UNIVERSITY OF NAIROBI

INSTITUTE OF DIPLOMACY AND INTERNATIONAL STUDIES

INTERNATIONAL CYBERCRIME AND NAMIBIA'S NATIONAL SECURITY

EMMANUEL T. IIKUYU

A Research Project Submitted in Partial Fulfilment of the Requirements for the Award of

Master of Arts in International Studies

May 2017

DECLARATIONS

I, Emmanuel Tshishungileni Iikuyu, declare hereby that this study is a true reflection of my own research, and this work, or part thereof has not been submitted for a degree in any other University.

Emmanuel Tshishungileni Iikuyu

Signature----------------------   Date-------------------

This project has been submitted for examination with my approval as the University Supervisor

Dr Anita Kiamba

Signature---------------------   Date ---------------------

Institute of Diplomacy and International Studies University of Nairobi

DEDICATION

This Research Report is graciously dedicated to my wife, Penondjila, and my children, Lukas, Natalia, Ruth and Immanuel.

ACKNOWLEDGEMENTS

An extensive research like this cannot be carried out in isolation; therefore, I would like to frankly thank the following individuals and institutions for their assistance.

Dr Anita Kiamba, my research project supervisor, for her advice, mentorship, guidance and encouragement throughout this study. I wholeheartedly applaud the University of Nairobi for giving me this gracious opportunity to improve my skill. The National Defence College Kenya deserves special credit for its invaluable support throughout this study.

I acknowledge with the enormous sense of gratitude, the hospitality of IDIS lecturers, NDC faculty and fellow participants who has constantly been a source of inspiration by offering their endless support during the entire time of the study.

A special thanks to Police Officers, Staff members from different department in Namibia who gave their precious time for interviews, for the sake of success of this study.

Finally, I thank my family for the backing and support throughout my study.

To all these people I owe my heartfelt thanks.

Abstract

Cybercrimes are becoming progressively universal and sophisticated and have more grave economic impacts than most conventional crimes. Cybercrime is made structurally different from conventional crime by the nature of its technological and skill-intensiveness, its worldwide coverage, and its inventiveness. The effect of cybercrime on society is being debated internationally, regionally and also nationally. The international community is taking measures such as reviewing of laws and creating task forces so as to mitigate its effect but, it seems that changes in laws are not made fast enough as the interlinked incidents of cybercrime makes it hard to trace offenders who use the third countries to commit crime. However, the fact remains that there is a disproportion between the internet usage which is increasing regularly and security control mechanism is lacking behind. Subsequently, this phenomenon is motivated by the sophisticated and self-sufficient digital underground economy in which data is the illicit commodity and has a monetary value.

Nevertheless, this study examines the extent to which cybercrime is affecting the society and put forward recommendations on how to better treat cybercrime incidents through introducing instruments such as; right policy and legal framework, well trained and equipped law enforcement organisations, with a support of modern infrastructure and high tech monitoring equipment, along with a well-coordinated inter and intra-agency cooperation at different levels, both locally and internationally. Above all, citizen’s awareness is essential for this campaign to succeed. *Keywords; ATM card, internet, hacking, computer system, law enforcement, computer network, cybercrime, cyber laws, cyber security***.**

TABLE OF CONTENT

LIST OF ABBREVIATIONS AND ACRONYMS

4G	Fourth generation of wireless mobile telecommunications technology
ACC	Anti- Corruption Commission,
Al Qaeda	Radical Islamic group
ATM	Automatic Teller Machine
AU	African Union
B2C	Business to Consumer
BON	Bank of Namibia
CCTV	Closed-Circuit Television
CERT	Computer Emergency Response Team
CP	Campaign planning Campaign Planning
CRAN	Communication Regulatory Authority of Namibia
DDoS	Distributed Denial of Service attack
ECOWAS	Economic Community of West Africa States
ENISA	European Union Agency for Network and Information Security
EU	European Union
FBI	Federal Bureau of Investigation
FNB	First National Bank
GCA	Global Cyber Security Agenda

GIPF	Institutions Pension Fund
HIPSSA	Harmonization of the ICT Policies in Sub-Sahara Africa
ICCPR	International Covenant on Civil and Political Rights
ICT	Information Communication Technology
INTERPOL	International Police
IP	Intellectual Property
IP	Internet Protocol
IT	Information Technology
ITU	Telecommunications Union
MICT	Ministry of Information Communication Technology
MOD	Ministry of Defence
MTC	Mobile Telecommunication Company
NAMPOL	Namibian Police
NCIS	National Intelligence Service
NCSS	National Cyber Security Strategy
NFC	Near-field Communication
NUST	Namibia University of Science and Technology
OECD	Organization for Economic Co-operation and Development

OMA	Offices, Ministries and Agencies
OTP	One-Time Pin
PC	Personal Computer
PCW	Pricewaterhouse Coopers
PIN	Personal Identification Number
Q4	Fourth Quarter
SADC	Southern Africa Development Community
SCO	Shanghai Cooperation Organization
SIM	Subscriber Identity Module
TELECOM	Telecommunication Company, Namibia
UDHR	Universal Declaration on Human Rights
UN	United Nations
UNSC	United Nations Security Council
USA	United States of America
WACS	West Africa Cable System
WHK	Windhoek, Namibia
WSIS	World Summit on the Information Society

CHAPTER ONE:

INTRODUCTION

1.0 Background of the study

The evolution of information technology has brought many successes to the world. People and businesses depends on computers and mobile phones to communicate through the internet, conducting financial transactions, read information, interact via social media any time. However, this progress is being confronted by the ever increasing crime that is present with technology. A conventional crime, for example breaking into the bank to get money or in an office to get information has been there, but present technology has made these activities easier to commit. Computers and mobile phones are being used by criminals to steal information from consumers and profit from it. Computer-related crime and cybercrime have become a significant global challenge and more a concern for national security. With the advent of new technology, criminals are using the opportunity to infiltrate and attack businesses through their computer systems. For instance, the Namibian police (NAMPOL) report contains hundreds of thousands of registered attempts to interfere with, or illegally access, computer systems each day. Hundreds of new computer malicious software and viruses are detected every month which is a challenge to computer users, and even to deploy countering measures is difficult because of limited skills.[1] The compromised computer systems affected database with records for approximately 80 million people and business information every day.[2] This action is called data breach and is controlled by different criminal groups; the most powerful Internet services can be attacked. A data breach is commonly defined as the unlawful and illegal gaining of personal details that compromises the

[1] Isaac Ben-Israel and LiorTabansky, *"An Interdisciplinary Look at Security Challenges in the Information Age,"* (Military and Strategic Affairs 3, no. 3, 2011), p 24.

[2] Elizabeth Weise. *Massive breach at health care company Anthem Inc*. (USA Today, Feb 2015) p 5.

security, privacy or integrity of personal details.[3] Such threats are expansive, both in quantity and quality for the reason of the growing persistence and stealthiest of cybercrime.

Cybercrime causes various damage such as loss of business classified intellectual property and information, opportunity costs; including service and employment disruptions, and reduced trust for online activities. It also disrupts services or damaged systems to a state, its citizens and organizations. In total, it costs the world 2.4 billions of dollars in 2015.[4] The scope of such damage is difficult to ascertain because various damage estimates submitted in the debate are largely unreliable and exaggerated. But even without agreement on the scope and damage incurred by citizens, organizations, and states, the responsibility rest with the state to act in response to the available chances and challenges of the reality as it unfold, given the implications cybercrime causes on these entities. As cyberspace persistently enters into every daily business of life, it put huge demands on the state to assure personal and national security.[5] Cyberspace by nature dictates to the state to enlarge its involvement extensively.

Obliviously, the framework of state involvement in cyberspace operations has been emerging in the 21st century, and one of the encumbered issues being the mutually contradictory values of privacy and national security. In a democracy, the process for formulating a government policy including on cybercrime involves public debate, political scuffles, and long term legal treatment.[6] More so, cyber-criminal groups are known to present resources, infrastructures, and even low charge of their service to customers. They did so because in the process they install backdoor which they can use to enter those systems and get information they want. It's importance is even greater because of the prevalence of impending elements of danger

[3] Ponemon Institute, 2014 Annual Study: U.S. Cost of a Data Breach, p 6.
[4] Donnelly, L. *Civil Penalties for Cybercrime Lag Behind Hackers' Habits*. (The New York Times, 2013) p 8
[5] Shinder D. L. and M. Cross. Scene of the Cybercrime (*Burlington, MA: Syngress, 2008*) p 11.
[6] Wall, D. Cybercrimes: The Transformation of Crime in the Information Age (Cambridge: Polity, 2007), p 10.

capable of acquiring cyberspace weapons and recruiting 'fighters' on the cyber-criminal black market.[7]

In Africa, the AU Convention on Cyber Security and Personal Data Protection, 2014, Article 27 sections (a) and (c), states that:

> "Each State Party shall adopt the necessary measures to create an appropriate institutional mechanism in charge for cyber security governance" and that, "cyber security governance should be set-up within a national framework that can respond to the alleged challenges and to all matters concerning to information security at national level in as many areas of cyber security as possible."[8]

This suggest that states have responsibilities of addressing cybercrime within its sovereignty. As the high authority with the constitutional power, state has to make structures within its authority and ensure that all institutions and ordinary users are well informed and organized to engage in the campaign to mitigate crime including those happening in cyberspace. Despite government efforts, the Chief Information Officer, Kleinntjies was quoted on July 2016, to state that "Namibia might be a small country known to only a few people internationally, but became a popular target for cybercriminals to practice their trade," According to him, by December 2015, Namibia was identified as the top African target for cybercriminals by Check Software technologies.[9]

This target by cybercriminals in Namibia can be ascribed to the very good communications network which allows criminals access to move information and money away from the country. Other reasons are that its thriving banking sector with multiple points of presence country-wide and internationally via Automatic Teller Machine (ATM) networks offers

[7] Wall, D. Cybercrimes: The Transformation of Crime in the Information Age (Cambridge: Polity, 2007) p 11.
[8]AU Convention on Cyber Security and Personal Data Protection, 2014, Art 27(a & c), p 9.
[9]Kleinntjies, B. '*Namibia a Top Destination For cyber Criminals*". (Bankwese, 6th July 2006, Republikein*) p 4.* Available at http://www.republikein.com.na/nuus/namibia-a-top-destination-for-cyber-criminals/

opportunity to commit crimes. Furthermore, laws that focus on dealing with and bringing cybercriminals to the court of law are inadequate. Another impeding thing is that there is a limited capability of pro-actively observing and averting such attacks. Henceforth, it is required that security operatives fast-track the efforts set in place in combating cybercrime. Though the Namibian government is still engaging in the process of drafting the Electronic Communications, Data Privacy and Cybercrime Bill tabled for approval in parliament, there is real danger on its state security being targeted. The deliberation on the bill is still not yet completed after four years of debate, which obviously indicate that there are technical challenges that hold up its approval.

1.1 Statement of the Problem

The implication of cybercrime for national security is derived from the way technology is used by individuals or groups of people, known as cybercriminals, who uses computer networks to attack other people's computers systems to commit wicked deeds, such as scattering viruses, data theft, identity theft, hacking and espionage. Many African countries have well-developed internet networks that make it affordable in relation to Information Technology (IT) security. These systems are then used by criminal to access through backdoor, into larger countries or organizations network systems. By definition, backdoor is an unapproved technique of acquiring entrance to a folder, online service or whole computer system. A backdoor is inscribed by the computer programmer who generates the code for the program which is only known by the programmer which is an impending security threat. [10] Cybercriminals target weaker security

[10] McAfee. *The Economic Impact of Cybercrime and Cyber Espionage*. Center for Strategic and International Studies. (Santa Clara, Mission College, July 2013) p 9.

controls. In Namibia, cybercriminals target mobile devices through which they can access sensitive data. Similarly, there are records of high rate incidents of card fraud. In these incidents, victims lose private information, money and other valuable goods through illegal online activities, and had caused public outcry. Namibia being rated the top targeted state by cybercriminals in Africa brings to focus the need to for this study to analyze the existing state of cybercrime, with regards to national policy and laws, and its impacts on the nation's national security.

1.2 **Research questions**

The study endeavored to answer the following questions.

1. How effective is the legal and policy framework to mitigate cybercrime in Namibia?

2. How effective is the policing of cybercrime offences in the country?
3. Does Namibia have the required equipment as well as human resource to manage cybercrime?
4. How effective is the inter-agencies cooperation in detecting and respond cybercrime related incidents?

1.3 Objectives of the study

The main objective is to analyze international cybercrime and Namibia's national security. Below are the specific objectives.

i. To Scrutinize the interconnectedness of international cybercrime, and how it affects the international security.

ii. To analyze the impacts of international cybercrime on Namibia’s National Security.

1.4 Literature Review

This section highlights the scholarly conceptualization of cybercrime and its global application. The section will therefore look at cybercrime and also the repercussions of cybercrime on national security.

1.4.1 The Conception of International Cybercrime

Definitions of cybercrime mostly vary upon the reason of applying the term and the variety of specialty of the studies. The core of cybercrime is confined to acts against the secrecy, integrity and accessibility of computer records or systems. Further than that, though, cybercrime is associated with computer-related activities aimed for private or financial benefit and to do harm to the person or system. Cybercrime is also associated with harming of personal identity in addition to computer data content manipulation amongst other incidents also fall in the grouping of a wider sense of the phrase ‘cybercrime’. Meanwhile, a definition of cybercrime is wholly not as relevant for other purposes, such as defining the series of unique assessment and international cooperation, which focused more on electronic proof for any crime, instead of a broad, ‘cybercrime’ concept.

In this context, numerous academic works, for example, by Yar and Rosenbach[11] made effort to describe ‘cybercrime.’ National legislations, however, does not seems concerned with a strict definition of the word. Out of almost 200 items of national legislation cited by countries in reaction to the Study questionnaires, fewer than five percent used the phrase ‘cybercrime’ in the title or scope of legislative provisions.

[11] Majid Yar, Cybercrime and Society, (New Delhi: Sage, 2006) p 58.

Rather, by regulation, the common phrases used are; electronic exchanges, 'computer crimes, information technology, or 'high-tech crime.'[12]

Practically, many of these pieces of legislation recognized criminal offences that are incorporated in the theory of cybercrime. The common ones are interference with a computer data. Where the title of national legislations did precisely use cybercrime in an act or section (such as 'Cybercrime Act'), the section that defined the legislation seldom incorporated a meaning for the word 'cybercrime.' When the phrase 'cybercrime' is incorporated as a authorized meaning, a collective approach was to describe it simply as 'the crimes referred to in this law.'[13]

Indeed, as technology has developed so have also the meaning of computer crime. Yar and Rosenbach opined that when defining computer crime, the particularity, the knowledge or the application of modern technology is put into consideration. The Organization for Economic Co-operation and Development (OECD) Guidelines on Cyber security of 2002[14] included a working definition as a basis for the study: United Nations member states declared computer crimes related to the use of computer as unlawful and unethical. Similarly, they declare illegal behavior involving the habitual processing and the spread of data without the owner's consent. OECD Recommendations of 2002 adopted a functional approach and computer connected offence as calculated and explained in the proposed guidelines or recommendations for national legislators. In the 1995, the Council of Europe Recommendations on Criminal Procedural Law, used offences as the tem connected to the Information Technology" (IT offences or IT crimes).

[12] Ministry of ICT. Computer Crime Act 2007, Colombo. Sri Lanka p 30.
[13] Oman, Royal Decree No 12/2011 issuing the Cybercrime Law; p.11.
[14] The Organization for Economic Co-operation and Development (OECD) Guidelines of Cyber Security of 2002, p5.

The Council in its recommendation further defined IT offences as: encompassing a unlawful offence. In the final analysis, the investigating powers that be have to get right to information being possessed or conveyed through computer systems, processing through systems electronic data.

Similarly, there are no specific international officially authorized instruments that described cybercrime. International organisation such as the Council of Europe Cybercrime Convention, The Draft African Union Convention, and the League of Arab States Convention,[15] contained a definition of cybercrime, but not accepted world-wide. Similarly, the Commonwealth of Independent States Agreement uses the term computer information' to describe related offences.[16] Likewise, the Shanghai Cooperation Organization Agreement alluded to 'information offences' as 'the exploitation of information property that impact on it in the informational sphere for illegal purposes.'[17] The definitional methodologies derived from national, international and regional instruments inform the method adopted by this Study.

As such, the phrase 'cybercrime' is not measured as a legal term. It is notable that this is equivalent to the approach adopted by international instruments such as the United Nations Convention against Corruption. This tool does not define 'corruption', but somewhat helps States Parties to forbid a specific set of conduct which can be more effectively described.[18] For that reason, 'cybercrime' is henceforth best reflected as a anthology of conduct.

Scholars such as Alec Ross, and bodies for instance, the African Union tried to describe notions such as 'computer', 'computer system', 'data' and 'information,' but until then, nothing was agreed, therefore it is helpful to examine descriptions surrounding these concepts. Their

[15] Draft African Union Convention, Part III, Chapter V, Section II, (2000) Chapters 1 and 2

[16] Commonwealth of Independent States Agreement, Art. 1(a), p 6.

[17] International Telecommunication Union. Understanding Cybercrime: A guide for Developing Countries, 2011, p .22.

[18] United Nations. Convention against Corruption, Art 15, 2004, p 9.

meaning is fundamental to understanding the objects and/or protected legal interests which cybercrime acts concern. [19]

Some tools that are used intercontinental concerning cybercrime covers the narrow description of the data as the crime object.[20] Others address a wider variety of transgressions, comprising acts where the crime object is a person or value, as opposed to a computer data, even if the information system is nonetheless a central part of the formula of the offence.[21]As the world moves towards an 'internet of things' and nano-computing, descriptions such as 'computer system' or 'information system' will likely be interpreted as encompassing a variety of devices. In principle, however, the nucleus of 'automated processing of information' would likely be sufficiently flexible to include, for instance, a monitoring and control smart chip with Near-field Communication (NFC) and Internet Protocol (IP) connectivity, embedded into a household appliance.

In many countries, the eruption in global connectivity appeared at a time of economic and demographic revolutions, with rising income disparities, tightened up private sector spending, and reduced financial liquidity. Over-all, experts the study interviewed perceive increasing incidents of cybercrime, as driven by profit and personal gain, as both individual and planned criminal groups exploit new opportunities. The research shows that 80% (per cent) of cybercrime offences start off in some form of well thought-out activity, with cybercrime black markets set-up on a cycle of virus software creation, that infect computer through botnet running, gathering on private and financial data. They then start to sell data and profited from this financial

[19]EU Decision on Attacks against Information Systems and Commonwealth of Independent States Agreement, Brussels, 2010, p. 30.

[21]ECOWAS Draft Directive, Art. 17 (Facilitation of access of minors to child pornography, documents, sound or pornographic representation), in Pocar, F. New challenges for international rules against cyber-crime. (*European Journal on Criminal Policy and Research*, 2014)10(1): pp27-37.

information. [22] As technology develops, it becomes less complex such that cybercrime committers require less skills or techniques.

