowledges the threats posed by Cybercrime (and Cybersecurity issues) which potentially can circumvent socio-economic growth if not appropriately addressed.

In view of the foregoing and the significance of ICTs, it is acknowledged that through the collective input and collaboration of all stakeholders and international partnerships, we will work together to combat Cybercrime.

This can be achieved through the development of an effective legal and regulatory framework in light of the ensuing Guiding Principles resulting in a better, trustworthy and secure ICT environment.

3. Guiding Principles

The development of an effective legal and regulatory framework in accordance with the Guiding Principles will result in a better, trustworthy and secure ICT environment.

This Policy seeks to provide a legal and regulatory framework to –

- Protect Papua New Guinea communities from cybercrime;
- Preserve our cultural and traditional values;
- Create safer cyber environment for all users;
- Build confidence in electronic commerce;
- Ensure that Papua New Guinea laws on Cybercrime are, to an extent where possible, in harmony with other regional and international laws dealing with Cybercrime (and Cybersecurity issues);
- Promote and enhance international cooperation in addressing and combating Cybercrimes;
- Enhance and strengthen Papua New Guinea's law enforcement capacity in addressing and combating Cybercrime (and Cybersecurity issues);
- Create and increase awareness, education and training on Cybercrime (and Cybersecurity issues) within Papua New Guinea; and
- Ensure effective coordination and collaboration amongst all stakeholders, especially the law enforcement agencies.

4. Cybercrime and Cybersecurity

Cybercrime and Cybersecurity are often misconceived to mean the same thing. Cybersecurity refers to "*the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyberenvironment and organisation and users' assets*[1]." In essence, Cybersecurity is the deterrence of Cybercrime. Deterring cybercrime should be an integral component of any national cybersecurity and critical information infrastructure protection strategy[2].

Cybercrime, on the other hand, refers to offences committed using electronic devices, systems and or networks[3]. Cybercrime is broad concept however it can be divided into the following four (4) subcategories[4] to be better understood -

[1] Understanding Cybercrime, 2nd Edition, ITU, 2011, Chapter 1, Page 17
[2] Understanding Cybercrime, 2nd Edition, ITU, 2011, Chapter 1, Page 17
[3] "Cybercrime" and "Computer Crime" are often used interchangeably. However, there is a fundamental difference between the two terms. Although it is impossible to come up with a single comprehensive definition, "computer crime" refers typically to crimes related to computer data and systems. Such crimes do not necessarily require the use of computer networks to commit them. "Cybercrime" refers to offences where computer networks are used. Although not every computer crime is a cybercrime, the emerging use of computer networks and the interconnection of computer or electronic system merges the meaning of both terms.

(a) **Offences against the confidentiality, integrity and availability of electronic data, systems and networks** (this includes *illegal access to electronic systems and networks, illegal remaining in an electronic system or network, illegal access to electronic data, illegal interception of electronic data, illegal data interference, illegal data acquisition, illegal system or network interference* and *illegal obstruction of use of electronic data*)

(b) **Content-related offences** (this includes *child pornography, SPAM* and *harassment utilising means of electronic communication*)

(c) **Copyright-related offences**

(d) **Other offences** including *computer-related fraud or forgery, identity-related crime* and *misuse of devices*.

5. History of Policy Development in PNG

There were concerted efforts made prior to and after Independence towards formulating a National Policy on Information and Communication. In 1992, the first real steps were taken when the Government tabled the National Policy on Information and Communications ("NPIC") in Parliament through the then Minister, Honourable Martin Thompson, M.P.

The priority of Government then was to empower citizens through information dissemination. Therefore the Policy focused more on media and information dissemination. Cybercrime was not anticipated as it was not considered a threat to Papua New Guinea at the time.

However, the advancement of technology and the increasing use of the Internet have transformed the world by providing opportunities for business, providing access to the global markets, delivering a wealth of information, enhancing social interaction and enabling greater community participation.

As a result, the Government saw the need to formulate a policy to enhance the use of ICTs for national development. In 2005 a national policy was developed and endorsed in 2008, as the "*National ICT Policy, 2008*". Although the objectives of the National ICT Policy, 2008 include the prohibition of Cybercrime, it accords minimal prominence to the subject matter.[5]

Under the National ICT Policy, 2008 and during the development of the new licensing regime now in existence under the *National Information & Communication Technology Act, 2009* there was some initial work undertaken by the Government with a view to

[4] M. Gercke, 14 July 2012.