In the developing country context in particular, there emerge a sub-cultures of young men who are technical savvy and engaged in computer-related financial fraud, due to unemployment and some of these participates in cybercrime from teenage years. [23]

Worldwide, cybercrime activities show an extensive expansion across spectrum and driven by financial needs as well as acts against the privacy, integrity and accessibility of computer systems. Risks and threats vary between Governments and business sector enterprises. Many countries view their systems of police recorded statistic as inadequate. Police-recorded cybercrime cases are at most linked to the levels of country technological growth and expertise of police. It could also be said that developed countries invested heavily in prevention of cybercrime, and therefore have well developed systems and experts.[24] Besides, to its socio-economic benefits such as linking the world together and facilitate trade and other benefits, the internet system can be used for criminal activities just as with other means enhancing capabilities of human interaction. While computer-related crime, or computer crime, is a comparatively long established phenomenon, the advancement of international connectivity is intrinsic to contemporary cybercrime. Other activities related to physical damage to computer gadgets and destroying of stored data; Further unlawful use of computer systems and the exploitation of

[22] Yar, M., The novelty of 'cybercrime': An assessment in light of routine activity theory. *(European Journal of Criminology, 2005*).2 (4): pp 407- 427.

[23] Koops, B. J. The Internet and its Opportunities for Crime. In: Herzog-Evans, M., (ed.) *Transnational Criminology Manual*. (Nijmegen, Netherlands: WLP, 2010.) pp.735-754.

[24] Ibid p. 754.

electronic records are some of computer-related fraud.[25] That has been acknowledged by the UN as criminal offences ever since the 1960s.[26]

In 1994, the United Nations Manual on the "Prevention and Control of Computer Related Crime" indicated that incidents can be classified as common computer manipulation; harm to or alteration of computer programs; computer forgery; unlawful right to use computer service; and unofficial duplication of officially sheltered computer program.[27] While such acts were often considered local crimes concerning unconnected or closed systems, the international dimension of computer offense and related criminal legislation was recognized as early as 1979. INTERPOL laid emphasis on the nature of computer crime worldwide, because of the progressively increasing communications by telephones, satellites and more, between the diverse countries. The main concept at the heart of today's cybercrime remains exactly that, that is, the idea that joining globalized information communication technology can be utilizing to commit illegal acts, with transnational reach. These activities has a potential to embrace all crimes committed through listed earlier, on top of many others, such as those associated with internet content for private or financial benefit. Placing the focus on worldwide connectivity does not omit crimes involving unconnected or closed computer systems from the range of cybercrime.[28] While officials of laws maintenance agencies in industrial countries have capacity to identify a

[25] Glyn, E.A. *Computer Abuse:* The Emerging Crime and the Need for Legislation. *(Fordham Urban Law Journal*, 12(1),1983):pp73-101. 20 Schmidt, W.E., Legal Proprietary Interests in Computer Programs: *The American Experience. Jurimetrics Journal, 21*:(1981) p345.

[26] INTERPOL. Third INTERPOL Symposium on International Fraud, Paris (11-13 December 1979) p 15

[27] United Nations, UN Manual on the Prevention and Control of Computer Related Crime, 1994, p20.

[28] Jaishankar. K., Expanding Cyber Criminology with an Avant-Garde Anthology. In: Jaishankar, K., (ed.) Cyber Criminology: Exploring Internet Crimes and Criminal Behaviour. (Boca Raton, FL: *CRC Press*, Taylor & Francis roup, 2011), pp103-120.

high percentage of cybercrime with a transnational motives, those in developing countries are deficient of the capacity to identify cybercrimes.[29]

On the one hand, it shows that perpetrators of cybercrime in less industrialized countries pay more attention on domestic incidents that happen on their computer systems. On the other, it could also be the case that, due to capacity challenges, these incidents are hardly detected or engage with, except in cases where foreign service providers are engaged or potential victims linked with international cases.

Even so, it is essential to consider the global connectivity as important in global peace and security, as many interactions is taking place through this media.

As IP traffic grows in cyberspace,[30] traffic from wireless devices exceeds traffic from wired devices, and as more internet traffic originates from non-Personal Computer (PC) devices, it may become unbelievable to imagine a ‘computer’ crime without the effect of Internet Protocol (IP) connectivity. The emerging of mobile devices for private use of, and the surfacing of IP connecting homes and offices, means that electronic data and transmissions could even be generated by, or become integral to, almost every human action, whether legal or illegal.

1.4.2 The Correlations between Cybercrime and National Security

National security studies have advanced over time. Traditionally, national security involved only a state’s military aggression and self-protective capabilities, thus focusing only on the external threats to a state. The notion of national security has broadened to include other sectors that form the interior changes of a state such as social, economic, societal, environmental and political

[29] Kigerl, A. Routine Activity Theory and the Determinants of High Cybercrime Countries. (*Social Science Computer Review, No* 30 (4), 2012): pp 470-486.

[30] Kigerl, A. Routine Activity Theory and the Determinants of High Cybercrime Countries. (*Social Science Computer Review, No* 30 (4), 2012) p. 470.

issues. National security developed overtime to include the individual as an item of security. This has seen national security concept become enlarged into five additional sectors: military, political, societal, environmental and economic issues. This idea originated from the Copenhagen school of international studies. The idea brought about the significance of the individual as an object of security, where the individual, such as cybercriminals and their activities thereof, can as well be a source of insecurity[31]

Accelerating the pace of political, social, economic and technological change in today's world, conventionally ascribed to globalization is essentially changing the character of threats to national as well as international security.[32] Media, internet and increased people's mobility and made the world look smaller, compressing space and time, and bringing events happening from distant to closer even without crossing borders physically. However, this contributes immensely to the expansion and awareness on threats of present and future conflicts in various directions of the world. Events that are happening far away have come nearer to us through the interconnectedness of the world.[33] Despite this, technology advance has enhanced a complicated and challenging security for both individual and national. Technology and its advancement has changed how wars are fought, and complicated how they are combated. For instance, terrorism heavily relies on advanced technology for cyber attacks on governments, recruiting and projecting its ideologies in addition to reporting. The tricky situation of cyberspace is its invisibility, where a network collective used by client who cannot see each other's.

[31] Buzan, B. People, Fears and States: An Agenda for International Security Studies in the Post-Cold War Era, (*Boulder, CO: Lynne Rienner Publishers,* 1991) p10.
[32] Alam, S.M. Shamsul, "Globalization and its Discontent: The Dialectics of World Development and the Emergence of New Social Movement," (*Journal of Developing Societies 2003*), p 40.
[33] Victor D. 'Globalization and the Study of International Security', *Journal of Peace Research*, Vol. 37, No. 3, (2000), pp.391-40.

The notion of national security underwent significant transformation in recent years.[34] Gone are the days when a country's main security threats were physical appearance within its border in nature and purely military in solution. No longer does a country require a physical or military invasion to happen to be declaring a threat to domestic security matters such as public health, national economy, or social cohesion. In this case cybercrime fill the gap as a type of crime that represents such new capability.

As earlier described, this crime take place through "computers which is connected to the Internet, meaning that the internet is the driving force behind cybercrime.[35] cybercrime characterizes globalization through scale, speed, and cognition.

Cyberspace is a medium that increases significant the velocity in information transfer, to allow interlink speeds to be almost instantaneous. It complexity has reached levels never witnessed before demonstrating a grave threat to society. The perception for how long things take to happen has reduced ominously appropriate to the speed in which cyber technology is advancing. Criminal gangs are also responding to the pressure placed upon such activities by law enforcement reorganizing their operations and attracting a new age group of coders and cyber specialists. The concept that the world is a global village has influenced how countries now view security.

In a globalized and cyber dependent world, there is increased vulnerability of assault on the system, at any time, from anywhere, in a whole manner of different ways at an incredible speed. The relatively low operating costs of cybercrime exemplify why cybercrime posing a direct menace to national security. Government, infrastructure, intellectual property, and personal information are all hypothetically threatened. These types of threats are significant to

[34] Grabosky P, Organized crime and national security. (Canberra, Australia: Regulatory Institutions Network, 2014) p.142.

[35] Birchfield, R. Cyber threats and data privacy. (New Zealand Management April, 2013) pp 46-51.

state security because of its potential for substantial distraction or damage to the functioning of Namibian society.[36] This is of meticulous concern when one considers that these threats are not only posed by other states who have abundant resources at their disposal but by rogue individuals who need only the know-how and entrance to a computer. This is seen as a potential threat.

One of the important matter close to the deliberations as to whether cybercrime should be reflected as a danger to national security its classification. Cybercrime, similar to transnational crime incorporates an array of crimes not all of which are seen as possible risk to national security.

Cybercrime generally includes crimes such as fraud, terrorism, child exploitation, hacktivism, money laundering, and intelligence collection. Grabosky offered the difference between planned and unplanned cybercrime when he discussed national security, suggesting that it's not inherently the organization that makes these groups a national security threat, instead it is their aims or motivations.[37] Furthermore, Rosenbach and Belk argue that separating cybercrimes into groups based on incentive better aids the people that have to manage it.[38] Therefore, by classifying cybercrimes into groups, a specific group of individuals or a government department can be given the duty of dealing with that crime, using specialists with the necessary skill in that particular field.

Nonetheless, in order to categorize and respond properly to cybercrimes, the motivation behind the crime must be known and understood. For example, hacktivists belonging the group

[36] Burke R.H, An Introduction to Criminological *Theory*. (Oxon, England: Taylor & Francis, 2009), pp 20-35.

[37] Op Cit, Grabosky, p 167.

[38] Rosenbach E and Belk R, U.S. Cybersecurity: The Current Threat and Future Challenges. In N Burns and J Price (Eds) *Securing Cyberspace: A New Domain for National Security*. (Washington, DC: The Aspen Institute, 2012), pp. 39-43.

called Morrocan Explorer put down the network of Namibian government including the Parliament in protest of the government of the republic of Namibia's support of the Polisario Front Liberation movement.[39] In this case, hacktivism is the action of infringing into a computer system, in demand of politically or socially amenities. The hacktivist referred to an individual who carry out an act. Terrorists can use similar method in seeking to damage critical infrastructure, or a conduct of corporate espionage committed by a rival power company seeking to increase its influence in the market. While it is advantageous to have specialist groups to engage with certain cybercrimes, the skill to accurately demarcate them into groups proved almost impossible. Occasionally, motivations are not definable for analysis, particularly if the perpetrator cannot be located or simply chooses not to claim responsibility.

In Africa, the contemporary situation in the continent has been captured by the aphorism "Africa rising", reflected in the continent's expanding middle class and quick embracing of mobile technology.

According to recent estimates by the International Telecommunications Union (ITU), the total of mobile subscribers in Africa reached 63% in 2013, and over 16 % of the African population are now using the Internet.[40] Furthermore, ITU estimated that the total worldwide value of web-based retail sales for 2013, amounted to $953 billion, while business to consumer (B2C) e-commerce sales for the similar period totaled $ 1.3 trillion.[41] Although the e-commerce market is controlled by developed economies, the global share of e-commerce for Africa is expected to rise from 1.6 per cent in 2011 to 2.3 per cent by 2016. However, new challenges ascend together with growth, and growing technological exposure

[39]

[40] International Telecommunications Union, "ICTs facts and figures 2013" and, ITU Telecommunication Development Bureau (Geneva, 2008) pp 25-30.

[41] Goldman S. "e-Commerce expected to accelerate globally in 2014", (*Equity Research, New York, The Goldman Sachs Group, Inc.,* 5 March 2013) p 2.

1.5 Justification to the Study

The study of the link of cybercrime to national security is progressively established, as technology advancing, so too is criminal's capacity to cause harm and infuriation to individuals and a nation's critical infrastructure. Cybercrime is becoming a major worry for the 21st century, relative to both deterrence and exposure of the rising number of interrelated activities. In fact, cybercrime is the fastest-growing area of cross border crime. States the world over are increasingly dependent on digital networks and the opportunities for engaging in cybercrime are increasing, as the computer gradually grow into a vital component of commerce, entertainment, and government. Cybercrime attach is affecting essential services world-wide as it increases its attack on every nation. It is essential for every nation to be alerted so as to recover on time as this attack can affect essential services such as hospitals service. In fact such attack happened in May 2017, when hackers used ransomware to paralyzed essential services in 99 countries and mostly affecting Russia, Ukraine, India and Taiwan.[42] This type of threat is the highest in Namibia, where the opportunities for carrying out cybercrime are growing exponentially posing a vulnerability to the country's national security.

It with this conscious in mind that this study will therefore benefit the existing cyber war efforts in Namibia by the governments and societies that focus on the internal dynamic forces of technology, manage cyber security and connectivity within the states, its communities and creating resilience from cyber-attacks. The conclusions and recommendations will therefore inform policy makers.

[42] Ashford, W. NHS hospitals hit in global ransomware attack. Computer Weekly.com obtained on 14 May 2017 from http://www.computerweekly.com/news/450418720/NHS-hospitals-hit-by-suspected-ransomware-attack

1.6 Theoretical Framework

This study uses Barry Buzan and OleWaever's approach to securitization from Copenhagen School of security studies. This approach represents the core of the International Relations as the main methodology to understand how the security actor has to mitigate the phenomenon. It also used a Routine Activity approach, by Cohen and Felson.[43]. Routine activities approach is an environmental, place-based clarification of criminality, where the interactive forms and meetings of people in space and time effect when and where crimes ensue through which to comprehend the motivation behind cybercrime. The two methodologies converged to give a proper considerate of the study.

The securitization approach's main argument of is that security is seen from the traditional view, that is from global, state, and individual perspective. It has to concern about economic, health, education, employment and anything that concern society. The government leaders are main actors and has to pronounce the existential of threat that has to be securitized, to ensure that security is provide to everything that need it. The approach follow a 'speech act' by leaders when pronouncing something a security issue that it becomes one'.[44] By stating that a particular referent object is endangered in its existence, a securitizing actor acquires a right to extraordinary actions to ensure the referent object's survival. For instance, the president of Kenya declared cybercrime a national security threat in his address to NDC, Kenya on 3rd May 2017.[45] This calls for polices design to address the particular threat.

[43] Cohen, L. E. and M. Felson. "Social Change and Crime Rate Trends: A Routine Activity Approach." (*American Sociological Review, Volume Number: 1979)*, pp 44-04.

[44]Wæver, Ole. 'Aberystwyth, Paris, Copenhagen: New Schools in Security Theory, 2004, p 21.

[45] Kenyata, U. "Securing Kenya's prosperity in a dynamic threat environment". A lecture delivered to NDC, Kenya, on 3rd May 2017.

Busan look into the security as a social and inter subjective construction.[46] It also implied that an elected government has enter into agreement with the citizen to provide it with security, therefore it has a vital role in designing procedures to address security challenges. Based on this approach, governments are then responsible to lead to in ensuring that there is sufficient instrument to address cybercrime. The effective way is the multi-sectoral approach where different department are put together to tackle an issue.

This approach implied that not all issues are securitized, therefore the procedure of identifying those securitized entails three steps; which are:

a) Identification of existential threats;

b) If the threat can be addressed immediately; and

c) The consequence if the threat is not addressed. [47]

The approach urged a pro-active measure to avoid an issue become an existential threat: If this issue is not attended to while at infancy stage, everything else will be irrelevant because when it expand it will be impossible to deal with.[48] For example, if a gang of card fraudsters is allowed to steal from card holders, it can sway away people to use the service which could be beneficial for people to avoid carrying huge stash of money which is a risky. This is the first stage on the road to a successful securitization and is called a securitizing move. State as paramount actor leads all stakeholders to discuss and identify what should be securitized so that available resources can be allocated since only when an actor is convinced about an audience legitimate need can go yonder then compulsory rules and guidelines of securitization.

[46] Buzan, Barry, Ole Wæver and Jaap de Wilde Security: A New Framework for Analysis, (Boulder, CO: Lynne Rienner, 1998) p 30.

[47] Kenyata, U. "Securing Kenya's prosperity in a dynamic threat environment". A lecture delivered to NDC, Kenya, on 3rd May 2017

In practice, particularly to Namibia's cybersecurity concerns and efforts, securitization is thus far from being open to all units and their respective subjective threats.

Rather, it is essentially centered on who takes charge and whether that entity has the capability to identify and respond. This silo approach has proven ineffective and exposed the weakness in system and therefore means socially and politically it construct a threat. The learning of security is wide-ranging, thus challenging in selecting those issues to be securitize. These issues range from different sectors such as military, societal, economic and environmental. The issue should able to fit in the theoretical expression. Thus the securitization of the menace of cybercrime is important such that leaders are required to pass laws and actualize a set of measures to address cybercrime in Namibia, before the matter is out of hand. This is so because, Namibia like many less industrialize countries has not yet securitized cybercrime. given the threat it poses on its national security.

Conversely, the Routine Activity process is a criminological methodology that was propounded by Cohen and Felson.[49] This approach predicts that crime occurs when an inspired criminal get access to an appropriate object in the absence of a protector that could potentially thwart the lawbreaker from committing crime. A motivated offender assumes that benefit override loss in the action, as the chance of being arrested and even arrested is minimal or literally low. The suitable target here refers to an institution such as bank or government department, while the capable or appropriate protector refers skilled personnel and appropriate laws or CCTV systems to deter criminals. This approach proposes that crime happen when three conditions must take place at the same time and also in the similar space. The approach also posits that differences in crime rates could be explained by the supply of suitable targets and

[49] Cohen, L. E., & Felson, M. Social change and crime rate trends: A routine Activity Approach. American (Sociological Review, 1979), pp 28-36.

capable guardians and from their understandings, the theory is somewhat unclear about the role of the supply of motivated offenders.[50] The assessment of the situation determines whether or not a crime takes place. Routine Activity method positively relates to cybercrime heedlessly of the category. Accordingly, organized cybercriminals are motivated to fulfil their political bias, such as fundamentalism, while professional hackers are driven by the stench of money. According to Wamala, these kinds of hackers are mostly employed to hack the site of the rivals and get credible, reliable and valuable information.[51] A lack of cybercrime awareness, relevant laws, infrastructure and capable human capacity to monitor cybercrime happenings in the country makes Namibia a suitable target. It is paramount to point out here that, a commitment is required from government and other interested party to intensify the awareness campaigns about this danger and to prepare the nation into digital world.

[50]. Cohen, L. E., & Felson, M. Social change and crime rate trends: A routine Activity Approach. American (*Sociological Review*, 1979), p 28

[51] Frederick Wamala. The ITU National Cybersecurity Strategy Guide, ITU, (2011), p 40.

1.7 Hypotheses

a. The announcement of national cyber security policy will mitigate cybercrime incidents because it empowers the law enforcement to control cybercrime happenings in the country.

b. The pronouncement of national cyber security policy will not reduce cybercrime incidents in the country because technology is developing fast such that laws are chasing the moving target.