[5] The National ICT Policy, 2008 addresses Cybercrime as the very last subject matter and covers only two (2) pages. The objectives of the National ICT Policy, 2008 are to ensure that pursuant to the legal framework of PNG –

(a) Cybercrime is prohibited;
(b) Privacy is protected to a degree meeting International Privacy Standards;
(c) Consumers and traders who conduct business electronically are adequately protected;
(d) The Intellectual property of others are adequately protected; and
(e) Critical IT systems are protected in the event of war, disaster or civil disturbance.

implementing the objectives of Policy. The strategies envisaged under the Policy to address Cybercrime are –

(a) The adoption of criminal laws against attacks on the security and integrity of computer systems and information, thereby criminalizing hacking, illegal interception and interference with availability of computer subsystems.

(b) To have clear procedures meeting international standards for government access to communications and stored data when required for criminal investigations. Such procedures will allow government to carry out their investigations, but will also assure businesses and consumers that there cannot be any unjustified monitoring of all types of communications.

(c) To put in place procedures and laws facilitating the use of credit cards and electronic forms of payment, in a legal framework ensuring consumers and business proprietors who transact business online have recourse if the transaction does not go through or if the product or services purchased are unsatisfactory. It will also ensure that consumer data provided to merchants will not be misused.

(d) To review the existing intellectual property laws to ensure that there is adequate protection in the digital setting.

(e) To have procedures and processes in place to take all critical systems offline in the event of war, disaster or civil unrest, which otherwise could jeopardize or place such systems at risk.

Based on the above, the Policy alludes to certain recommendations as a way forward. Despite these recommendations, there has not been any real progress until now.

6. Challenges in Determining the Threat Level

When developing policies and strategies in the field of criminal justice and crime prevention, very often crime statistics are used as an indicator for the seriousness of a subject matter and the need for the Government to respond. Consequently crime statistics are used by policy-makers to support the decision-making processes.[6] However, it is difficult to quantify the impact of Cybercrime solely on the basis of the number of offences carried out within a given time-frame[7] because Cybercrime victims very often fail to report incidents.[8] This could be due to the lack of knowledge and or awareness and the absence of appropriate reporting facilities.

For example, in a recent national survey undertaken in preparation of this Policy [9], answers generated from questions relating to people's understanding of Cybercrime and incidences of Cybercrime showed that appropriate awareness is lacking. A notable percentage (almost 50%) of those surveyed did not have knowledge of or were unsure of what Cybercrime is or the types of offences that constitute such crime.

[6] *Collier/Spaul*, Problems in Policing Computer Crime, Policing and Society, 1992, Vol.2, page, 308.

[7] *Walden*, Computer Crimes and Digital Investigations, 2006, Chapter 1.29.

[8] Understanding Cybercrime, 3rd Edition, ITU, 2012, Chapter 4.2.

[9] This survey was widely circulated through the media covering most of the country. However, only 314 questionnaires were completed and returned albeit covering a decent cross section of society.

The results of the survey are summarised in the table below –

QUESTION	TOTAL: 314	ANSWER	PERCENTAGE
Gender	Male	164	52.23%
	Female	150	47.77%
Occupation	Self-employed/Employed	125	39.81%
	Unemployed	6	1.91%
	Student	182	57.96%
	Not specified	1	0.32%
Age group	5-13	113	35.99%
	14-18	58	18.47%
	19-25	34	10.83%
	26-40	62	19.75%
	41-55	39	12.42%
	56+	8	2.55%
Use of Electronic devices and or systems	Yes	313	99.68%
	No	1	0.32%
Internet Usage	Yes	292	92.99%
	No	22	7.01%
Awareness of cybercrime	Yes	170	54.14%
	No	86	27.39%
	Unsure	58	18.47%
Knowledge of meaning of cybercrime	Yes	170	54.14%
	No	86	27.39%
	Unsure	58	18.47%
Incidences of cybercrime	Yes	170	54.14%
	No	86	27.39%
	Unsure	58	18.47%
Education as a measure against cybercrime	Yes	295	93.95%
	No	17	5.41%
Adequacy of Awareness	Yes	34	10.83%
	No	275	87.58%
	Unsure	5	1.59%
Opinion on Government Sponsorship of Cybercrime Awareness	Yes	291	92.68%
	No	19	6.05%
	Unsure	4	1.27%
Service Providers duty to combat or Preventing Cybercrime	Yes	288	91.72%
	No	18	5.73%
	Unsure	8	2.55%

Devise Sellers's duty in combating or preventing Cybercrime	Yes	259	82.48%
	No	47	14.97%
	Unsure	8	2.55%
Security of e-commerce	Yes	103	32.80%
	No	198	63.06%
	Unsure	13	4.14%
Law enforcement's capability/capacity to investigate & prosecute cybercriminals	Yes	102	32.48%
	No	197	62.74%
	Unsure	15	4.78%
Use of security measures	Yes	255	81.21%
	No	51	16.24%
	Unsure	8	2.55%

Moreover, 87% of the respondents to the question regarding the adequacy of awareness were of the view that there is insufficient awareness. In addition, almost 93% of those surveyed thought that the Government should be more proactive in undertaking awareness initiatives on Cybercrime.

Other authoritative sources of information such as reports and surveys are frequently used within the process of determining the threat of computer crime and cybercrime. Surveys published in the last year show an increasing trend. The 2011 Norton Cybercrime Report for example states that "Cybercrime is bigger than the global black market in marijuana, cocaine and heroin combined ($288bn) and approaches the value of all global drug trafficking ($ 411bn)".[10] However the use of such surveys within the process of drafting policies carries with it certain concomitant challenges. One major concern is related to the extrapolation of sample survey results – a common methodology used by such non-scientific surveys[11]. In addition the major surveys undertaken are related to jurisdictions such as Europe and the US but are not specific to the Pacific in general and more particularly Papua New Guinea.

In light of the foregoing, the development of this Policy takes into consideration the predominant global trends relating to Cybercrime that would undoubtedly have an impact on the incidence of crime in Papua New Guinea.

7. The Need for Cybercrime Policy and Legislation

The liberalisation of the ICT market has exposed PNG to cybercrime, information security threats and related offences as experienced by other countries[12]. This necessitates the urgency to develop appropriate policy and legislative framework to combat and prevent the commission of offences through the use of ICTs.

[10] See. http://www.norton.com/cybercrimereport
[11] Understanding Cybercrime, 3rd Edition, ITU, 2012, Chapter 2.4.2.
[12] The survey conducted revealed incidences of the following types of Cybercrime: SPAM; viruses; hate mail; propaganda threats and intimidation; obscenity; pornography and others.

The Government, through the Department of Communication and Information, National Information and Communication Technology Authority (NICTA), ICT industry players, various stakeholders and the International Telecommunications Union (ITU) will take robust steps to bring about real and constructive progress in this area.

The purpose of this Policy is to define the different instruments and mechanisms that may effectively be used to address Cybercrime. This includes, but is not limited to, determining the general principles and considerations related to the Policy and a legislative response and preventative measures to address Cybercrime.

8. Existing Legislation

The *Criminal Code Act, 1974* deals with criminal offences, including pornography and indecent materials, however, does not adequately accommodate cybercrime or offences committed using electronic devices, systems, or networks.

In addition, the following legislation somewhat address certain aspects of Cybercrime:

(a) *Banks and Financial Institutions Act, 2000*;

(b) *Business Names Act, 1963*;

(c) *Central Banking Act, 2000;*

(d) *Classification of Publication (Censorship) Act, 1989*;

(e) *Companies Act, 1997*;

(f) *Copyright and Neighboring Rights Act, 2000*;

(g) *Criminal Code Act, 1974*;

(h) *Customs Act, 1951;*

(i) *Evidence Act, 1975;*

(j) *Internal Security Act, 1993*;

(k) *Lukautim Pikinini Act, 2012;*

(l) *National Broadcasting Corporation Act, 1973;*

(m) *National Intelligence Organisation Act, 1984;*

(n) *National Information and Communications Technology Act, 2009*;

(o) *Patent and Industrial Designs Act, 2000*;

(p) *Protection of Private Communications Act, 1973;*

(q) *Securities Act, 1997*;

(r) *Telikom PNG Ltd Act, 1996; and*

(s) *Trade Marks Act, 1978*.