1.8 Methodology

The study uses a qualitative method intended to collect initial and comparable records in a complex area while capturing the diversity of diverse settings and levels of exposure to cybercrime and national security.

1.8.1 Data

Primary data were obtained through a semi-structured interviews with key informer from government employees, institutions and individuals in Namibia who are well vested in the arena of international security and technology among other relevant fields. The researcher contacted the following Departments and agencies; Ministry of Information Communication Technology (MICT), NAMPOL Special Branch, Ministry of Defence (MOD), National Intelligence Service (NIS), Communication Regulatory Authority of Namibia (CRAN), Bank of Namibia (BoN), Anti- Corruption Commission (ACC), local banks and ITU local consultants. The study design was an exploratory design which used interview guides to gather qualitative descriptions. Each guide addressed a particular objective. It was administered to the interviewees from the sampled groups. By using qualitative techniques, the design enabled the researcher to obtain valuable understandings of the phenomenon.

This study was drawn from subordinate sources of information. A subordinate sources of data used are such as; cybercrime statistics, government policies, government publications and other written material about Namibian cases. These data were sourced from a collection and reviews of published data and unpublished material, journals, academic papers and periodicals. It was taken through intensive and critical analysis.

1.8.2 Data Collection

The consultations were conducted using pre-tested interview questions that were administered to the study population. This involves using various individual and institution from different areas and spreading the figure in all the sites to gather data. The interviews cut across the study population which included; government employees, individuals and organizations in the arena of international security and technology among other relevant fields.

1.9 Chapter outline

This research study comprises five (5) chapters. Chapter 1 gives a general introduction of the study, bringing out the statement of the problem, objectives, justification, literature review, as well as theoretical framework. Chapter 2 is about a synopsis of International cybercrime and analyse the effect of cybercrime on the international discourse. Chapter 3 brings out an overview of the impacts of international cybercrime on Namibia's National Security. Chapter 4 covered the critique through cybercrime and cyber security analysis, and finally, Chapter 5 contains discussion of findings, conclusion and recommendations.

CHAPTER TWO

AN OVERVIEW OF INTERNATIONAL CYBERCRIME

2.0 Introduction

Cybercrime is an international phenomenon which emerged with the advent of information technologies. As innovation takes a toll on virtually all areas of human endeavored, it also developing rapidly and spreading widely. This chapter will venture on the overview of international cybercrime focusing specifically on incident being encountered and mitigating measure that is in place. It will examine the effectiveness of legal framework available and suggest gaps that require action.

Cybercrime is committed when hackers goes in the network system, look for other network and keep on spreading until it got what they want. The recent breakthrough of hackers that shocked the world in May 2017, was caused by ignorance. Cardona stated that hackers entered into the international internet network system because users failed to update their systems although Microsoft provided them with new updates.[52] The effect was that it disrupted many services around the world. In UK, hospitals doctors turned patients away because computers were affected. It showed that even well developed countries which invested heavily in technology can be victims if they ignore the laws.

The world is becoming closer and inter dependencies become more significant in all facets of life. These changes create actual opportunities to achieve economic success, prosperity, political freedom, and promote international peace. Conversely, it produces dominant forces of

[52] Cardona, N. Hackers launch a massive cyberattack. Obtained 14 May 2017, from ; https://www.msn.com/en-us/sports/more-sports/new-justice-department-move-will-send-more-people-to-prison/vp-BBB3FB7

social destruction, forming serious weaknesses, and spreading the seeds of ferocity and conflict. Economic crisis transcends the state boundaries and are creating global suffering.

As alluded to in chapter one, the conception cybercrime is used to largely define illegal activities in which computers and networks are an instrument, an object, or a location of illegal action and possess all possible tools, appliances and electronic gadgets which enabled them cracking the networks. Serious incidents recorded are Denial of Service attacks (DoS).[53]

Cybercriminals are taking this benefit by using the infrastructure provided for by globalization to reach places where the law is weak. Most dangerously, the threat become worldwide in space and severe in its effects as a consequence of the spread of knowledge, the dispersion of advanced technologies, complemented by the free movements of people. This chapter discusses the special effects of international cybercrime by comparing works of various researchers on the topic.

2.1 An Overview of Cyberspace

Cybercrime is a crime that is committed using cyber means. Through the cyber means you conduct speech, espionage against other countries. You steal money from the bank, information from office computers and conduct other activities. The ministry of ICT is spearheading the legislation, and setting up of communication infrastructure together with other stakeholders. However, it is a crime that use computer as a vehicle to perform its activities.[54] Since the emergence of internet system, economies joined national security to become reliant upon IT and the information infrastructure, Networks of networks directly support the operations of all

[53].Karamchand, V. An Overview Study on Cybercrimes in Internet. (*Journal of Information Engineering and Applications*,Vol 2, 2012), p 22.

[54] Fred Schreier. Trends and Challenges in International Security: An Inventory. (Geneva Centre for the Democratic Control of Armed Forces. Occasional Paper – №19, 2010) pp140-143.

economic sectors; transportation, energy, finance and banking, defense industries, information and telecommunications, emergency services, public health, food, water, agriculture, postal and shipping. [55] These computer networks took control of physical matters such as electrical convertors, electric train, air and ground traffic control, chemical vats and pipeline pumps that make radars reach yonder the bounds of cyberspace. Globalization and mass popularization of internet network provide new actors today with competences that were until that time only accessible to the largest, most powerful states, challenging the power and steering capacity of major actors. According to Fred, as the Internet reaches all corners of the globe, several countries become incorporated into the World Wide Web and national economies of a rapidly increasing, hence, acquiring both violent and peaceful cyber capabilities.

Similarly, non-state actors will equally acquire certain capabilities. The Copenhagen School of international studies recommended that security players should put effort together to hold back cybercrime. Incidentally, major global exporters of IT and depositaries of IT talent, such as China, Russia, the US, and Israel pose the gravest threats. Scot make reference that China has intensely expanded its level of effort in internet operations worldwide during the past years, and it uses this medium to collect intelligence both economic and military[56]. Routine activity process argued that, crime occurred if there is no guardian which in this case is law enforcement. This calls for a well-established security apparatus in the country. International cybercrime, while itself not new, it has deepened to develop into a more potent factor for change world-wide among other crimes, during recent years, and particularly since the end of Cold War. The terrorist spells on USA, September 11th 2001, highlighted concerns about vulnerabilities of

[55] Fred Schreier. Trends and Challenges in International Security: An Inventory. (Geneva Centre for the Democratic Control of Armed Forces. Occasional Paper – №19, 2010) pp140-143

[56] Scott, J. Understanding Contemporary Society; Theories of the present. (New York. Sage Publications, 2013), p 23.

future attacks. Cyberterrorism become one of those new area of concern, whereby terrorists can use internet system to attack key infrastructures. Key content includes defining security in the global political agenda, military threats posed by states and also by non-state actors, social character and the economy as threats to security, environmental and health threats, terrorism, natural, accidental and criminal threats and cyber security danger which is well thought-out as a new dimension of threat the world is experiencing.[57]

According to Baylis, technology is becoming a challenge when it is used for fraud and money laundry, but it is also a solution to detect thing like corruption and help identify the culprit. Although scholars in the field of international relations such as Baylis recognized and appreciated technology, it is a global phenomenon recognized that make the subject related to national security becomes more complex in the 21st century. Baylis further contends that the amplified complexity poses new challenges to the formulation of state Defense policy.[58] A need arises to balance between the security of a country and the anxiety on human security. Technology reduced boundary and hence, the effect has been positive such that the relationship between states leader become more faster and has reduced the potential for conflict on human security.[59] Nevertheless, it rise to new security paradigm which intensify tensions not necessarily between states but individual privacy. Technology brings the world closer as witnessed by events that occurred world-wide are intertwined. It has immensely expanded the scope of national security border. Obliviously, for nations, communities and individuals alike, security has always meant freedom to pursue a freely chosen way of life without undue threat, interfering or

[57] Powell, B. Is Cybercrime a Public Good? Evidence from Financial Service Industry. (*Journal of Law and Economy*. 2005) p 23

[58] Baylis, J, "*International and Global Security in the Post-Cold War era*". London: Oxford University Press (2011), p 35.

[59] Lynn, D. E, Globalization's Security Implications.*(Issue paper*, Rand. California, 2013) p 3.

uncertainty. Technology generates and exposes weakness to what had previously seemed remote or unconnected.

An assortment of technologies, are evolving rapidly and scattering widely. Trade is increasing worldwide, as is the undertaking of private capital and investment. There is growing inter-dependencies across many facets of life.

Most dangerously, a diversity of threats become global in space and more serious in their special effects as a consequence of the spread of knowledge and expertise, the scattering of advanced technologies, and the free movements of people.

These same progresses, combined with expanding global economic relations, add to some of the complications and resentments that lie at the root of these security threats. Paradoxically, those same facets of technology offer new prospects to achieve economic growth and democracy,[60] and while doing so, advancing the threats as well as some of their underlying causes.

The 11th September terrorist attacks clearly showed the Al Qaeda organization's ability to effectively exploit new communications technologies, and this can happen to the global financial networks, and pose danger to the interaction of people. International community response has also benefited from some of globalization's effects, mostly in technological advances, innovation and in communications systems and in military weaponry. Although it is inconclusive to say definitively, the outcome of these attacks has exasperated the global community and motivated the scientists to find solutions and gradually developed technology to address other things.

[60] Gilpin, R. *The Challenge of Global Capitalism*, (Princeton, N.J.: Princeton University Press, 2000), p 106.

Furthermore, financial dealings receive better enquiry and security steps were introduced to limit the financial mobility of people. [61]

The international spread of technologies and ideas is undeniably facilitating states, and even disgruntled groups, to develop the most-dangerous technologies.[62] So it is fair to question whether a strategy can be designed that can offer any real prospect of preventing cybercrime. But before judgment, a serious analytic effort is necessary to determine the motivating force behind the acquisition of this critical knowledge, materials, and technologies, and whether it could be denied to those bent on acquiring them.

2.2 Global dimension of cybercrime

When cybercrime is compared with conventional crime, there is no much difference as both include conduct, whether by commission or omission, which cause breaching of legal rules and offset by the authorization of the state. According to Chowbe,[63]cyber criminals have been using various Web-based channels to distribute illegal materials such as email, websites, Internet newsgroups, Internet chat rooms; it also includes anything from the simple things like downloading illegal music files, to stealing dollars from online bank accounts.

One common characteristic of these criminals, according to Chowbe, is anonymity. People usually hesitate to provide their real identity information, such as their name, age, gender, and address, as a pre-requisite to participate in cyber activities. When cybercrime is compared with

[61] Grindle, M. S.. “Ready or Not: The Developing World and Globalization,” in J S. Nye and J D. Donahue, (Eds), *Governance in a Globalizing World*, (2010) pp. 184–188.

[62] Bolton, J. “*Beyond the Axis of Evil: Additional Threats from Weapons of Mass Destruction*,” (Washington, D.C, 2002), pp 60-69.

[63]Chowbe V, S. Legal Control of Cyber Crime in India; Problems and Prospects (India, 2015), pp. 12-14

other conventional crimes, the difference is that cybercrime presents diverse risks and rewards to those conventional crimes. [64]

Take for example, a cybercrime where an 'outside' fraudster infiltrates a banking system remotely to steal money, passwords, codes personal information or simply to put an end to someone's computer. There are less risks when compared with physically stealing assets from an organization because the fraudster is not present at the location in person, thus there is slim chance to be detected. There is also slim chance for law enforcement to recognize the wrongdoers or find out where criminals were based when they committed the crime, although this could be detected through detailed analysis which requires experts and the cooperation's with the courts. Usually, the perpetrator is located in a different country through the third country as a pawn to reach the intended target.

That situation rendered it problematic to recognize, detain and accuse criminals by old-fashioned means. Although the most obvious hurdle for victims of cybercrimes according to Donnelly, is catching the perpetrators, victims who surpass this hurdle may be surprised to learn that there is slender chance to succeed in civil court.[65]

Moreover, as Donnelly indicated, the occurrence of this crime is 40 times when compared with classical crime, of which 90 % remains practically undiscovered, because the detection and producing evidence for this crime is exceptionally difficult. In addition, criminals who perpetrate classic crimes realize the power and advantage of computers and they start using them as helping device when committing classic crimes.

Kissling posited that international criminals steal intellectual property (IP), either at the request of a government or for their own use. She emphasized further that even small companies can be

[64] Ibid, p 15.
[65] Donnelly, L. Civil Penalties for Cybercrime Lag Behind Hackers' Habits. (The New York Times, 2013), p 90.

targeted. Estimates of these losses are 10 billion dollars annually. Germany, for example, whose economy is 1/8th the size of world economy, estimated its own IP losses due to industrial espionage at $25 billion to $50 billion, many of which is caused by weak Internet security. Most enterprises hesitates to report harms and may not even be aware of them. [66] Although it is know that more than 80 major companies were victims of cyber-attacks, it is an international practice that hacked companies conceal their losses to avert scaring customers.

The ITU report of 2005 indicated that advanced cyber criminals have the abilities that challenge national intelligence agencies in cyberspace. The report further linked some criminals relationships with their governments, implying that when a new method is designed, criminals are also made aware, which created a thriving black market supports for cybercrime. This create a platform where gadgets like the latest malware can be acquired, learn of recently discovered vulnerabilities, or rent "botnets" (a criminal groups that remote control a group of computers without the awareness of computer owners') [67]. It is also a place where numbers of credit card, personal information, and bank account data can be illegally bought. Some sellers offer guarantees, indicating to be in control.

The financial system is more targeted by cyber criminals. They go after automated teller machines (ATMs), credit cards and online bank accounts. Some crimes of that nature have been remarkable: In one example, a Russian gang took $9.8 million from ATMs over a Labor Day weekend.[68] The chief planner is said to be at large, while his or her identity is not even known. As per Routine Access approach, where law enforcement is weak, cyber criminals are safe.

[66] Kissling, J. Understanding the Damage of Cybercrime. (Lancope, 2011) p 46.

[67] Ibid, p 49.

[68] Lynn, D. E. Globalization's Security Implications. *(Issue paper*, Rand. California, 2013) p 7.

2.3 Cybercrime Tools and Methods

According to Chowbe, cybercriminals are use numerous illegal tools such as *key logging* which imply using software or devices to covertly monitor and record keystrokes, that assisting espionage activities or the collecting of personal data.[69] The other famous method is DDoS attack. Lau *et al* described a DDoS attack as a decided effort by an attacker to avert legitimate users of a service from using the desired resources. The attacker can use several methods such as an attempts to “flood” a network, which implies thwarting legitimate network traffic, by distracting links between two apparatuses, in that way denying right of entry to a service. Likewise this is an efforts to foil a particular individual from accessing a service and an efforts to disrupt service to a specific system or person[70].

Other methods that are being employed are; *pharming* which entails directing traffic from a legitimate Web site to a site controlled by a criminal hacker; *phishing*, a method used to illegally access an individual’s financial data to capture online banking and financial information; and, most recently, *botnets* or networks of infected machines, customarily accomplished by a single command center, that are able to cause serious impairment to networked systems and enabling large-scale identity theft. Hackers obtain botnets commercially, using them to access bank accounts.

2.4 Effect of cybercrime on society

Information technologies and systems are central characteristics of globalization and are becoming progressively important to the operation of many critical systems, such as;

[69] Chowbe V, S. Legal Control of Cyber Crime in India; Problems and Prospects (India, 2015) pp. 12-14.
[70] Lau, F., Rubin, S. H., Smith, M. H., Trajkovic, L. Distributed Denial of Service Attacks. (Burnaby, BC, Canada, 2003), p 44.

communications, transportation, energy, water, electricity and banking. These services are now potential target of cybercriminals thus rendered it vulnerable to the danger of cyber-attacks and disruption. As Rosenbach posited, of the rising number of connected activities, cybercrime has become a major concern for the 21st century, in both prevention and finding.[71] Factually, cybercrime is regarded as the fastest-growing area of crime, where young and old, individual and syndicates excel.

The cybercrime threat has become widespread touching all corners of the globe and affecting various developmental efforts on social, economic and security. As Salifu argues, the internet is a "double edge sword", offering many opportunities for users to develop. On the centrally, it brought with some new opportunities to commit crimes.[72]

Digital networks spread world-wide and all countries are increasing depending on it for commerce and trade. On the centrally, criminals are taking chances to engage in cybercrime, because "the computer" is gradually developing into a dominant component of entertainment, and government uses. This now means the opportunities for engaging in cybercrime are growing exponentially as the number of people utilize hand held devices capable of exploitation and the accessing of private and professional data increases. Crimes such as hacking, fraud, trafficking in child pornography, stealing identities, intellectual property, and violating privacy becomes everyday activities for those involved in committing cybercrime.[73]

Moreover, cybercrime has not created new crimes, simply provided an additional method through which to commit offences such as theft, extortion, illegal protest, and terrorism. Similarly, Grabosky argues that international security was shaped by the dynamism of

[71] Rosenbach, E. & R. Belk U.S. Cybersecurity: The Current Threat and Future Challenges. In N Burns and J Price (Eds) *Securing Cyberspace – A New Domain for National Security*. (Washington, DC: 2012), p 56.
[72]Salifu, A. The impact of internet crime on development, (Journal of Financial Crime, 2008) p 4.
[73] Maughan, D. The need for a national Cybersecurity Research and Development Agenda. (Communications of the ACM, 2010) pp 29-31.

cybercrime and increase its focus due to the parallel approach to which attacks can take place.[74] According to Grabosky, whose assessment this study support, physical attacks in no longer the only approach to undermining or overcoming a nation’s security. Cyber warfare in Estonia in 2007, and Georgia in 2008 provide a clear testimony.[75] In a modern time, connected digital networks offer an almost equivalent approach that is, in certain settings less costly, more discreet and more damaging than the once sole approach to physical attack. Seemingly, the linkage between cybercrime and national security is gradually becoming predominant. As technology improve, so as criminal’s ability to cause harm and frustration to individuals and a nation’s critical infrastructure by undermining its vital instrumentalities. What this has therefore created is a new methodology to the emerging ways in which old problems like defending national security can be addressed, utilizing in some cases, changes in a nation’s law.

Cybercrime stays on the raise and challenges developed nations in dissimilar ways. Existing information about cybercrime activities was compiled from periodic reports by law enforcement organizations, IT and info security companies and consulting firms. In general, the inherent problems in identifying the phenomenon, which equally affected the crude use of statistical methods for a quantitative analysis, and the inclusion of unintended damage in monetary assessments persists, hence, it could be said that the existing information is not reliable. It appears that monetary assessments are unswervingly inflated. Nonetheless, great potential of risk in cybercrime is always emphasized at many forums and by various scholars.