9. Role of the Government in Combating Cybercrime

The Government has a key role in ensuring the development of appropriate policy, legislation and strategies, which will provide the framework for combating and preventing Cybercrime.

This Cybercrime Policy sets out the Government's objectives and strategic framework for meeting these challenges. In doing so, this Policy will ensure –

(a) That relevant government departments and instrumentalities engage in co-ordinated activities to combat and prevent Cybercrime; and

(b) The appropriate enforcement of the regulatory regime by relevant agencies that are independent yet accountable and with clearly defined powers, functions and jurisdictions.

9.1 Department of Justice and Attorney General

The Department of Justice and Attorney General is responsible for the general administration of government policies on law, and justice.

In respect of preventing and combating Cybercrime, the Department of Justice and Attorney General will be responsible for facilitating and coordinating international cooperation in relation to extradition, mutual assistance and proceeds of crime.

The Department will provide advice and assistance in respect of the continuing development of Cybercrime law.

9.2 Department of Communication and Information (DCI)

DCI is responsible for the administration of government policies on ICT matters.

It will coordinate with all relevant government agencies to ensure appropriate Cybercrime policies are in place and reviewed from time to time on par with advances in ICT technologies, trends and practices.

DCI will provide advice on the development and timely review of Cybercrime and related policies.

In collaboration with NICTA and other government stakeholders, DCI will undertake public awareness on Cybercrime.

9.3 National Information and Communication Technology Authority (NICTA)

NICTA is responsible for the implementation of the National ICT Act, 2009.

NICTA primary mandate is to regulate the ICT industry. It will coordinate with industry, regional and international bodies and provide timely advice to the Government on issues relating to Cybercrime, emerging trends and practices and possible solutions.

9.4 Royal Papua New Guinea Constabulary

The Royal Papua New Guinea Constabulary is responsible for maintaining security and law and order in the country. Through its established crime enforcement units, it will ensure relevant laws are enforced accordingly.

The primary mandate of the Royal Papua New Guinea Constabulary is to investigate complaints and facilitate the prosecution of such complaints. The Police will be assisted by other law enforcement agencies including NICTA.

The Transnational Crimes Unit should be adequately equipped and specifically trained to investigate and deal with Cybercrime through mutual assistance and international cooperation.

9.5 Office of the Public Prosecutor

The Office of the Public Prosecutor is principally responsible for the prosecution of all indictable offences, including those that can be prosecuted both summarily and on indictment.

Depending on the severity of the Cybercrime or offence, and the penalties imposed, such offences may be prosecuted either summarily or on indictment.

9.6 The Judiciary

The Judiciary is principally responsible for the dispensation of justice and the interpretation of the laws.

In respect of cybercrime the Judiciary should be adequately equipped and trained to receive and prosecute cases relating to cybercrime.

9.7 Department of Prime Minister and NEC (PM & NEC)

PM & NEC provides overall monitoring, evaluation and coordination of policy and general service delivery for the Public Service, through its chairmanship of the Central Agencies Coordinating Committee (CACC).

The PM & NEC Act, 2002 will assist on Cybercrime matters as they relate to the sovereignty, unity and security of Papua New Guinea.

In addition, the National Intelligence Organisation Act, 2002 gives responsibility to the NIO to help determine the levels of threat, whether external or internal, and advises the Government and other stakeholders to take appropriate measures to defend, protect and preserve the national sovereignty of Papua New Guinea. This includes the defence, protection and preservation of critical national infrastructures (like airports, ICT installations, and utilities), processes and its people. Threats also include sedition, espionage, sabotage and matters affecting and or threatening public order.

9.8 Other Government Stakeholders

Other relevant stakeholders not specifically mentioned in this Policy, including PNG Customs, PNG Immigration and Citizenship Services, and Censorship Board will also have an equally important role in preventing and combating cybercrime.