Conversely, the analysis in a study that was conducted by Richardson shows that in effect, a large range of cybercrime does not construe a risk to international security. In specific cases such as on; industrial espionage, harmful contents, fraud, hate speech, damage of websites

[74] Grabosky P., Organized crime and national security. (Canberra, Australia. 2014) p 107.
[75] Richardson, C., Cyber criminals demand a modern approach to security. (The Dominion Post. 2015), p 12. Retrieved on 29 September 2016 from http://www.stuff.co.nz/technology/digitalliving/64625717/.

and denial of service, which has a potential to become an international security problem, and as there is a evident of increase in these incidences and their effects are lasting.[76] Therefore, it is vital to take action on time to lessen the risk and make it more hard for cybercriminals to operate in this environment.

Even more, the phenomenon cybercrime needs to be explained by researchers so that policymakers can understand to address it. For the reasons stated above, a mere monetary loss assessments do not provide a steady genuine basis for accepting the idea in order to formulate policy. Hence, a reconsideration of cybercrime activities is needed to propose proper national policy. In developed countries like Namibia, there is deficient description on the scope of direct and indirect damage caused by cybercrime, it definitely touches how citizens, organizations, and society as a whole function.[77] As Scott posited, citizens and small businesses are silently damaged by cybercrime. He further stressed that incidents such as spam, digital identity theft, internet fraud, interfere in privacy, economic espionage, blackmail, and damage to intellectual property are all widespread and harm some citizens and organizations.

Regular hacking occurrences were reported by the ITU to have rocked the technology and internet world recently. As these hacking become a phenomenon in modern world, with the prolific use of computers and high-tech software, it has a potential to compromise customer's information account.

In the study by Scott, offenders are divided into four groups: the first group comprised employees who are disgruntled with the treatment at work place, some are corrupt and since they

[76] Richardson, C., Cyber criminals demand a modern approach to security. (The Dominion Post. 2015), p 12. Retrieved on 29 September 2016 from http://www.stuff.co.nz/technology/digitalliving/64625717

[77]. Wall, D S. *Cybercrimes: The Transformation of Crime in the Information Age* (Cambridge: Polity, 2007), p 10.

want to part with the employer, they the potential to destroy valuable files.[78] The second group is comprised of idealists who just aim at getting into community spotlight through minimal risk. The third group is a greed-motivated people whose objectives is to attack websites of financial institutions such as banks and insurance companies to obtain money. The forth group included the emerging trend in cyber space well-known as cyber terrorists who possess real threat to cyber security. The composition of these clusters are made of mostly young people who are highly skillful specialists in digital environments. Scott pointed out that cybercrime can be reduced by increasing the seeming risk of apprehension, reduce the expected rewards of cybercrime and find ways to make it more challenging to commit. This could be done by producing National cyberspace strategies which legalize the tasks of law enforcement to investigates alleged cybercrimes.

According to Thorel [79], terrorism in cyberspace can take many different forms such as physical destruction of machineries crucial to IT infrastructure, remote interference of computer networks, disruption of government networks, or even disruption of social networks such as mass media.

As an example; In December 2015, an alleged Russian cyber-attacker seized control of the Prykarpatnergo Control Center (PCC) in the Ivano-Frankivsk region of Western Ukraine. This incident left 230,000 people without power for up to 6 hours.[80]

High profile cases of cyber-attack of that magnitude are increasingly becoming the norm. In another example, in 2015, the US Administration reported the theft of personal files of about

[78] Scott, J. Understanding Contemporary Society: Theories of the Present. (New York. Sage Publications 2014), p 36.

[79]Thorel, R.J. Cyber Threat. Paper presented at the workshop of Shield Africa, (Gabon. Libreville May 2015)

[80] Daniel Wagner. The Growing Threat of Cyber-Attacks on Critical Infrastructure. (The Huffington Post, 2016), p 23.

than 22 million government employees from the computer systems of the Office of Personnel Management, and suspects China of the mess. Similarly, it did not take long for the U.S. to conclude whether North Korea was guilty for the cyber-attack against Sony electronic company in 2015.[81]

Although monetary value seems to be inflated, the growth of cyberspace increases numbers of potential victims by the day and broadens even further methods of committing crimes against citizens and groups. Awareness about this has also picked-up although not relational with the actual increase in cybercrime. In the given scenario, citizens of developed countries will reasonably demand that the state take steps to provide personal, and national cyber security strategies. There is a growing media publicity of data breaches and cyber-attacks which is indication that there is great risks posed by cybercrime.[82]

David Burg, an expert in cybercrime elucidates that cyber criminals evolve their tactics very rapidly, and the repercussions of cybercrime are overwhelming for any single organization to address it alone.[83] This researcher does not support Davis Burg on the going solo idea, rather, cybercrime need to be addressed by mutual effort. It’s therefore imperative that public and private organizations collaborate to fight cybercrime and gain intelligence about security dangers and prepare to react to them. According to him, a united response will prove an indispensable tool in advancing the condition of cyber security.

[81] US Defence Department. North Korea has 6,000-strong cyber-army, says South (The Guardian) Retrieved on 06 February 2017 from; https://www.theguardian.com/world/2015/jan/06/north-korea-6000-strong-cyber-army-south-korea

[82] Yar, M. Cybercrime and Society: Crime and Punishment in the Information Age (London: SAGE Publications, 2006) p 67.

[83] Burg, D. PwC’s Global and U.S. Advisory Cybersecurity Leader, (2014) p 5.

2.5 Global Cyber Security threat

Lee and Brewer defined cyber security as the collection of tools, policies, security concepts, guidelines, security safeguards, risk management approaches, training, actions, assurance. best practices, and technologies that is used to defend the cyber environment, organization and user assets. It also involve with the protection from deliberate attacks such as from disgruntled employees, industrial espionage, and terrorists.[84] According to Yar, cyber security concerned with the inadvertent compromises of the information infrastructure due to user errors, equipment failures, and natural disasters. Cyber peace is the most critical security concerns of modern information age. Cohen and Felson elucidated in the routine access approach that criminals are prowling to prey on the unguarded and use their technical skills to break into networks systems of different users for economic benefit and also to gather intelligence that they will use in future. They do this through social engineering. By definition, social engineering is the method of luring a person or impersonating in order to get the required information.

The US government, this year admitted to be under serious cyber-attacks, almost beyond their control. Given the condition of cybercrime, national security in many states is at risk if aggressions and extremism are taken into cyberspace. Current attempts to mitigates these challenges both nationally and regionally are insufficient, as cyberspace is boundless and limited only by human imagination.[85]

The boundaries of the info society have no direct connection with existing topographical borders, obliviously, cyber threats can arise anywhere, at any time, causing huge destruction in a short space of time, before they are tackled.

[84] Lee, A. L. & T. Brewer, (Eds). Smart Grid Cyber Security Strategy and Requirements. (USA. *National Institute of Standards and Technology report, 2009)*, p 7*6.*

[85] Shinder, D. L. & M. Cross, *Scene of the Cybercrime* (Burlington, MA: Syngress, 2008), p 20.

In the opinion of Shinder and Cross, cybercrime has now surpassed international drug trafficking as a terrorist financing enterprise. The Indonesia Police stressed that criminals are using methods such as Internet Ponzi schemes, identity theft, counterfeiting, and other types of crimes which get away with huge financial profit under the covering of anonymity. According to press reports, Indonesian police officials believed the 2002 terrorist bombings in Bali were partially financed through online credit card fraud.[86]

Yusuf Kileo, expert of digital forensics and cyber security investigation opined that the biggest security threats faced by Africa are to its critical infrastructure and mostly to financial institutions. He further expounded that in Tanzania alone, it is estimated that more than $10 billion lost in 2014, caused by the malware, DoS attacks, and identity and data theft targeted at financial Institutions.[87]

The misuse of social media is another security threat in the world, as witnessed in many African states of Libya, Tunisia, Kenya, Burundi and SA. Social media platforms, according to Blitstein have been used to disseminate destructive information, including propaganda that promotes violence, extremist activities, and the recruitment and training of potential terrorists.[88] The exchange of confidential information over social media has been a serious matter requiring serious measures. As per securitization approach, security operators need to use appropriate policies to mitigate these incidents as they are danger to state security.

[86] Indian Police Report, New Delhi, India (June 2010), p 2.

[87] Yusuf, K. Africa's critical infrastructure vulnerable to attack. (Presentation at IT Web Security Summit, Johannesburg, 2015)

[88] Blitstein, R. Cyber Cops; US Targets Terrorists as Online Thieves Run Amok. (San Jose: Mercury News, 14 November 2007), p 8.

2.6 International responses to cybercrime

Cybercrime present new challenges for policy makers, researchers and law enforcement alike. Its transnational nature demand that it need a factual and comprehensive response through international collaboration involving participation of all concerned parties in the international community. However, vulnerability emerges from enlarged dependence on technology, lack of legal procedures, and limited cooperation both national as well as international levels. That represents real impediment toward effective reaction to these threats. In sum, limited global agreement in terms of responding to cybercrime is the over-all problem.

International response has been overwhelming, the ITU introduced the Global Cyber Security Agenda (GCA), which calls for the embellishment of approaches to develop cybercrime legislations that is internationally applied and compared with conventional national as well as regional legislative measures.[89] Build on these strategies, the ITU has introduced a project called "Harmonization of the ICT Policies in Sub-Sahara Africa" (HIPSSA), which is mandated by ITU to assist Sub-Saharan countries make cybercrime laws, first regionally, then nationally. So far three workshops were conducted in Namibia on the transposition of SADC Model law on Cybercrime into Namibian Law[90]. This model law is being used as reference to the new electronic transaction and cybercrime bill that is being developed in Namibia.

The growth of global crime, in the words of Sterling, is a risk to the rule of law, without which there can be no sustainable world improvement. Transcontinental criminal markets traverse the planet, arms, spreading drugs, trafficked women and children, toxic waste, stolen natural resources or protected animals' parts such as rhino horn. According to Sterling, hundreds of billions of dollars of dirty money crisscross through the world every year, falsifying local

[89] Gercke, M. Understanding *cybercrime: Phenomena, Challenges and Legal Response*: Geneva: ITU Publication. Vol. 6, (2012) p.36

[90] Ministry of ICT. Harmonization of ICT Policy in Southern Africa. (Workshop, Windhoek, Namibia. 2013)

economies, corrupting institutions and stimulating conflict. The intercontinental organized crime basically destroys health, peace and prosperity that is a requirement inhabitants wish to have at each new year. Instead, it brings disease, violence and misery to exposed regions and vulnerable populations. International agreements were ratified to step up the shared reply to these common threats.[91]

In 2003, the United Nations Convention against Transnational Organized Crime was adopted. The next year, 2004, the United Nations High-level panel on Threats, Challenges, and Change, acknowledged organized crime as the "6th constellations of threats with which the world must be concerned in the future".

In February 2010, the UN Security Council acknowledged "with concern the grave threat posed by drug trafficking and transcontinental organized crime to international security in various areas of the world."[92]

Another aspect mystifying progress is that present organized crime is truly global. Unlawful business has globalized rapidly, leaving its legal counterpart. Transnational trafficking started on one continent and transfer on another, often by means of a third. In this setting, virtuously national or even regional methodologies are unlikely to solve the problem.[93] At best, they may dislodge it, as traffickers find new methods, transit routes, or end point for their illegal imports. Law enforcement in particular, like all national actors, is not well prepared to militate in international issues. As stated by the UN, INTERPOL and various regional organizations have done much to enable information distribution and combined operations, but, as a final point, each

[91] Sterling, C., Crime Without Frontiers: The Worldwide Expansion of Organized Crime and the Pax Mafiosa. (New York: 1995), p 57.

[92] UNSC, SC/9867: Security Council Calls for Strengthened International, Regional Cooperation to Counter Transnational Organized Crime, in Presidential Statement. (New York, 24 February 2010) p 2

[93] United Nations. A More Secure World: Our Shared Responsibility; Report of the High-level Panel on Threats, Challenges and Change, (New York, 2004), p 2.

criminal must be put on trial in a national criminal justice system.[94] Tracking down cybercrime is a daunting task because international organized crime client are so changing too much. With regard to global geopolitical events, a multifaceted mesh of interrelating features can cause unexpected shifts in the nature of illicit commerce. These issues are being exacerbated by inequality, migration, and the casual economy all part of the cause of organized crime progresses.

The affect cybercrime activities against the private sector and individuals is already felt in the world economy. According to the EU report, cybercriminals are using ever more sophisticated techniques for interfering into information systems, stealing critical data and holding companies to ransom.

Another threat, as per European Commission, comes in the form of espionage on economic and other activities sponsored by some state in cyberspace. These activities are increasingly posing a new category of threats for EU governments and companies. [95] As said by the report, in Zimbabwe, governments is misusing cyberspace for control and shadowing over its own peoples. This misuse of cyberspace prompt governments in many countries to started developing their own cyber security strategies and to reflect cyberspace as more and more essential international issue. The Global Protocol on Cyber security and Cybercrime call upon governments in partnership with other participants to develop necessary legislation for the scrutiny and trial of cybercrime.[96]

The European Union Agency for Network and Information Security (ENISA) is supporting countries to produce their National Cyber Security Strategy (NCSS) as a key policy

[94] Lampe, K, 'Not a process of enlightenment: The Conceptual History of Organized Crime in Germany and the United States of America'. *Forum on Crime and Society* Vol. 1 No. 2, (December 2001) pp. 99-116.

[95] Helmbrecht, U. European Commission, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (Greece, 2004), p 16.

[96] Schjolberg S and S. Ghernaouti-Hélie, *A Global Protocol on Cybersecurity and Cybercrime*, (Oslo, 2009), p 36.

feature, helping them to challenge the danger brought by cybercrime.[97] However, ENISA indicated some gaps in many countries, particularly in terms of national competencies, organization in cases of incidents that extent across borders, and in terms of involvement of all participants and their preparedness. It encourages more research in this field in order to build a strong security to protect the world economy. This study is taken on the premise of this recommendation.

2.7 Jurisdictional Issues

Conventional crimes in the world are committed close to home as the offender physical presence is required. Conventional crime refers to those traditional, illegal behaviors that most people ponder of as crime, such as corporate crime, white-collar and occupational crimes.[98] For this reason, criminals travel far if there are sufficient incentives. Some crimes such as kidnapping, breaking into a bank are "attractive" enough to do so, but for it to success, the physical presence of an individual is required.

These crimes require much more planning. On the centrally, crimes in the digital world differ considerably on this dimension. Most cybercrimes are conducted remotely, miles away from the target scene. A high proportion of cybercrime investigations are impeded by sovereignty, thus have significant jurisdictional problems. In many cases, cybercrimes crossing borders slow down responses to such crimes considering the sovereignty of states. National boundaries limitation had thus created serious obstacles to law-enforcement agencies. Arrangements for extradition is not yet developed between most states. Some states initiated

[97] European Union Agency for Network and Information Security, *An evaluation Framework for National Cyber Security Strategies, (Brussel, 2014*), p 11.
[98] UN. Conventional crime from an international perspective. Retrieved on 14 April 2017 from; http://sociologyindex.com/conventional_crime.htm

arrangements for working together between law-enforcement organizations in different jurisdictions but this is not sufficient to solve cybercrimes as the structure development differs. In instances where for example, Russia entered into arrangement with the US to help in investigating a number of crimes, cybercrimes are not included[99.]

In another incident in 2010, the FBI arrested two Russian hackers by ensnaring them through inviting them to the United States with job offers. Upon getting the required information, FBI Agents who is handling the event copied data from the two suspects machine which was located in Chelyabinsk, Russia. In 2010, Russia filed hacking charges against the FBI in dispute that it was illegal to download data from computers physically positioned in Russia. While industrialized countries are discussing about worldwide collaboration to combat cybercrimes, many poor states are not yet involved in the discussions. Conspicuously, many countries have not yet passed cybercrime laws. One estimate suggested that in 2010, more than 60% of Interpol member states lacked the appropriate legislation to deal with cybercrimes.

2.8 Policy Implications

Cyber security plays a significant part in the ongoing evolution of information technology, along with internet services. According to Gercke,[100] the safety of the Internet has become fundamental to further development of new service area on top of government policy. Therefore, cybercrime deterrence should be appreciated by all states as an essential part of a national cyber security where critical infrastructure is required as a protection strategy. Particularly, the program embraced the adoption of fitting legislation against the abuse of ICTs by cybercriminals. It also

[99] Schjolberg S and S. Ghernaouti-Hélie, *A Global Protocol on Cybersecurity and Cybercrime*, (Oslo, 2009), p 39.

[100] Gercke, M. Understanding cybercrime: Phenomena, Challenges and Legal Response: (Geneva: *ITU Publication*. Vol. 6, 2012) p.36.

serves other purposes and activities that affects the integrity of national critical infrastructures. Nationally, it is a collective obligation that requires harmonized action connected to deterrence, preparation, reaction and regaining momentum of government authorities, the private sector and citizens after incidents.

Regionally and internationally, it involves collaboration and coordination with pertinent allies. Mutual action is required, as a matter of principle, given globalization which makes the interconnectedness of international network possible. In this connection, the World Summit on the Information Society (WSIS) acknowledged the real and noteworthy perils posed by insufficient cyber security and the proliferating of cybercrime. At WSIS, world leaders and governments nominated ITU to assist with the execution of WSIS Action Line, dedicated to building assurance and safety in the use of ICTs. Accordingly, the ITU Secretary-General initiated the GCA 47 on 17 May 2007, together with partners from governments, industry, regional in addition to international organizations, academic and research institutions.[101]

Gercke described the GCA as a worldwide forum for exchange of ideas to promote international cooperation and harmonize the international reaction on the rising challenges to cyber security, that enhances security and safety in the information society[102].

Laws, Gercke posits, are the back-borne through which society is secured. Cybercrime need stringent laws which not only are relevant but follow technological development. Its formulation needs an expert in cybercrime laws. However, cybercrime can be allayed through conventional laws of the states if new laws are lacking. Most countries that did not yet develop

[101] Gercke, M. Understanding cybercrime: Phenomena, Challenges and Legal Response: (Geneva: *ITU Publication*. Vol. 6, 2012) p.35

[102] Ibid p38

cyber laws use conventional laws for cybercrime trials. Bednarz[103] postulates that offenders hold some important implications for efforts to fighting cybercrimes, as the method they use are not known, simply design it for a specific mission. Global policies to tackle cybercrime threat face a multitude of challenges.

Aside from the resource shortages and other practical difficulties, Finnie et al, [104] postulated that the law enforcement efforts to battle cybercriminals are hampered by a deficiency of essential and dependable information are needed to create offender's profiles. These are critical because they offer helpful lead for ongoing investigation of cybercrimes and, thereby, upsurge the competence of current prosecution efforts. Cyber criminals are well vested in committing crimes since they are aware that only few legal experts on cybercrime who have the ability to detect these activities. Based on this argument, a more effective global response by both the criminal justice system need to work together with other department to address offences of cybercrime nature.

Brenner[105] recommend the formation of a component within law enforcement responsible for arresting and trial of cybercriminals, to serve as a deterrent effect. With regards to law enforcement, the findings of his study recommend that the formation of a deterrent effect through enhanced arresting and prosecution is an essential component of efforts to combat cybercrime. However, it could be tough to get and maintain loyal individuals to serve in this group. Unfortunately, present measures to limit cybercrimes are hardly suited to accomplish this goal. Notwithstanding the yearly snowballing number of cybercrimes, only a rather few notoriety

[103] Bednarz, A. Profiling cybercriminals: A promising but immature science. (2004) Retrieved from http://www.networkworld.com/sup p/ on 12/10/2016

[104] Finnie,T. T. Pete, & J.N. Jarvis, (Eds). The Future Challenges of Cybercrime*:* (*Volume 5 Proceedings of the Futures Working Group.* Quantico, Virginia 2010), p 13.

[105] Brenner, S. Defining cybercrime: A review of state and federal Law. In R. D. Clifford (Ed.), *Cybercrime: The Investigation, Prosecution, and Defense of a Computer-Related Crime*. (Durham, NC: Carolina Academic Press, 2006), p 394

cases are successfully tried at present, whereas many of them do not lead to swift or severe punishments.

A study steered by Shinder[106] revealed that many hackers have a nuanced risk awareness. According to him, the majority of reports indicates that hackers becomes more concerned about risks in modern years, a finding that suggests that increased efforts to fight cybercrimes does not go unnoticed in the hacking community.

Hackers has proven elusive in many previous attempt to arrest them, and need complex system which may be very expensive to have if it is an individual case, but perhaps if it is a large organisation that can include this process as part of it future strategy. Furthermore, many hackers evidently distinguish between the probabilities of becoming detected and apprehended and the consequences of these two events.

The different hacking methods showed that, social engineering attacks are the most successful ones. This method tricks the individual into revealing information about user passwords, whether the systematic guessing of weak or standard passwords or the theft of user logins.

Contextually, Finnie et al stressed that the weakest points of organisations and institutions are their employees[107]. Therefore, they emphasized that institutions have to educate their employees about social hacking methods, and also put control measures in motion to ensure compliance. The education of employers, while definitely an important protective measure, is not the only contribution that will be mandatory from organizations. They are also required to start reporting all incidents against them to the authorities.

[106] Shinder D. L. & M. Cross, *Scene of the Cybercrime* (Burlington, MA: Syngress, 2008), p 10.

[107] Finnie,T. T. Pete, & J.N. Jarvis, (Eds). *The Future Challenges of Cybercrime: Volume 5 Proceedings of the Futures Working Group.* (Quantico, Virginia 2010). Retrieved on 20 February 2017 from;

On the instances in which many organizations abstain from reporting incidents to protect their own interests and thereby harm the interest of all businesses, it needs to be changed because, unless more happenings are reported, computer crimes are not likely to become controllable. It would also pose challenge to law enforcement agents on guidance as to which cases to dedicate their attention to, rather than be reliant on the willingness of institutions or agencies to submit their cases in order to press charges.

2.9. Cyber security in developing countries

The securitization methodology postulates that it is the duty of the states to ensure security of its citizens and their assets. In this regards, numerous less industrial countries had already formulated strategies and started a process of protecting key infrastructures from Cyber-attacks. Kenya has developed the National Cyber Security Strategy, to fight cybercrime in the country with specific focus on four areas: These are; 'enhance the nation's cyber security posture', building 'national capability', information sharing and collaboration' and provide national leadership' through a "single, unified agenda that will guide all relevant national stakeholders".[108]

An incident of cybercrime was reported in Kenya involving a cybercrime hacker syndicate which penetrated the Kenya Revenue Authority and several blue-chip banks, several parastatals and well as a supermarket chain.[109] According to John Kamau, the hacker syndicate use salami attack and electronic transfer. In a salami attack, a crook steals small undetected amount and deposit in one account before launching a major attack. However, police were able to arrest the syndicates. According to the report, the unit responsible for investigating cybercrime

2016 from http://www.c4dlab.ac.ke/2014/07/national-cybersecurity-strategyhopesholes-and-way-forward/

[109] Kamau, J. & S. Cherono. 16 seized as police bust ring of hackers in multi-million shilling KRA, bank thefts. (*Daily Nation*, Nairobi, 9 March 2017), p 1.

estimates that Kenya lost more than Sh17 billion to hackers in 2016 alone.[110] The syndicate also used a backdoor system to steal money. A backdoor is defined by this researcher as a financial software created and install in a computer that allow illegal access to the account and siphon money from unsuspecting victim.

The breakthrough is an indication that Kenya had been able to create capacity to trace and apprehend offenders. For Kenya, these initiatives are a guiding principles to fine tune cyber laws and follow technological development, in addition to identify new areas that need further research.

India is another country that has developed National Cyber Security adopted in 2013. ***Present trends of Cybercrime in India***: Report from the National Cyber Records Bureau, India is trying to implement a local initiative called the Digital India project, which entails to use maximum connectivity with minimum cyber security risks to the best of its capabilities. In sum, India’s cyber security record is poor ut the envisaged project is expected to ease this fear. According to Home Ministry statistics, all together 71,780 cyber frauds were reported in 2013, while 22,060 such cases were reported in 2012, which indicated a tremendous increase.

By June 2014, there was 62,189 incidents of cyber frauds.[111] The ministry further reported that in 2013, 28 481 websites belonging to Indian were hacked by numerous hacker groups from across the globe. Another 23,665 were reported in 2012 and 21,666 in 2011 hacking incidents were reported to the Bureau. Along with the cyber-crime data preserved by National Cyber Records Bureau, a total of 1,688, 3,496 and 4,370 cases were reported under the Information Technology Act in 2011, 2012 and 2013, respectively. Equally, 425, 601 and 1,344 cases were registered under cyber-crime related sections of the Indian Penal Code in 2011, 2012

[110] Ibid, p 2.

[111] Kumar, S. Present scenario of cybercrime in India and its preventions. (*International Journal of Scientific & Engineering Research, Volume 6, Issue 4, April-2015*) p 4

and 2013, respectively. The operational coordinating entity is Computer Emergency Response Team (CERT) which is involved in high level policy discussion related to information security collect all cybersecurity incidents, conduct researches and profiling attackers. According to the Ministry of ICT, private sector representative in India are well developed and are pro-active on cybersecurity.[112] However, there are no dedicated private, public partnership and therefore no joint cybersecurity plan in India. To address that gap the authority in India took an initiative to set up a cybersecurity experts study group operating under the Ministry of Home Affairs for reviewing domestic cybersecurity and develop new policies.

In South Africa, there are 6.8 million Internet users and 341 organized crime groups and cybercrime is fast becoming a severe and costly threat. According to Novell, it is estimated that R25 billions of government's annual procurement budget is lost to corruption and other factors.[113] South Africa undertook several cyber security initiatives although the cybersecurity policy is not yet finalized. According to the minister of Justice and Constitutional Affairs, Jeff Radebe, in 2012, 113 cases of cybercrime were finalized, with 83.1% conviction rate.[114] Grobler et al observed that various societies in the country are engaging in cyber security awareness exercise each with its particular purposes and focus areas.[115] The institute of education and research has responsibilities of training in the country to current and future users of the computers on safety and secure online habits and this increased the awareness and indulgent of the dangers of the Internet. This program also provides individuals users with the required knowledge to make the right choices in Internet-related circumstances. The reasons for the

[112]Notification National Cybersecurity Policy (India Ministry of Information and Communication Technology, 2013) p 6.

[113] Novell Connie Grobler. Cybercrime now a serious and costly threat in South Africa. Retrieved on 15 March 2017 from http://www.itweb.co.za/index.php?option=com_content&view=article&id=59355

[114] Phahlamohlaka, J. Which Cyber incident could qualify as cyber warfare? A national security argumentative Analysis. A presentation at SADC Cyber Conference. (Pretoria. 4 November 2015)

[115] Grobler, M., S. Flowerday, R von Solms, and H. Venter. "Cyber Awareness Initiatives in South Africa: A National Perspective". (Pretoria, 2011), p 38.

putting into practice of cyber security concepts and awareness programs in convincing the audience of the significance of cybercrime awareness programs that needs be implemented. It seems a perfect approach, however, cybercrime is a technical field and need more concentration on response mechanisms, because is one thing to identify a crime, and the other thing to prove it.

In Uganda, a substantial number of this non-violent crimes have hit the business community hard as the banks are more affected. According to Bernard Busuulwa, Stanbic between January 2016 and January 2017, Uganda documented 80 fraud incidents. The bulk of these incidents were initiated by external sources. Furthermore, 650 fraud incidents were thwarted during that period. According to the internal security data compiled by bank staff, around 95% of the stated fraud incidents were ascribed to the use of counterfeit currencies. An estimated Ush 600 million ($164 347) was recovered from fraud incidents in the bank about that time. Busuulwa further epitomized that banks tried to stop fraud attempt but it kept on mounting up. Uganda Banks Association is setting up an anti-cybercrime committee to guide the industry on ways to tackle problems. It shows that, in Uganda, the government has no capacity yet, hence the bank association initiative. The absence of the law is being exploited by corrupt elements who appears to be assisted by bank staffs.

2.10 Development of Cyber laws

The upsurge of cybercrime in the world arena prompted the need its regulation. However, cyberspace laws vary from jurisdiction to jurisdiction. Apart from international regulations, each country can come up with laws to control specific local activities based on its interest. For example, in Kenya, a hate speech using media has a penalty of 20 million shillings or 20 years in prison. Kenya can also use this tool to regulate the communication from Kenya to Somalia if that communication is to give information to terrorist is a punishable crime.[116] Cybercrime is dynamic and therefore the law should also be flexible enough to suit the condition.

[116] Kyalo, Victor. ICT and National Security. (Lecture given at the National Defence College, Kenya, on 02 August 2017).

Below are the top fifteen (15) countries that consider that their homegrown law enforcement agencies are not sufficiently resourced and trained to combat economic crime, according to the Global Economic Crime Survey 2016, conducted by researchers Campbell et al sponsored by PricewaterhouseCoopers (PWC), a South African firm.[117]

Table 2: Top 15 countries with weak cybercrime laws

S/N	Country	Percentage (%)
01	Kenya	79%
02	South Africa	70%
03	Turkey	60%
04	Philippines	58%
05	Bulgaria	58%
06	Poland	58%
07	Ukraine	57%
08	Mexico	56%
09	Zambia	55%
10	Nigeria	54%
11	Australia	52%
12	United States	52%
13	France	51%
14	Venezuela	50%
15	India	49%

***Source**: Global Economic Crime Survey 2016 – 5th South African Edition*

[117] Campbell, M., Amra, J., Sharia, J., Fakey, M., Develin, R. & Opperman, L. Economic Crime: A South African pandemic. (PWC, Cape Town, 2016).

A commonly held and oft-repeated view that has reached allegory status is that these adverse feelings only arise in developing less industrial states. As it stands, developed countries such as US, China, Russia and Germany among others invested heavily in both communication infrastructure, skills, legal framework and structures, compare to developing states especially in Africa, even though they are still vulnerable to cyber-attacks. It is assumed (perhaps because of It is further presumed that every citizen shares this view. On the contrary, though, our global survey uncovered a prevalent deficiency of self-confidence in local law enforcement agencies, a phenomenon that is not limited to regions or level of financial development.

It is, of course, likely that this metric could arose to numerous differing factors, comprising countrywide rates of economic crime, the degree to which law enforcement agencies in the respective countries publicize or even downplay their expertise in certain areas like cybercrime, and at some point, law enforcement interventions are perceived to be above political.[118]

Scott emphasized that "having the NCSS in place may not fight cybercrime. There is need to implement these strategies so as to engage cybercrimes"[119]. Nye reaffirms this claim arguing that the police need to have more skills apart from money so as to engage cybercrime. However, this can only be realized once there is continued sharing of strategies that are being used by different countries to fight cybercrime.

[118] Louis, Strydom. Economic Crime: A South African pandemic. No sector or region is immune. (Global Economic Crime Survey 2016, 5th South African Edition), p 4.

[119] Scott, J. Understanding Contemporary Society: Theories of the Present. (New York. Sage Publications, 2013), p 20.

2.11 Conclusion

This chapters defined cybercrime and discussed its dimension in the international system. It looked at the impact on the international communication network with specific emphasis on available capabilities to mitigate it. The global community comprehends and appreciate well the scopes of technology and the features of the related threats and prospects in the field of cybercrime. The initiatives taken by many actors are meant for awareness as it was observed through various reported cybercrime incidences that users of networks are the weakest links if not well prepared, but strongest link if well informed. Cybercriminals are among the communities and their need and aspirations may not be different with a bigger margin with those of the communities in which they leave. States need to pursue and implements its initiative to reinforce cybersecurity which is a major security concern. It is also indispensable to grab the occasions brought forward by globalization to encourage economic growth and promote fairness. In this way, they can not only foster long-standing values but also address some of the critical sources of these international threats. It is also important to create the international collective decision-making processes.

CHAPTER THREE

OVERVIEW OF CYBERCRIME IN NAMIBIA

3.0 Introduction

This chapter gives the synopsis of the penetration of IT in Namibia's' society and discusses cybercrime incidents that continue to affect businesses negatively. It looked into statistics of cybercrime incidents from NAMPOL and collate views from technical and also law enforcement practitioners on cybercrime matters. It also appraised the current capabilities the country has with the purpose of providing easy judgement about gaps brought about by defective laws, manpower, systems and intra and inter coordination between agencies of government and private sectors.

The Republic of Namibia has a population of 2,198,406 (2011 census)[120]. According to TELECOM Namibia, Internet users as of December 2013 stood at 305,578, or 13.9% of the population. As of December 2012 the country had 231,340 Facebook users, or 10.7% penetration. In Q4 of 2012 the total figure of individuals who subscribe to mobile phones in Namibia was approximately 2,760,000 and in Q4 of 2013 the total was approximately 3,025,000, an increase of 9.61%. The West Africa Cable System (WACS) fiber-optic submarine cable landed in Namibia in 2011, which boast the development of Namibia's Internet and broadband sector.

According to TELECOM Namibia, internet penetration is low at approx. 9% (August 2012), although 4th generation (4G) mobile services resulted in a 111% mobile phone penetration

[120] Government of the Republic of Namibia. Results of National Statistics 2011. Statistics Office. Windhoek, Namibia, p 20

rate.[121] Namibia is interconnected to the international internet network through which it conduct business with the rest of the world, and therefore is a target of cybercrime.

The integration of Namibia into global structures is not new, it began with colonialism before the turn of 20st century. After independence, the country continues to engage into various voluntary arrangements, which led to equally benefit and detriment implications.[122] Positive in terms of technological advancement, cooperation with other states, free trade, and interconnectedness to the world among others. Nonetheless, globalization also led to negative implications such as menace of cybercrime.

Criminals in cyberspace are rising a threat as they control a pervasive, well advanced on-line service economy in illicit cyber capabilities and services, which are obtainable to everyone willing to pay. Notwithstanding the worldwide nature of Internet, the state is forced to rise its participation significantly so as to monitor its operation.[123] The framework of state participation in cyberspace has been evolving during the past ten (10) years, the most observed complex issues being the opposing values of privacy as well as national security.

In a democracy, the procedure for developing a public policy on cybercrime includes public debate, political debates, and a pro-longed term legal treatment. Second, the deficiency of technical and operational skills is lowering the chances for entering the cyber warfare ground, mounting the anticipated threats beyond states and large terrorist organizations, and retaining a very heavy liability to national security authorities.

Cyber-criminal societies access the resources, infrastructures, and even client service at lower cost. They can abuse users unknowingly to engage in crime for financial yield and also to

[121] TELECOM Namibia, press Release, Windhoek, Namibia. May 2014
[122] United Nations, author. Namibia: Situation Analysis (United Nations in Namibia and Government of Namibia), 2011, p 2.
[123] David S. W. Cybercrimes: The Transformation of Crime in the Information Age (Cambridge: Polity, 2007), p 10.

perform direct attacks on national security.[124] To achieve cyber security, critical infrastructures requires protection against cyberspace threats. The threat could be even greater given the frequency of potential elements of risk capable of acquiring cyberspace weapons and recruiting "fighters" on the cybercriminal black market.

3.1 Cybercrime and Namibia's National Security

Much was said regularly in international and local print and electronic media in Namibia about cases of cybercrime involving illegal transactions, scams, forgeries and accessing of classified information. Reports from NAMPOL are that an average of twenty cases of cybercrime is reported by individuals in Windhoek alone per week[125]. Typical examples are cases of card fraud, where most withdrawal/transactions report on cell phones, and these alert complainants. Due to limited withdrawal amount per day, individuals mostly suffered loss ranging between N$ 1 000.00 to N$ 6 000.00 before they report the matter to their banking institutions for their account to be blocked. NAMPOL further indicated that a big number of complainants/victims of card fraud alleged that, they last used their ATM credit cards at shops, bought groceries or paid their accommodations at the hotels for tourists.[126] In Namibia, consumer use services such as e-banking, money transfer and credit facilities for shopping are appreciated, but internet users are becoming more concerned on the safety and reliability of their information because of increased hacking of online devices.

[124] Hathaway, E. M. "Falling Prey to Cybercrime: Implications for Business and the Economy," ch. 6, in Securing Cyberspace: A New Domain for National Security (Queenstown: Aspen Institute, February 2012), p 29.

[125] Muraranganda, E. (27 February 2015). Cyber Criminals on Borrowed Time. (Windhoek. Namibian Sun) p2.

[126] Namibian Police Crime Report, Windhoek, November, 2015.

According to NAMPOL, there are several reported cases by celebrities and politicians about fake accounts being opened in their names on Facebook, Twitter, LinkedIn, YouTube and Instagram where unsavory content is posted[127].

A study by Mvula, the Chief Executive Officer of National Commission for Research, Science and Technology, indicated that Namibia has shortage of proper legal framework to shield internet users.[128] Accordingly, the approach to address cybercrime should be mutual, with a full force by all stakeholders directed by the government as a national security threat, in conformity with the securitization approach. Although this approach need somehow further analysis because in multi sector cooperation, people are attracted by incentives which in this case may be abstract, forcing some sector to pay less attention. However, as pointed out earlier, Namibia’s Cybercrime laws are up till now to be completed to give law enforcement operatives power to prosecute offenders. Without clear strategies to protect people from cybercrime, all the improvements made through the enlargement of infrastructure to drive ICT may lose its value.[129] This could be the main motives why every country needs to have clear strategies to mitigate cybercrime. In Rushi’s words, the states is obliged to make effort that guarantee that the cyber world is safer for the interest to all stakeholders.[130] This could be done by putting up deterrent measures against cyber criminals by providing national cybersecurity plans for protecting critical infrastructure of the nation. While several states such as India, South Africa and Kenya amongst a few, produced their National Cyber Security Strategy, Namibia and Uganda are still reeling around conventional laws which is still used to charge cyber criminals. Despite policy measures,

[127] Namibian Police Crime Report, Windhoek, Namibia. December 2015

[128] Mvula, E. Establishing and Strengthening the National System of Innovation. Paper presented at a workshop in Windhoek, June 2015, p 3.