PART TWO: AREAS OF FOCUS

1. Legislation

1.1 Development of National Cybercrime Legislation

The Government realises that in order to prevent and combat cybercrime effectively, legislation must be enacted that criminalises and or defines conducts that constitute cybercrime, and create and or empower relevant agencies to address the issue.

Cybercrime is an ongoing priority as the range, frequency and scale of electronic attacks on individuals, businesses and the public sector, continue to grow. The Government is aware that cybercrime is a constantly evolving threat and legal measures will require concurrent amendments in future in order to counter such threats. Although technical solutions such as firewalls, encryption, passwords, etc. may be effective, these must be complemented by adequate legislative measures.

Legislation criminalising certain acts or conduct, as well as an appropriate procedural framework are critical in enabling law enforcement agencies to investigate and effectively prosecute such crimes in Court. This approach should not lead to over-criminalisation.

The Government aims to ensure that conduct and acts committed without the use of the Internet, are also criminalised when committed in an electronic environment (e.g. offensive text or audio messages, obscene images, via Bluetooth and MMS). Acts lawfully carried out without the use of the Internet in a comparable situation should only be criminalised when committed with the use of electronic devices, provided that there are precedents to justify such an approach.

Countries that are without an adequate legislative framework create a dual level of risk. On a national basis law enforcement agencies will not be able to support citizens that have become victims of cybercrimes. In addition, within the international sphere the absence of legislation criminalising certain acts and conducts may encourage or even motivate offenders from abroad to move illegal activities to countries that are devoid of a protective cybercrime legislative framework.

a) Establishment of Common Interpretations for Key Terms

Legislation should properly define terms such as “computer”, “computer system”, [vis-à-vis “electronic system”] “device”, “system”, “network” and “hinder” etc., using sufficiently broad-based wording and where possible illustrative examples. It should clearly provide which terminology shall be left for judicial construction and the

procedure for ensuring the alignment of both the judicial and statutory interpretations and definitions.

As far as possible, technical terms should be defined, technologically neutral as much as possible, and harmonisation of the application may be facilitated through the sharing of judicial precedents.

b) Development of Substantive Criminal Law

Legislation should contain provisions covering the most common and internationally accepted forms of Cybercrime as well as those offences that are of specific interest for the region (such as SPAM). It should be compatible with international standards and best practices, in order to enable and sustain cooperation with law enforcement agencies regionally as well as on an international basis.

- It should provide for the criminalization of the intentional and illegal accessing of an electronic system as well as the intentional illegal remaining in the said system.

- Intentional and illegal access to electronic data (both in cases where the offender acts with and without intent to commit or facilitate the commission of an offence) as well as the intentional and illegal interception of electronic data should be criminalized.

- Legislation should provide for a criminalization of intentional and illegal data interference, data espionage as well as the illegal obstruction and use of electronic data.

- Intentional and illegal interference with electronic systems shall be criminalization.

- Legislation shall contain aggravated sentences where one of above mentioned offences interferes with critical infrastructure.

- The intentional and illegal production, import, export, possession of tools designed to commit crimes (illegal devices) as well as illegal receiving or giving access to electronic data shall be criminalized.

- The legislation shall also provide for the criminalization of electronic-related fraud, electronic-related forgery, identity-related crime, SPAM and harassment utilizing means of electronic communication.

- In order to safeguard investigations the legislation shall criminalize the intentional and illegal disclosure of details of an investigation (where confidentiality is explicitly stipulated) and the failure to provide assistance.

c) Criminal Procedural Law

Legislation should contain the required procedural mechanism to ensure an effective investigation of cybercrime. However, despite the fact that today many investigations are technically feasible the procedural rules should not interfere with or derogate from fundamental human rights. Consequently, a balance is necessary to facilitate the

efficient conduct of investigations while maintaining the protection of an individual's fundamental human rights.

- The legislation should enable competent authorities to order the expedited preservation of electronic data, as well as the partial disclosure of preserved electronic data. It should also enable competent authorities to order the production of electronic data.

- The legislation should enable competent authorities to use specific search and seizure instruments related to electronic evidence and technology. It should regulate search and seizure proceedings in such a way that the collection of evidence and treatment of the surrounding environment from which the evidence is extracted, is in full compliance with lawful processes.