[129] Guanci, R. J. Unrestricted Warfare: The Rise of a Chinese Cyber-Power. (Seton Hall University, 2014), P 488

[130] Rishi. R. Strategic National Measures to Combat Cybercrime: (Perspective and learnings for India, 2015), p 45

cybercrime has continually been on the rise as new methods are facilitated by the rapid advancement of technology vis-à-vis laws, causing laws to be 5 to 10 years behind the worldwide crime curve relative to technological capabilities.[131]

Cyber criminals also seemed to be motivated by the shortage of enough well trained IT and legal experts, and monitoring infrastructure in Namibia and other less industrialized countries..[132]

3.2 Cybercrime statistics in Namibia

Between 2010 and 2015, NAMPOL crime statistics show various cases of money laundering, card cloning, card fraud, phishing, data diddling, salami, hacking, email bombing, DDoS, virus/worms, Trojan, web jacking and obtaining private information from individuals' computers, for which the existing instruments were used to prosecute offenders. In 2015, card fraud alone cost the economy more than R480 million between January and September.[133]

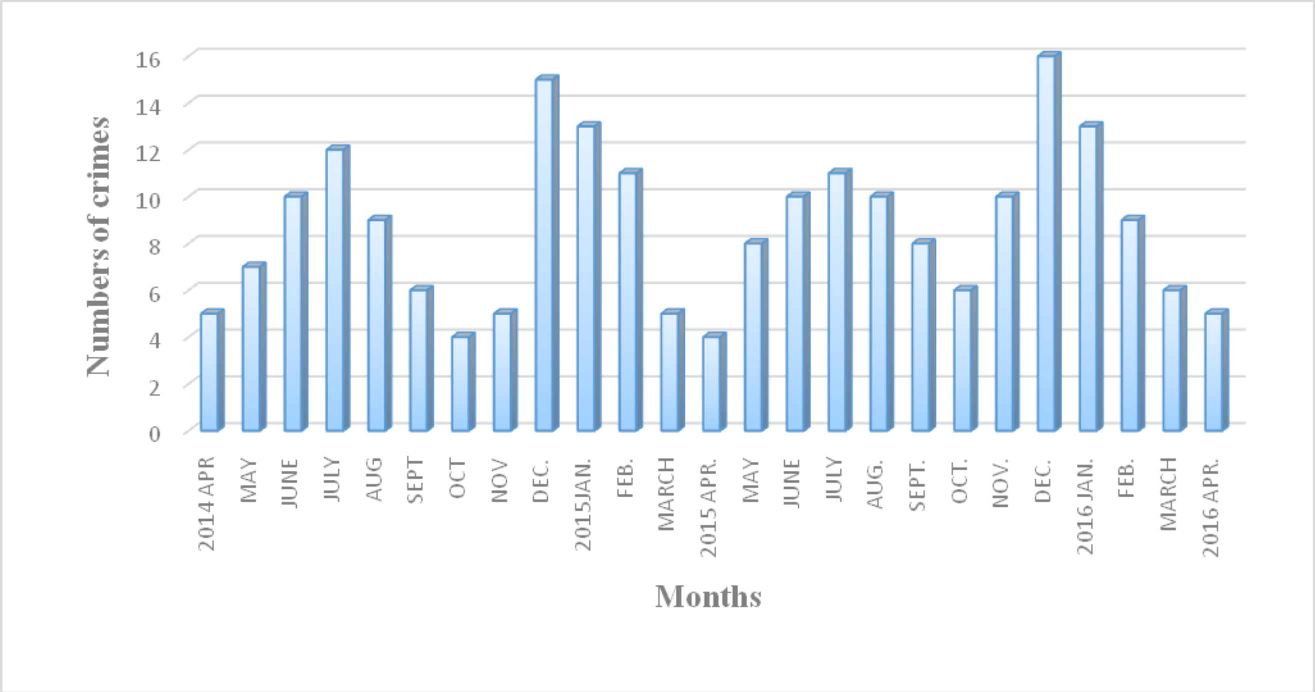
Card fraud is continuing concern for the bank and electronic payment firms such as Visa. Whereas Namibia seems not to be a cybercriminal's primary target country for card fraudsters, commercial banks are spotting fraud incidents that could not be identified through consumer education. Predominantly, banks and customers are in danger of card cloning being instigated by external sources. These take in a various of happenings such as skimming of card along with personal identification number (PIN) interception. Card cloning start with the criminal holding a customer's card for a few seconds during which time the criminal copied the information on the magnetic strip of the card onto a handheld scanning device. The swindler then observes the

[131] Goodman, M. *Interpol's Role in Fighting High Tech Crime*. (Geneva, 2006), p13
[132] Ibid, Goodman, p15
[133] Katjiukua, I. FNB and Visa join hands to fight card cloning fraud. (New Era. Windhoek. 16 April 2015), p7

customer pinning the PIN onto the keypad of an ATM or a retailer’s card machine. With this information, the impostor is capable of creating a forged card and then uses it with the PIN to complete transactions or withdraw money at an ATM from the victim’s account. Cases of this nature are increasing in Namibia.

Below is the statistics of ATM fraud reported to NAMPOL over the period of two years (2014 - 2016).[134]ATM fraud is top of serious crimes experienced in Namibia during the past years. This statistic includes all fraud cases reported in the country and includes; ATM Frauds, depositing money into bogus bank accounts to buy cars after cars advertised in the social media, e-wallet to buy/deposits items in South Africa and locally to unknown, used fake government orders to buy properties, buying goods with fake money).

Fig 2**: ATM Fraud April 2014-April 2016 (‘000)**



Source: NAMPOL

[134] Namibian Police Crime Report statistics, Windhoek, Namibia. May 2016

The graph above shows the volume of incidents for card fraud reported in Namibia over the period 2014 – 2016. The picture showed some specific times of the year where crime upsurge and the other time it declines. The reason behind this indication is that fraudsters target foreigners who come to spend their holidays in Namibia from other parts of the region and abroad. Namibia used to receive tourists mostly from Germany because of historical linkage. Some Germans have properties in the countries. As can be seen, the months of June and July crimes increases. At this time of the year, Europeans come for holiday to enjoy a hot sunny. Fraudsters are attracted by the foreign currency they carry such as US Dollars and Euro. As some of them does not now the country well, as these services are available country-wide, they access service everywhere thereby being preyed by criminals.

These type of incidents are also higher during December and January months. During this time in Namibia, consumers spend too much because it is holiday and festive season. People are conducting weddings, Christmas and New Year parties, and also a start of cultivating season. During this time, criminals are busy to use any opportunity available. As per rational activity approach, crime takes place when there is no control. During this time, most law enforcement operators are on leave, hence the intensification in crimes.

The Bank of Namibia reported a new defrauding scheme that tries to defraud organisations and individuals by dishonestly attaining a spare SIM card through acquiring security data such as One-Time Pins (OTPs) banks used to send to customers when performing specific services. Consideration is taken when such information is received, card holders and business enterprises are alerts to be vigilant and not be duped into this prevailing scam. Obliviously, the modus operandi are that fraudster typically approaches a mobile operator, impersonating a customer or pretending to act on a customer's behalf, with a falsely acquired copy of customer's identity document and requests for a SIM card replacement. The challenge is that even if members are alerted, some will still sufferer the scam. Thorel posit that "an uneducated population the weakest link, while an educated one is a strongest link).[135] The securitization approach also stated that security is paramount and is the obligation of every citizen.

NAMPOL data illustrates that at least an average of ten (100) cases of which 70% are card fraud are reported per week in the country. According to NAMPOL, a big number of complainants/victims alleged that, they last used their ATM credit cards at shops bought groceries or paid their accommodations at the hotels when it is tourists. The suspicious is that, criminals are operating together with some shop and hotel cashiers/employees by supplying them with cloning devices machines so as to clone the customers' credits cards whom they think are having much money on their accounts. Some criminals are insert their cloning device machines at the ATM machines during pay days to clone the victims' ATM credit cards. Banks which are mostly targeted are FNB, Standard Bank and Ned bank's ATMs at the suburbs where no cameras are in place, and are sometimes overcrowded. However, due to limited withdrawal amount per day arranged by complainants/victims and that most withdrawals/transections report on cell phones, victims mostly suffered loss ranging between ±N$ 3 000-00 to N$ 6 000.00 before they (victims) became aware and contact the banks and report the matter for the account to be stopped.[136]

However, fewer incidents were reported whereby complainants/victims asked for assistance by people they found at ATMs, which indicates that customers are showing some

[135] Thorel, R.J. Cyber Threat. Paper presented at the workshop of Shield Africa, (Gabon. Libreville May 2015)

[136] Interview with Sandema, Rector. Head of NAMPOL anti-money Laundering Unit (interviewed on 21 July 2015 in Windhoek, Namibia)

awareness behavior. These criminals are given PIN numbers by the victims and after withdrawing they give wrong ATM cards to the victims and immediately travel to the neighbor town or point to withdraw the money. Only in few cases, according to NAMPOL, suspects were arrested and prosecuted, because the nature of cases is mostly complicated as it includes technology, which become a challenge in Namibia.

However, with the increasingly sophistications of cybercrime, the interpretation of the Namibian laws on these is still vague and can be challenged in the court, therefore, many cases are withdrawn because on technicalities.

Criminals, however, are manipulating that technology for their dubious use. As Kamutuezu expounded, existing law cannot charge someone who intentionally interfere with data which causes such data to be altered or else rendered ineffective.[137]

According to NAMPOL, crime of computer misuse is a challenge for law makers because the dimension of crimes has changed requiring a challenge for investigation and trial of such crimes, this provision is not provided for in the law, or its interpretation is untested.[138] That is why the new trend for the authority to legislate new laws for cybercrime to limit or exclude uncertainties when a crime is identified, but new laws alone are no guarantee, it experts experts to interpret it.

3.3 Cycle of combating cybercrime in Namibia

Article 13 of the Constitution of the Republic of Namibia made provided for the right to privacy including communication, for all citizens, therefore, these rights have to be sheltered by the

[137] Interview with Ms Elizabeth Kamutuezu, Acting Director, Policy and Regulations: Ministry of ICT. (Interview conducted on 21 December 2016 in his office, Windhoek, Namibia)

[138] Detective Chief Inspector Rector Sandema; Head of NAMPOL Anti-Money Laundering Unit (interviewed 21 July 2013)

state.[139] On that note, this research was undertaken with this consideration in mind. Privacy of using communication networks is significant for constitutional rights, individual liberties, and economic efficiency. According to Kamutuezu,[140] threats to online privacy are: gathering marketing information, investigating crime, espionage or terrorism, misusing legal investigative authorities, stealing government or business secrets or financial information and gaining private information from individuals' computers.

In order to appraise the extent of cybercrime in Namibia, the researcher, developed a radial cycle model which is useful to appreciate the level of development in Namibia with regard to combating of cybercrime.

This process model is a project performed by different roles participating in different institutions and agencies. Like all projects, there are defined roles for each institution. In fact, this is grounded on the four questionnaires this researcher put to experts and responsible officials on the subject matter.

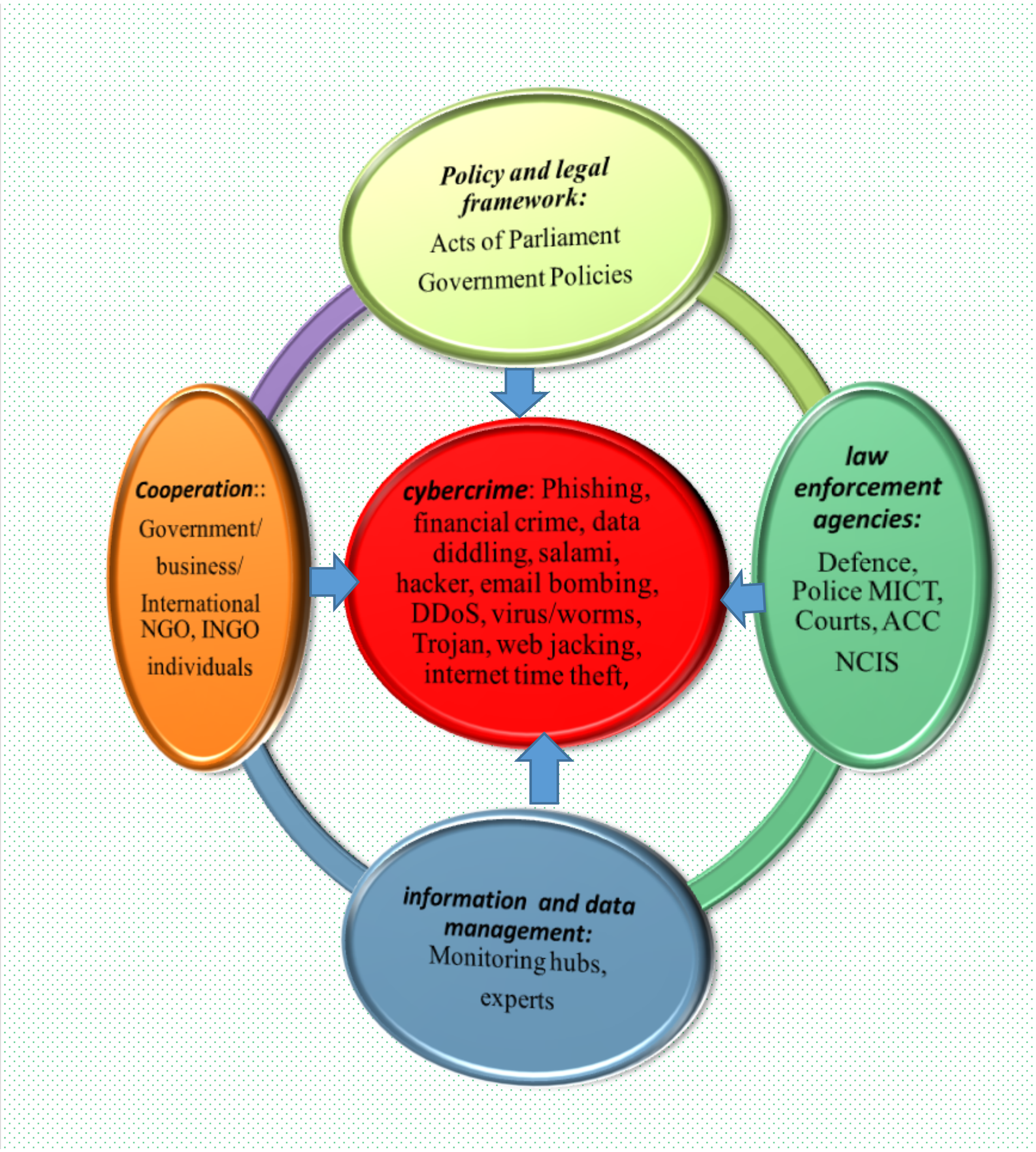
Firstly, it examines current Namibia's cybercrime related laws to ascertain their effectiveness to mitigate cyber violations as stated in local media, and its bearing on the rapid dependence of internet;

Secondly, it examined the efficacy of local capacity on law enforcement operatives to manage cybercrime;

Thirdly, it assesses the capacity building efforts towards the battling of cybercrime, and; finally, It assessed the input of inter-agency cooperation within Namibia security sector and abroad on cybercrime related incidents.

[139] National Assembly. Constitution of the Republic of Namibia, 1990
[140] Op Cit, Kamutuezu.

Figure 3: **Process model of fighting cybercrime in Namibia**


Policy and legal framework:
Acts of Parliament
Government Policies
Cooperation::
Government/
business/
International
NGO, INGO
individuals
cybercrime: Phishing, financial crime, data diddling, salami, hacker, email bombing, DDoS, virus/worms, Trojan, web jacking, internet time theft,
law enforcement agencies:
Defence,
Police MICT,
Courts, ACC
NCIS
information and data management:
Monitoring hubs,
experts

(Source: Author)

This model is comprised of four approaches, which are; legal framework, law enforcement agencies, management of information and interagency cooperation, connected together to successfully mitigate cybercrime. This model is seen by the researcher as imperative to comprehend appreciate the input of various sectors to battle cybercrime together, whereas if one of them is detached, then the fight will never be effective. Namibia requires such model as a means to mitigate not only cybercrime, but other organised crimes as well. As Buzan says: "The 'national' security problem becomes a universal security problem in which individuals, states and the system all take part, and in which economic, societal and environmental factors are as significant as political and military ones"[141]

The state is the authority responsible for the defence of citizens and its properties in a country and ensures that individual, society and state are taking part. It ensures safe operating environment for business to flourish by making laws and procedures which regulates those actions. The laws are to be relevant with the time and has the capacity to trial cases of any magnitude. At present, old laws are the reasons that some cases that are being discharged in the court in Namibia on technicalities. The Ministry of ICT is the leading department to craft cybercrime laws. Since 2012, Namibia is struggling to formulate cybercrime laws, but shortage of expertise and the quick improvement of technology means, it will take a while.

Available legal instruments are always enforced by relevant branches of the state that are responsible. In Namibia, the Office of Prime Minister (OPM), Ministry of Defence (NDF), NAMPOL, the courts, Anti-Corruption Commission (NCC), Bank of Namibia (BON), Ministry of ICT, Namibia Central Intelligence Service (NCIS) are among the law implementers responsible for cybercrime laws. The task of law execution need some coordination. In Namibia, this set-up is at its infancy, therefore, statistics shows high crime.

[141] Marianne Stone. Security According to Buzan: A Comprehensive Security Analysis. (Security Discussion Papers Series. NY. Columbia University. 2009), p 10

In order for the law implementer to accomplish its tasks, it need equipment and organisation structure, for instance monitoring hubs and specialists to man them. The infrastructure to monitor are not adequate, those available are poorly equipped. The other area that needs attention is the experts who are well vested in new technology and able to trace cases beyond the border.

3.4 Types of Cybercrime

To mitigate cybercrime, it requires intra and inter cooperation, to share relevant information and take joint action. This calls in the centre where all stakeholders converge and receive directions, take mutual action. As cybercrime occur through network, private business also forms part of the team. This process requires a national centre to receive reports from everyone including individuals who detect any suspicious. Some crimes that were detected in Namibia are as indicated in table 3:

Table 3. Types of Cybercrime

Identity theft	When a person disguises to be some other person, with an aim to making a scam for financial advantages.
DDoS attacks	Are used to make an online virtual service inaccessible and put it down, by barraging or overpowering it with stream of traffic from various sites and sources.
Botnets	Networks of compromised processors, orderly controlled by attackers remotely to send spam to other computers.
Phishing	Methods where cyber criminals lure user to give out the info they want. Users can be seduced through business proposal, or a promise of money which you never subscribed.
Spam	basically unwelcome emails and messages

Social engineering	A technique in which cyber criminals establishes a contact directly with you through of emails or phones. They first build confidence and when they succeed, it will be easier to obtain the data they need.
Card fraud	when a swindler acquires user's private identification Number (PIN) or the data on user's ATM card to obtain access to the funds in your account
Salami attack	In a salami attack, a crook steals small undetected amount and deposit in one account before carrying out a major attack.
Backdoor	A financial software created and install in a computer that allow illegal entree to the user's account and siphon money from unsuspecting victim.
Hacking	The act of breaching into a computer system, for a socially or politically driven resolve. The individual who executes an action of hacktivism is called a *hacktivist*.