- Competent authorities should be enabled to order the lawful collection of traffic data and the lawful interception of content data.

- In cases where no other instrument is applicable, competent authorities should also be enabled to utilize sophisticated investigation techniques such as key-loggers and remote forensic software, to obtain passwords, data used by a suspect, or to identify the connection used by a suspect.

d) Jurisdiction

In relation to the difficulties associated with the application of traditional principles of state sovereignty and jurisdiction to the elements of Cybercrime, the legislation should contain the requisite provisions dealing with jurisdiction that is in line with international and regional best practices.

2. Harmonization

Harmonization of the Cybercrime legislation with those of other countries within the region and internationally is imperative. Since 2000, the Commonwealth, Common Market for Eastern and Southern Africa (COMESA), European Union (EU), Council of Europe (EC) and other regional organizations have introduced legal frameworks and model laws that aim to harmonize Cybercrime legislation.

The harmonization of legislation is widely recognized as critical in the global endeavour to combat Cybercrime. The reason for a harmonization of legislation is mainly that a number of countries base their mutual legal assistance regime on the principle of dual criminality. Therefore, if a country develops standards that fundamentally differ from international best practices this can effectively preclude such country's ability to cooperate on an international level. Further, the absence of applicable and enforceable laws in a country can lead to the creation of safe havens[13]. The existence of safe havens creates the threat that offenders will use legislative loop holes to hamper investigations and prosecution of offences. One well known example of such occurrence is the "Love

[13] This issue was addressed by a number of international organizations. The UN General Assembly Resolution 55/63 points out: "States should ensure that their laws and practice eliminate safe havens for those who criminally misuse information technologies". The full text of the Resolution is available at: http://www.unodc.org/pdf/crime/a_res_55/res5563e.pdf. The G8 10 Point Action plan highlights: "There must be no safe havens for those who abuse information technologies". See below: Understanding Cybercrime: A Guide for Developing Countries, ITU 2009, Chapter 5.2.

Bug" computer worm, developed by a suspect in the Philippines in 2000[14] which infected millions of computers worldwide.[15]

Local investigations were hindered by the fact that the development and spreading of malicious software was not at the time criminalised in the Philippines.[16]

For Papua New Guinea the relevant regional harmonization approaches are the Commonwealth Model Law on Computer and Computer-related Crime (2002) and the Skeleton for Cybercrime Legislation (2011) that was developed by and for Pacific countries within the EU/ITU co-funded project (ICB4PAC). Both documents reflect prevailing Commonwealth standards and are also in alignment with the harmonization approaches adopted by other regions such as the Council of Europe Convention on Cybercrime and the European Union Directives and Framework Decisions related to computer crime and cybercrime.

3. Crime Prevention

3.1 Awareness

This Policy recognises the need for implementation of effective awareness of Cybercrime (and Cybersecurity), its impacts and what steps can be taken to prevent and combat Cybercrime.

To achieve this, the Government sees the need to raise awareness particularly amongst young children, the general populace who are not otherwise aware of the threats posed by Cybercrime. Accordingly, such awareness should also be undertaken by responsible Government agencies and industry stakeholders.

3.2 Education

The Policy also recognises the need to educate the citizens of Papua New Guinea about Cybercrime, what it is, how it can negatively impact society and how to prevent individuals becoming victims. In this respect the Government will endeavour to bring about educational reforms by introducing subjects or courses about Cybercrime, how it can impact society and prevent measures, in its syllabus.

3.3 Capacity Building

[14] For more information, see http://en.wikipedia.org/wiki/ILOVEYOU; regarding the effect of the worm on Critical Information Infrastructure Protection, see: *Brock*, "ILOVEYOU" Computer Virus Highlights Need for Improved Alert and Coordination Capabilities, 2000.

[15] BBC News, "Police close in on Love Bug culprit", 06.05.2000.

[16] See for example: CNN, "Love Bug virus raises spectre of cyberterrorism", 08.05.2000; *Chawki*, "A Critical Look at the Regulation of Cybercrime", http://www.crime-research.org/articles/Critical/2; *Sofaer/Goodman*, "Cyber Crime and Security – The Transnational Dimension" in *Sofaer/Goodman*, "The Transnational Dimension of Cyber Crime and Terrorism", 2001, page 10; *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233.