Source: Author

It is therefore important that the four arms are important as clearly alluded to in the securitization procedure by Buzan *et al*.

3.4.1 Policy and legal framework

According the Director of Communication in the Ministry of ICT, Internet laws that cover cybercrime in Namibia are in its primary stages. There are at this time no suitable laws that clearly cover cybercrime. In 2014, the ITU in conjunction with the government started working on a cybersecurity law that is still being developed. He further indicated that the Namibia University of Science and Technology is working with the ITU to implement child online protection laws but they are still in development.[142]

[142] Telephone Interview with Mr Klaasen, Director of Communication, Ministry of ICT, September 2016.

NAMPOL indicated lack of up to date Laboratory equipment to conduct investigations on different devices that were used in cybercrime. This, according to NAMPOL, delays the finalization of the investigation on time, pilling up outstanding's of laboratory reports. Another concern noted by NAMPOL is the deficiency of experience among the investigators and prosecutors caused by the emergence of this types of crimes which is very unique and complicated.[143]

HIPSSA which is an ITU major project is embarking on transposition of the Cyber security Model Laws of SADC into National Laws of member states, specifically on data protection, electronic transaction and cybercrime[144]. Moreover, this exercise is being carried conducted in all sub-regions of Africa, which gives hope that once it is completed, it will make a change in fighting international cybercrime.

The present laws are not effective and the legal and policy frameworks that should talk to cybersecurity are not there yet.

Meanwhile, on the word of the Director of Policy in the Ministry of Justice, the following laws are presently used:

- The Financial Intelligence Act, (No. 13 of 2012), made provision for the fighting of money laundering, and in doing that, it establishes an Anti-Money Laundering Advisory Council; to provide the Bank of Namibia with the necessary powers to collect, assess and analyse financial intelligence data, which may lead or relate to money laundering;

[143] Namibian Police Crime Report, Windhoek, Namibia, April 2016
[144] Gercke, ITU expert, interviewed 21 December 2016 in Windhoek, Namibia.

- The Prevention of Organized Crime Act, (No 29 of 2004), which provide for measures to fight organized crime, money laundering and criminal band activities;
- Payment System Management Act, (No 3 of 2010), which give the police force the power to confiscate stolen items from criminals;
- Communication Act, (No 8 of 2009), which regulate telecommunications systems and networks**;**
- Anti-Corruption Act, (No 8 of 2003), which established the Anti-Corruption Commission and its functions; to prevent and punish of corruption.
- The Information Technology Policy for the Republic of Namibia, (Ministry of ICT, 2009) which stipulated the expansion ICT to contribute towards the attainment of vision 2030.[145]

These and other laws are the tools used to apprehend cyber criminals currently in Namibia, and contribute immensely to the combat of cybercrime. Moreover, cybercrimes are progressively become sophisticated and new forms and methods of such crimes are developing at an increasing rate.[146]

3.4.2 Law Enforcement Agencies

As the say goes 'it is one thing to make a law, and another to implement it'. Law Enforcement Agencies contribute immensely to the fighting of cybercrime by ensuring that laws are adhered to. However, the regularity of occurrence of cybercrime activities being reported indicated that the resident Law Enforcement Organizations like NAMPOL, NDF, NCIS, the Courts, BON and Receiver of Revenue seems to struggling containing these crimes. Law Enforcement Agencies,

[145] National Library, Windhoek, Namibia, December 2016.

[146] Riptech. *Riptech Internet Security Threat Report*. (Riptech University: USA; Arizona) obtained on 4 July 2016 from http://www.4law.co.il/276.pdf

as indicated by the NAMPOL, lack laboratories at regions and that makes things more difficult because every item is forwarded to WHK which is overcrowded with items awaiting examinations from all regions. NAMPOL further stressed that, there are shortage of Investigators and Prosecutions on cybersecurity owing to lack of fund, thus makes the courts less effective in dealing with cybersecurity.[147]

According to Riptech report, police forces in some states are highly localized and not well prepared to participate in this international nature of cybercrimes, and they are also experiencing manpower shortage to handle cybercrimes. As such, NAMPOL point out that NAMPOL has been unable to recruit and retain the best available IT talent, adding to what the former Governor of the BoN, Tom Alueendo stated that Namibia has a very small Police IT Unit[148]. Therefore, the gravest challenge facing Namibia is the deficiency of resources and the limited capacity available to train specialists to investigate cybercrime.

As said by the Chief of Staff ICT in the Ministry of Defence, the NDF has just established the IT technical section, and its capability is not yet tested.[149] As for the NCIS, shortage of resources and knowledge gap are among reasons impeding them to acquire capacity to monitor cybercrime, despite the provision in the Communication Act, No 8 of 2009.

As Gercke put it, "weakness of defense mechanisms co-varies positively with the probability of attack".[150] As such, Namibia's under-develop system exposed the country to more attacks. While some weaknesses are technological, others are behavioral/perceptual in nature,

[147] Namibian Police Crime Report, Windhoek, Namibia, August, 2016

[148]Alweendo, T. *Report on Financial Crime in Namibia; Evidence, Economic Effects and Countering Mechanisisms*. Windhoek: Safari Hotel. (20 June 2007), p 6.

[149] Interviewed with Haihambo Jimmy, Chief of Staff ICT, Namibia Defence Force, (Windhoek, Namibia, 20 December 2016),

[150]Gercke, M. *Understanding cybercrime: Phenomena, Challenges and Legal Response. (*Geneva: ITU Publication., 2012) p 57.

hence, failure to catch up with technologies will cost the economy dearly. It calls upon the executive to realize this deficiency and reply positively to this demand.

The computer literacy level in the police force is very low and agreeing to the crime squad report they are planning to establish partnership with other participants such as BON and the Prosecutor-General's office to facilitate basic computer training programs for the investigators, while encouraging members to use computer training facilities in their space to upgrade themselves. This training is basically for operators and cannot produce experts. Paradoxically, it experience lack of training material.

3.4.3 Information and data management

Acting Director; Policy and Regulations in the Ministry of ICT indicated that Namibia does have the required infrastructure and resources[151]. There two (2) Universities that are currently doing wide-ranging study of cybersecurity. Namibia University of Science and Technology (NUST) at this time has a research cluster of about 20 people that are exclusively researching in Cybersecurity and are producing at most 10 honor and Masters students a year that have studied Cybersecurity.[152] On the centrally, Bank of Namibia deputy Director stressed that, there exist a gap of coordination in the utilization of available resources by stakeholders. These stakeholders have not developed their institution and prepare it on cybersecurity. Therefore student who completes their university programs cannot be hired on cybersecurity related jobs within the market.

[151] Interview with Ms Elizabeth Kamutuezu, Acting Director, Policy and Regulations: Ministry of ICT. Interview conducted on 21 December 2016 in his office, Windhoek, Namibia.
[152] Interview with David Ndatipo, Intelligence Officer, Namibia Defence Force. 26 December, 2016, Windhoek.

According to NAMPOL, the force is under staffed, and no resource is available to send people for training. In addition, many trained personal are leaving for private sectors seeking better salaries. Lack of fund affected the procurement of new equipment to monitor cybercrime activities, especially those can retrieve messages and images from computers and cell phone.

Consequently, effective risk controlling and preventive system demand implementation of a well-proven security standard.[153] As mentioned above, cybercrime research are highly complex, so as resource and expertise intensive, and this can impede the developing countries could not to probe all reported cybercrime.

Moreover, section 70 of Communication Act, (No 8 of 2009), made provision for the establishing of interception centers to monitor networks for national security.[154] These centers are to be staffed by members of the Namibia Central Intelligence Service (Act No. 8 of 2009). According to Kaasen, the Director of ICT management in the Ministry of ICT (interviewed 16 July 2013), these centers are in the process of being established, citing difficulties with assets and expertise.

Infrastructure and equipment contribution immensely to cybersecurity effort, for it is through which all information and data are obtained. This task requires commitment and enthusiasm from the line ministry to be realized, and this may be a gray area that require urgent attention from the government because the country needs well trained people to manage cybercrime as a matter of emergency.

As Lorents and Oties put it, the police can investigate a case, and when the police follow the ‘leads’ the cyber criminals knew the police were going to raid them and seize their hardware and

[153] Riptech. *Riptech Internet Security Threat Report*. Riptech University: USA; Arizona obtained on 4 July 2016 from http://www.4law.co.il/276.pdf

[154] Communication Act, 2009 of the Ministry of ICT. Windhoek, Namibia

therefore destroyed the evidence.[155] As such, there is a pressing need of IT experts to examine situations and networks and/or computer to establish the space of compromise.

In addition, Lorenta and Oties further stressed that there could be a legal expert to guide IT expert as to how to preserve evidence and advise him that evidence will be crucial in establishing the basics of crime. These require highly qualified professionals which Namibia lacked.

However, reported cases are being investigated by NAMPOL Crime Unit, except in parts where it lacked expertise and means such as IT and legal, which always lead to interruptions in finishing such cases.

Some cases are still undecided in the court for absence of evidence because the landscape of cybercrime requires sophisticated tools and expertise to follow, which our police did not have, since evidence can be cleared quickly. The reported cybercrimes might not necessarily be committed locally; but be actioned in different countries, and spread to Namibia.

3.4.4 Inter-agency cooperation

Inter-agency cooperation can be described as a procedure in which two or more organizations decided to share resources so as to solve a specific problem or meet a specific need.[156] The Buzan and Weaver[157] from Copenhagen School of security studies, alluded to this in their securitization process by indicating that by working together, agencies will increase their effectiveness, strengthen resource base, and decision making capabilities, to effectively assist in

[155] Lorents, P. and Ottis, P. *Cyberspace: Definition and Implications*. (Cooperative Cyber Defence Centre of Excellence. Estonia: Tallinn, 2013) p 16

[156] Canham, R. *Interagency coordination and rapid community growth*. (University of Arizona.1999), p 34

[157] Buzan, Barry, Ole Wæver and Jaap de Wilde Security: A New Framework for Analysis. (Boulder, Colorado: Lynne Rienner, 1998), p 150.

the determination of a community needs or problem that any single agency cannot accomplish acting alone. As such, inter-agency cooperation brings an important force multiplier to the combating of cybercrime. According to ex-Minister of ICT[158], corporation is vital hence a requirement between different agencies, land particularly lawyers, police and the courts to properly prosecute cyber related crimes..

NAMPOL opined that cooperation at some levels is limited and this is restricted by the monitoring equipment and experts. Among different agencies, only Bank of Namibia seems well equipped and is having qualified personnel who are always assisting the Police with investigations. Moreover, other Banks, Ministries and Parastatals. Anti- Corruption Commission (ACC) and other Private Auditing Companies, such as Pricewaterhouse Coopers (PCW) share the little they get with the police.

However, lack of inter-agency collaboration hampered law enforcement agencies' ability to solve cybercrimes. As per the law, there are some specific agencies which are given a role to coordinate cybercrimes country-wide, for instance the Bank of Namibia, the Courts, CRAN, Receiver of Revenue, the Police force and NCIS, these institutions should then coordinate with commercial entities such as Telecom Namibia, MTC, Commercial banks and other firms in the country.

Specifically, the Communication Act provided for the formation of an independent Communications Regulatory Authority of Namibia; and the creation of an Association to manage the internet domain name, space and for other things connected therewith.[159] Prevention of Organized Crime Act, (No. 29 of 2004), provided for the formation of a Criminal Assets

[158] Menges, W. *Court Orders Removal of Facebook Smut - AllAfrica.com*. The Namibian. 25 January 2015, p 5
[159] Communication Act, 2009 of the Ministry of ICT, Windhoek, Namibia

Recovery Fund and a Criminal Assets Recovery Committee. All these are set-up to contribute to the fighting of crimes, including cybercrime, but is not yet fully operational.

3.4.5 Combined effort

The four mentioned components should contribute equally to combating cybercrime, and should not operate in isolation. Ironically, it showed that the state authority did well in setting up all these institutions; however, the implementation is lacking, that perhaps make it less active.

According NAMPOL, between 600 and 700 cybercrimes are reported per month, but given the crime rate in the world, this number is very small, which indicates that many happenings were not reported.

As stressed by Gercke, an ITU expert**,** cyber criminals target users who does not comprehend how they work**,** further indicating that many incidents of computer crimes occur on daily basis.[160] Equally, the statistic of victims in Namibia is not known because they are not taken serious as it affect individuals who capacity and skills to pursue it. Therefore, the lack of reporting cybercrime cases led to ambiguity as regards to crime**.**

In most countries, Namibia included, law enforcement has a shortfall of 5 to 10 years behind the international crime curve relative to technological capabilities"[161]. It seems there is challenge of common laws, no sophisticated technology at our disposal, nor the requisite manpower and expertise to effectively deal with complex criminal actions for example money

[160] Gercke, M. *Understanding cybercrime: Phenomena, Challenges and Legal Response*: Geneva: ITU Publication. Vol. 6, (2012) p.36

[161] European Union Agency for Network and Information Security, *An evaluation Framework for National Cyber Security Strategies. (*Brussel, 2014), p 46.

laundering. The police already have their hands full with the handling of so-called "traditional crimes", however, the country still faces the challenges mentioned above relating to training and manpower. Otherwise, given the progression of cybercrime and the speed of technology, the newly produced laws could be outdated without being implemented. It therefore suffices to say that, there is a pressing need for mobilization all state machinery to manage cybercrime.

3.5 Conclusion

This chapter examined cybercrime activities in Namibia and looked into the preparation and coordination of stakeholders in the country to fight the phenomenon. Information is provided by officials and technocrats who represented different offices, ministries and agencies, in Namibia and also other international institutions. It underscored the fact that, although new cyber laws are to be introduced into the future, the authority at this time use different laws, protocols, agreements and control measures which are underway at different levels, both locally and internationally, with significant successes. Nonetheless, different authors have written on the growing cybercrime trend in the international affairs and economic inter-linked. Although some commitments were undertaken towards addressing the challenges modelled by cybercrime, by reviewing laws and creating task forces, it seems that changes in laws are not made fast enough as the internationalization of cybercrime makes it hard to trace as offender use the third countries through which they commit crime. This study considered precisely Namibia’s organisational set-up to confront this challenge, by analysing the four main components of combating cybercrime, which are; the law, law enforcement agencies, information and data management and interagency cooperation. All should contribute equally, whereas, if only one fail to contribute, the effect will be felt by others, and it weaken the whole system.

CHAPTER FOUR

CRITICAL ANALYSIS OF CYBER SECURITY IN NAMIBIA

4.1 Introduction

This chapter analyses panorama of cybercrime in Namibia, critically looking at the ways it occurs and the remedies available, with the intention of identifying gaps in the judicial system, which the authority has to cogitate with the aim of containing the cybercrime phenomenon. Information security solidification require confidence framework, including authentication, network security, privacy and consumer protection for the improvement of the Information Handling Culture besides building self-confidence among users of ICTs. To achieve all these, a universal culture of cybersecurity is to be promoted, developed and executed in partnership with all participants and international expert bodies. Namibia need just that arrangement so that the phenomenon of cybercrime can be contained.

To analyse the findings, it is indispensable to closely examine the perspicacity of respondents so as to tease out inferences, hence, it is imperious to scrutinize these findings. As Thucydides in Zalta asserted, cybercrime is derived from the realism theory which deem information as power through which states wants to dominate others to defend their interest.[162] In this regards, it employs the method of collecting intelligence about military technology by hacking into other communication system. Data can be collected through various ways and by different players, being it individual or group.

Ironically, the usage of cyberspace has provided a leeway to be exploited by different groups and individuals whose ambitions are to gain more of information over others. A compromised information is detrimental to the owner thus create a threat. One typical example is

[162] Thucydides in Zalta, E. Political Realism in International Relations, (Stanford University, 2010), p 8.

purported China capability of anti-satellite system to shot down other satellite which is worry some to countries who owned satellite.[163]

This is because the information about satellite characteristics is collected through cyber means. The initiative is to secure interests and to reaffirm realist thinking that who hold power can win the race.

4.1.1 Effectiveness of the existing laws

The study acknowledged that anticipated cybercrime bill is still under debate and that existing laws have gaps that are being exploited by criminals. As technology is changing too fast, Namibian laws cannot catch-up with it. Most cybercrimes are conducted remotely, a considerable distance away from the target scene. As alluded to by Schjolberg and Ghernaouti-Hélie, a high percentage of cybercrime investigations are impeded by sovereignty, thus have significant jurisdictional problems.[164] Thus, it become difficult to make available evidence in the court of law and eventually rendering the interpretation of conventional laws difficult. Such argument was exploited as a ground for cases that are withdrawn on technicalities. It eventually, created a gap in the legal fraternity which is vehemently exploited by criminals.

As Director of Communication in the Minister of ICT stressed, the bill that regulate cybercrime and cyber-security, which are crimes that are committed through internet and their prevention, is not yet completed by Parliament. As alluded to in the Global Protocol on Cybersecurity and Cybercrime, all government carry the duties to make relevant laws.[165] However, in this case, the Namibian government is delaying to conform with this provision.

[163] Mahajan, V. *Chinese Anti-Satellite Means: Criticality and Vulnerability of Indian Satellites*. (CLAWS Journal, New Delhi, 2016), p 174
[164] Schjolberg S and S. Ghernaouti-Hélie, *A Global Protocol on Cybersecurity and Cybercrime*, (Oslo, 2009), p 30
[165] Ibid, p 35

The study also revealed that responsible government departments are not doing enough to produce new policies that commensurate with new technology, since the crime dimension has changed, and became a challenge for investigation and trial of such crime. Although section 70 of the Communication Act, (No 8 of 2009) provided for the creation of interception centers as a necessity for the fighting of crimes and national security, its implementation is wanting. The law sanctions the state to acquire technological capability to be able to listen, read and track down activities of intruders who use telecommunication.

Unwittingly, this section is being challenged by human right practitioners on the basis that the Constitution of the Republic of Namibia guaranteed human right and freedom in its Chapter three.[166] The Human Rights groups also made reference to Article 19 of the Universal Declaration on Human Rights (UDHR), the 1950 Council of Europe Convention for Protection of Human Rights and Fundamental Freedoms, and the International Covenant on Civil and Political Rights (ICCPR).[167] These international instruments prohibit infringement upon privacy right, including privacy of their communications. Equally, the law should protect the Law Enforcement operatives when calls for investigating cases, which at times can require entering the premises of the suspected individual.