3.3.1 Training of law enforcement agencies, judiciary, and the prosecution

Government acknowledges the impact and rapid changing pace of ICT development. In light of this government further recognises that the current status of relevant law enforcement is not adequately skilled and equipped to effectively address cybercrime.

To this end government sees the need to adequately train relevant law enforcement agencies in the prevention of and combating cybercrime.

3.3.2 Institutional and Infrastructure development

In addition to equipping relevant law enforcement agencies, it is equally important that the relevant institutions and infrastructures are created and appropriately equipped to enable law enforcement personnel to effectively investigate and prosecute offenders.

This would include the establishment of a Cybercrime unit within the Police Force, an adequately resourced forensics laboratory, technically sound logistical support and well fitted Courts for dealing with electronic evidence.

4. Regional and International Cooperation

The Government recognises the global impacts of cybercrime. Regional and international cooperation and coordination through relevant institutions, treaties and conventions, is therefore an important aspect in collectively dealing with cybercrime.

Therefore, it is necessary to review our current affiliations and improve ongoing collaboration with regional and international partners in preventing and combating cybercrime.

To strengthen existing regional and international cooperation and coordination, the Government recognises the need to accede to and or ratify certain international conventions and treaties on Cybercrime to enable their applicability and enforceability in Papua New Guinea. When participating in such conventions and treaties, the Government is fully cognizant of Papua New Guinean cultural and traditional values.

5. Electronic Evidence

5.1 Review or development of national laws to recognise admissibility of electronic evidence

The collection and production of electronic evidence in Court is presented with a number of challenges[17]. One of the main challenges is the admissibility of electronic evidence in the Courts to successfully prosecute offences. Very often, the ability to

[17] *Casey*, Digital Evidence and Computer Crime, 2004, page 9.

successfully identify and prosecute an offence is dependent on the expeditious preservation, collection and evaluation of electronic evidence.[18]

Therefore, the Government recognises the need for legislative reforms to permit the admissibility of electronic evidence into court. Further, the collection of electronic evidence requires the modification or introduction of new investigatory procedures and techniques. This Policy iterates the need to have in place such mechanisms and procedures.

Furthermore, considerable attention must be given to the way in which law-enforcement agencies and Courts deal with this new category of evidence.[19]

While traditional courts of law have asserted the best evidence rule of admissibility wherein the original document is adduced in the course of proceedings, the use of electronic evidence in some cases requires specific procedures that do not facilitate paper based conversion. Therefore modification of the rules of procedural evidence is one critical area that will require consequential amendment.[20]

5.2 Equipping relevant institutions to receive and process electronic evidence

In developing appropriate evidence laws and or provisions, there is a specific need to enhance and or equip existing law enforcement agencies and relevant institutions to facilitate the receipt, processing, authentication and retention of electronic evidence.

5.3 Establishment of a Cybercrime Investigative Unit and Forensic Laboratory

In light of the rapid advances in ICTs and corresponding and real threats of cybercrime, the Government is desirous of establishing a specialised Cybercrime Investigative Unit to refer cybercrime complaints for investigation and prosecution.

With the establishment of such a unit, the Government further observes the importance of enhancing and equipping the existing National Forensic Laboratory to deal with cybercrime forensics.

5.4 Cooperation between national law enforcement bodies

It is imperative there be cooperation, collaboration and sharing of knowledge and information between the specialised Cybercrime Investigative Unit, the Transnational Crime Unit, other law enforcement agencies and other stakeholders.

[18] Regarding the need for formalization of computer forensics, see: *Leigland/Krings*, A Formalization of Digital Forensics, International Journal of Digital Evidence, 2004, Vol.3, No.2.

[19] Regarding the difficulties of dealing with digital evidence on the basis of traditional procedures and doctrines, see: *Moore*, To View or not to view: Examining the Plain View Doctrine and Digital Evidence, American Journal of Criminal Justice, Vol. 29, No. 1, 2004, page 57 *et seq.*

[20] See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 3. Regarding the early discussion about the use of printouts, see: *Robinson*, The Admissibility of Computer Printouts under the Business Records Exception in Texas, South Texas Law Journal, Vol. 12, 1970, page 291 *et seq.*

6. Liability of ICT Service Providers

The Government recognises that cybercrime cannot be committed without the use of services and networks provided by ICT service providers who receive, store or transmit large volumes of content on behalf of their subscribers. Accordingly, it is necessary to impose some degree of responsibility and or liability on ICT service providers.

However, the Government acknowledges that it is practically impossible for ICT service providers to monitor the content in order to be held responsible and or liable for merely receiving, storing or transmitting illegal data, unless they knowingly aid or abet the offender, or are criminally negligent in their performance or discharge of any duty or obligation.

ICT service providers play an important role in making the Internet accessible to users. It is important to establish a reliable legal and regulatory framework defining the obligations of ICT Service Providers in the country, whereby the responsibility and or liability for crimes committed by users of their services should be restricted where necessary. In this context, it is essential to distinguish between the different types of service providers.

In cases where responsibility and or liability exists, legislation should limit the criminal responsibility and or liability of Internet Service Providers (ISPs) and or Access Providers on offences committed by users of their service, if the ICT provider –

- did not initiate the transmission;
- did not select the receiver; and
- did not modify the information contained in the transmission.

The criminal responsibility of Caching Providers should likewise be limited, if liability exists, for the automatic, intermediate and temporary storage of information.

Similarly, responsibility and or liability for Hosting Providers should be limited by the framework, in cases where the provider has no actual knowledge about the existence of illegal data or immediately removes them upon acquiring such knowledge.

Legislation should also specify the responsibility and or liability of Search Engine Providers and Hyperlink Providers.

As part of the terms and conditions of their license, ICT service providers shall have interception capabilities and to bear the costs of assisting in investigations in using such capabilities.

Given the qualified degree of responsibility for ICT service providers, legislation should prescribe if and for what period of time, ICT service providers need to preserve data and or content. Further, the Government considers it necessary that ICT service providers be obligated to report suspicious behaviour and to require a registration prior to making their services available.

STATEMENT BY SECRETARY

Having a policy on cybercrime is an initial step but the most challenging aspect of the process is the implementation of the policy directives and achieving the desired outcomes.

The roles of key implementing agencies are set out in this Policy, however in order for these agencies to be effective in implementing the Policy directives, it needs a central coordinating point.

In this regard, the Department of Communication and Information (DCI) in collaboration with National Information and Communication Technology (NICTA) will continue to provide the leadership in coordinating with all stakeholders to implementing the Cybercrime Policy directives.

Given the dynamic nature of Information and Communication Technology industry, both agencies will closely monitor the advancements in ICT development, trends and practices from time to time and coordinate with all implementing agencies to ensure that our efforts on addressing cybercrime and cyber security is on par and in harmony with international practices.

Equally important, whilst DCI and NICTA will coordinate the implementation of this Policy, it is incumbent upon respective agencies factored in this Policy to take ownership of developing relevant strategies and plans to implement the Policy directives of Government.

As long as the aggregate demand for ICT services and use of ICT in Papua New Guinea continues to increase, the associated incidences of cybercrimes and cyber threats will also increase.

Therefore, key government agencies must now collaborate in protecting our citizens as well as safeguarding critical infrastructures, institutions and systems against cybercrimes and threats.

PAULIAS KORNI
Secretary
Department of Communication and Information Technology

ACKNOWLEDGEMENT

We express our gratitude to the ITU for facilitating the development of the Pacific Model Cybercrime Policy framework for the Pacific Island countries, upon which the PNG Cybercrime Policy was framed.

We also acknowledge the ITU's assistance in providing technical advisory support to the Government of PNG during the development of this Policy.

We also acknowledge the professional advice and guidance of Cybercrime Expert, Dr Marco Gercke through the joint efforts of the ITU and the PNG Government.

We also sincerely thank all the stakeholders, both in-country and outside PNG, who have contributed to the finalisation of this Policy.

Finally, a special acknowledgement to the members of the Cybercrime Policy Core Working Group (CWG) who have been working tirelessly to enable the Government to realise this important Policy for the country.


danielkautu2015