Nevertheless, while freedom is a pre-requisite, so is security, and one’s freedom is another insecurity, the two are essential in live, hence, there necessity to be balanced. Proponent of constitutional rights sometimes overlook security issues, yet they look for solace in secure environment which guarantee their freedom. It is privy to remember that people need protection and that of their properties including their conversations, which is the duty of everyone

[166] Wafula, P and P. Alushulu. *State Defends Plans to Snoop on Kenyans.* (The Standard, 18 February 2017), p 3
[167] Schjolberg, S. The History of Global Harmonization on Cybercrime Legislation - The Road to Geneva. (Copenhagen, 2008), p 20.

complementing the government as advocated in the securitization approach. Conspicuously, too much freedom will create lawless, while too much security will be regarded as repressive, which is always associated with authoritarian system, securitization approach does not ignore this behavior. Notwithstanding, it is indispensable to demarcate the degree of freedom required in order not to give away state security which will render the country vulnerable, hence the government as a custodian of its people should take a bold action against all odds.

As it stands, the usage of section 70 of that Act is deficient pending the court ruling. The section is incomplete with the deficiency of any supporting institutions and infrastructure available to operationalize it. Although the relevant department is preparing to put-up the required structure as per the Ministry statement. Another important observation is the nonexistence of clear retribution for non-compliance in the Act. Perhaps this may well be provided for in the envisaged Data Protection law which still in a draft form.

Meanwhile, the draft bill proposes the formation of a data protection authority and seeks to create provisions for the use, processing and collection of private information in an attempt to protect citizens' rights to privacy which is currently lacking. It is nevertheless not clear on how it will address the problem. On this note, a follow-up study is indispensable to further identify gaps that will ensue. On the similar note, the government of the Republic of Namibia is working together with the ITU on the country's cybercrime bill, which is still in draft form, to comply with the HIPSSA project. Even this draft need a thorough scrutiny and analysis to comply with the fast developing technology which was lacking in the former laws. The envisaged new law is expected address gaps in the present laws.

As alluded to by realists' scholars such as; Thomas Hobbs, Robert Jarvis and Hans Morgenthau, the International System in which ICT is born out is anarchic; and self-help.[168] As such, anybody can design a software without certification, enter the systems and infringe into others privacy. It is like any builder who can design a structure and start building without certification. The Namibian conventional laws in place are not capable of being used against cyber criminals, therefore, as can be observed, cybercrime continue unabated.

As alluded to by Ms. Kamutueezu, Acting Director, Policy and Regulations. Ministry of ICT,[169] some policy in Namibia become redundant since they are not used, hence regular revision is advised to accommodate new changes. The envisaged new cybercrime strategy was being discussed at different forums for four years now. Since then, new development emerged that need inclusion, but is seems law makers are delaying to finalize it, which shows either limited of appraisal of the seriousness of cybercrime or perhaps deficient of political will. The new law supposed to indicate how cybercrime will be tackled during the implementation of Vision 2030, but according to Kamutueezu, these inputs are delaying the endorsement of this policy. Other important provisions that requires some consideration is that of tasking institutions to budget for cybercrime mitigation projects, and put standard of training requirements (to have one minimum standard) to make it easy for control purposes.[170] As with other methods of ICTs, since this policy is critical, there is the requirements to gain political support. It can come from the government, interest groups, political parties or private sector advocates, thus any stakeholders can push for these legislation and rules.

[168] Gaus, G. Contemporary theories of liberalism: Public Reason as a Post-Enlighten Project (London: Sage, 2003), p 70.

[169] Interview with Ms Elizabeth Kamutuezu, Acting Director, Policy and Regulations: Ministry of ICT. (Interview conducted on 21 December 2016 in his office, Windhoek, Namibia)

[170] Peter Grabosky and Russell Smith. *Crime in the Digital Age*. Sydney: Federation Press, 1998, p 21

4.1.2 Effectiveness of the law enforcement agencies

The findings showed that the enforcement mechanism have deficient resources and expertise to monitor, seizure and prosecute crooks.

This finding is amazing because the government had put more resources for the past twenty (20) years to make policies and laws which required various departments to coordinate through meetings and boards at different forums to look into implementations aspects.[171] However, some respondents felt that present challenge is the absence of proper structure in Namibia that make things worse. The regularity of occurrence of cybercrime activities being reported indicated that the local stakeholders such as NAMPOL, NDF, NCIS, the Courts, BON and Receiver of Revenue seems to struggling containing these crimes. Law enforcement agencies, as indicated by the NAMPOL, lack laboratories to process the route of crimes.

The study revealed that majority of Namibian institutions are not well organized to participate in the fighting of crime, which is not among their priorities. As Taureck opined, securitizing move is in theory an option opens to any unit because when the leading actor, in this case, the government, introduce binding policies and convinced other actors of the legitimate requirements to lessen the phenomenon, that a mutual effort will inevitably address it as a security matter. [172]

The study identified lack of experts in policing as one of the gaps contributing to the slow response to cybercrime incidents. According to Sandra Garises of the central Bank of Namibia, government made funds available to enable the Bank of Namibia’s Financial Intelligence Centre

[171] Interview with Ms Elizabeth Kamutuezu, Acting Director, Policy and Regulations: Ministry of ICT. (Interview conducted on 21 December 2016 in his office, Windhoek, Namibia)

[172] Taureck, Rita. Securitization theory and securitization studies. (*Journal of International Relations and Development*. Warwick, 2006), p 11.

to conduct training workshops for local police units across the country, on cybercrime prevention during the 2014/2015 financial year. Garises further indicated that during the period, 13 training workshops were conducted on money laundering, identifying the earnings of crime, freeze assets and track down the funding of terrorism and its proliferation with assistance of experts from Australia. Although this is a short term effort and could not address the core challenge of shortage of expertise, at least it will do something meaningful. For the country

Criminals are developing new tricks commensurate with latest technologies, therefore, cybercrime need technical expertise who underwent extensive training for the reason that it involves technical aspects such as identifying problem and tracing the offender online. It therefore calls for a National Cyber Security Strategy, a package that put emphasis on long term measures to fully control this phenomenon. A program that is funded to an extend that it really addresses the problem country-wide. This project should be inclusive, with full government commitment to sponsor proper and identical education of all stakeholders that empowers policing agencies and subsidiaries to effectively carry out investigation of offences and prosecute offenders. Hans Morgenthau, a realist, posited that the country's security can solely be entrusted to the state, which has authority and power to make laws and implement it.[173] This statement elucidated the power politic in the international system.

According to NAMPOL; existing law are deficient to adequately address challenges of technology matters such as security breaches and/or online crime. Thus, the lack of legislations to address online criminality makes it problematic to prosecute offenders. The Namibian law enforcement organizations are not computer literate and have a critical shortage of forensic laboratory within any branch of the NAMPOL. The only few available are at Commercial Banks

[173] Morgenthau, H. Politics Amongst Nations. The Struggle for Power and Force (London: McGraw Hill, 1993) p 101.

which assist NAMPOL at regions to view and analyse cybercrime related issues. Due to the above mentioned impediments, NAMPOL does not publish and release statistics of cybercrime incidents in the whole country, and this make it problematic to see the trend.

A study directed by United Nations in Jamaica and Jordan states shows that there are initiative to establish specialized prosecution structures and they have plans to create a new tribunal structure for cybercrime. [174] While in some countries, the general levels of preparedness on cybercrime specialization are lower but law enforcement experts are better organized than other institution. 60% of all responding countries have established specific prosecutorial structures for cybercrime. It further indicated that the facility of police to gather and analyse electronic evidence during investigations can be critical to the successful identification and trial of perpetrators. In some countries evidence rules show a discrepancy considerably between jurisdictions, even amongst countries with related legal traditions. In general terms, however, legal structures of common law tradition tend to have defined rules as to the admissibility of evidence.

4.1.3 Information management

The study, explicitly, illustrated lack of modern infrastructure and monitoring equipment at different institutions, mainly because cybercrime is not well-thought-out as an urgent matter, and therefore is not even budgeted for. Hence, this knowledge gap, made employees not to be concerned about cybercrime. According to Sandema, specific institutions, such as banks have put

[174] UN. Comprehensive Study on Cybercrime. (United Nations Office on Drugs and Crime. Vienna, 2013), p 54

more efforts in setting up infrastructure to mitigate cybercrime.[175] These are commercial businesses and are concerned only with their customers.

This finding does not augur well for government which has a responsibility to protect privacy of all people as enshrined in Article 13 of the Constitution of the Republic of Namibia[176].

Equally, as was indicated in previous chapters of this report, cybercrime is motivated by economy; therefore, by having no control over it will likely sway away potential investors from other country.

Cybercrime phenomenon carried some reforms in handling of information which older people who had been in service for longer than 25 years could not comprehend. Most of these aged people occupy senior positions in offices various departments and agencies and supposed to impose stern control over their subordinates. However, this research found that the control is lax in many offices, ministries and agencies, presumably due to posting computer illiterate people at different departments within the government system. Then again, younger employees who are technically savvy, at times their authority is undermined by these senior employees who ignore instructions by nature of being seniors. Strong institution is always supported by the enthusiasm of employees to succeed. This campaign requires cohesion supported by understanding and inclination to attain the objectives of the institution. In Namibia, only the minister of ICT talks about cybercrime at different forums, while other branches are quite, which simply indicates that this phenomenon is not among their priorities. Even that, the speech act tells a lot on the existential of the issues to be securitized as postulated by Barry Busan.

[175] Sandema, R. Cybercrime on the rise. The Namibian. Windhoek, Namibia, (21 Jan 2015), p1
[176] Constitution of the Republic of Namibia, 1990. Windhoek, Namibia

The former president of Namibia Sam Shafiishuna Nuuyoma once said that, ignorance is a disease that can destroy the nation.[177] According Ms Kamutuezu, some Offices, ministries and agencies (OMA) have invested in modern IT system which could be utilized to monitor cybercrime. However, some challenges are obviously seen specifically in managing and maintaining these systems for its effective use. Balzacq et al underlined that to securitize an issue is to give it sufficient advocacy to win the assent of the audience, which enables those who are authorized to handle the issue to use whatever means they deem most appropriate to address it.[178]

In this case in point, the government as the authority which has overall power supposed to make certain that security is well structured so that all individuals and entities participate during securitization exercise. The most appropriate way is to start capacity building campaign for the policing agencies and other partners in order to keep well-informed about new development and enable flexibility.

The study also illustrated that some OMA does not prioritized cybercrime and is not even appearing in their budget. This is an indication that management has no required knowledge of modern technology, and this can cause network exposure to cybercriminal unknowingly. The increase success of cybercriminals gives them confidence to continue with their evil work as measure taken does not really affect their operations. Cohen and Felson alluded through rational activity process that cybercriminals assess the situation to determines whether a crime takes place.[179] Based on that assessment, it seems that the deficiency of a national Internet gateway for

[177] Sam Nuuyoma. Where Others Wavered: The Autobiography of Sam Nujoma. (Panaf Books, 2001), p 59

[178] Balzacq, T. *et al*. Securitization' revisited: Theory and cases. (The Institute for Strategic Research (IRSEM); University of Namur. 2015), p 30

[179] Cohen, L. E., & Felson, M. Social change and crime rate trends: A routine Activity Approach. American (Sociological Review, 1979), p 19.

Namibia had allowed more entry which in turn created many gaps that are exploited by criminals.

The major challenge is that only managers and administers who have little knowledge about the system sit in forums of preparation and decision making, while scientists and technical people with variety of expertise are not consulted. In that case there could be no proper budgeting for cybercrime activities. The governments of India and Egypt, government apportion about 2% of the national budget to the fight of cybercrime. In Namibia, that standard is not yet achieved, the study found it absurd and suggest that right people are put at right places to achieve such standard. In line with the securitization process, state as paramount actor leads other stakeholders to discuss and identify what should be securitized so that available resources can be prudently allocated. In this case the existence of the risk of cybercrime in Namibia is a reality therefore the government need to budget for those measure that are instrumental to contest cybercrime before the matter is out of hand.

The discovery of this malicious acts could be ascribed to law enforcement. In some structure, government makes laws but has challenge to enforce it because of lack of capacity such as of expertise and infrastructure like monitoring hubs. In this instance, the ability to detect the infringement, is a gray area in many systems and give the idea to be the fact. This may perhaps be ascribed by shortage of modern monitoring infrastructure, experts in cybercrime laws and supplemented by proper coordination among law policing agencies. Conceivably, the laws may be there, stakeholder's committees may be there, but the implementation and execution is a concern. It may be caused by negative attitude and morality of officials complimented by their lack of skills. Lack of control, it looks as if those who are entrusted to control different department are not doing their work, at times employees morale is low to deal with tasks. In that condition, there can be no improvement.

4. 1. 4 Education of employees

The study exposed that employees in government departments are unaware of cybercrime. This picture illustrated that this phenomenon is widespread but users are inept to identify it. Given the degree to which cybercrime has penetrated the global network systems for which Namibia is part of, measures to confront the impasse are immediately required. Further, the study revealed that few local IT and legal experts are capable of gathering evident, tracing and prosecute cybercrime, while ICT departments are staffed with expatriates who are imported from other country at the expense of Namibians, an exercise which is very costly. Security, as Barry Busan posited, cannot be outsourced.[180] It is the duty of the citizens of that state to improve it.

This finding illustrate perhaps that efforts to provide emergency training for Namibians is essential and therefore the government is anticipated to act swiftly by investing in this venture. It is also essential to introduce retention policies to retain such scarce skills especially in the ranks and files of the law enforcement.

As posited by Thorel, human being are the weakest link if not well prepared, but can be the strongest link if well educated[181]. The findings revealed that measures adopted to curb internet fraud in Namibia are grossly inadequate and therefore poses a serious danger to investment opportunities locally and in the region. The major challenges especially in Namibia is lack of security awareness among employees. Respondents signposted that most activities

[180] Buzan, B. & Little, R. International Systems in World History. Remarking the Study of International Relations, 2000, p 42.

[181] Thorel, R.J. Cyber Threat. Paper presented at the workshop of Shield Africa, Gabon. Libreville (May 2015)

ranging from administration, finance, political, security are dependent on computer, but security orientation is given to employees at recruitment raising the cybercrime concerns and the weakness of sensitive departmental information.

Cybercrime is stealthy by nature, something that move quick and silent. The intruder enter the network quietly with no sign of identity for general people, unless experts, but even them has to relay on special equipment and software gadgets to identify an intruder.[182] The effective method that seems to address this menace is users awareness on what their computer and mobile phones are capable of doing. By having employees who understanding the concept cybercrime and be alert at all time when using those gadget is paramount, to conceal the identity of the caller, but also the called and other information stores in the gadget, being it telephone numbers, emails or information therein.

Criminal intelligent agents use social engineering an intrigue way to tactically extract information from employees. Where employees are tempted to unknowingly deliver information concerning the department, senior officials and programs either through phone or email. For example, a secretary being requested to provide phone number and email of his/her boss by unknown person pretending to secure an appointment. This information will then be use to go into the system. Intelligence agents only need a hint of information as a lead, the rest is history. In this world, individual intelligence is put under test every moment, thus, it required a well vested individual to escape this tolled.

The common cybercrime in Namibia is card fraud. Card fraud happened when a swindler gets user’s Personal Identification Number (PIN) or the information on the ATM card to acquire access to the funds in your account. Many Namibians use credit cards wen shopping and other

[182] Avevor, I., *et al*. Cybercrime and Criminality in Ghana. (Journal of Information Technology Impact, 2011), p 16.

services. While this method is appreciated, it is exposed to fraud. NAMPOL is overwhelmed with consumers reporting incidents of card fraud. SA Banking Risk Information Centre indicated that card fraud cost the economy dearly with R 454 million loss in 2014[183] alone. As was indicated by the Manager at Forensics, First National Bank (FNB) Namibia, during interview, card fraud is a concern for the bank and electronic payment firms like Visa. To address this challenge, FNB and Visa joined each other to offer card fraud prevention information to Namibian consumers in whatever is anticipated to become an annual card security awareness campaign. This is line with securitization process which requires stakeholders to address security issues together.

Preliminary, Namibia was a transit for cybercrime, through which fraudsters attacked other systems, but at the moment it is among the soft target where criminals entered the system undetected, that could be prevented by consumer education. Banks and users are at risk of card cloning. To this effect, BoN reported a sequence of incidents such as skimming of card and PIN interception which were recorded in several parts of the country.[184] Several card fraudsters were arrested in the past, some of which were convicted, while others were set free on technicalities. This demonstrated a lack of capability to seriously punish these fraudsters and that encourage the increase of this acts, which target people at rural areas who do not have the funds for good lawyers.

NAMPOL has over the time raised angst on the increased public complained that accounts are being opened and operated in their name. The challenge affecting the performance of police seems to relation with cybercrime sub-division lack of the required capacity and

[183] Mbokazi, S. SA credit card fraud losses rise to R454m. SABRIC, (*Independent Newspapers, Nov 25, 2014)*, p 16.

[184] Muraranganda, E. Cyber Criminal on Borrowed Time. (Windhoek. Namibian Sun, 27 February 2015), p 13

authority to investigate, if anything on the network that poses threat to the Namibian publics is detected. Law makers are therefore informed by these empirical evidence which indicate clearly the impact of cybercrime to the economy, political, safety and security in their country that will eventually determine the speed of passing the law to address it.

4.1.5 Budget allocations

The research found that several offices, departments and agencies in Namibia does not yet budget for cybercrime activities. These entities are either not yet absorbed on the securitization project in the country, which is the government duty to provide leadership, or the government itself is too lax to take the lead. It is internationally agreed that 2% of the budget should be apportioned for programs against cybercrime. India, Kenya, Australia and SA are all inclined to this provision of international law, and are able to make significant development in the combat against cybercrime in their countries.[185]

In Namibia, the government has strength in formulating policies, but weakness in funding it. Even in the bill under discussions this provision of percentage on national budget that goes to battle cybercrime is not there. The important to raise awareness among law makers to know that the more they ignore funding cybercrime, the faster it increase.

4.1.6 Inter and intra-agency coordination

As stated by the Ministry of ICT, the government invested too much in the expansion of IT both infrastructure and education. In addition, it has organized several forums over the past seven (7)

[185] Parulekar, D. Strategic national measures to combat cybercrime: Perspective and learnings for India, (August 2015), p 38

years to organize agencies to coordination and sharing information and data pertaining to cybercrime throughout the country.[186]

Despite that effort, the study found the deficiency of incongruity of development between different offices, ministries, and agencies in the part of IT with regards to the pursuit of technological changes, because, as the study shows, some institutions have up-to-date communication systems and infrastructure, while other are lacking behind, thus, caused by technology gap. The training seemed not to produce the real need of the users as many people trained have no capacity to make an impact by of propagating the message to their institutions. The much talked about multi-agencies approach seems challenging as people from different sectors may not cooperate, because these are organisation brought together and told to do somewhat they have no incentives.

Most of respondents are skeptical on the coordination among government, business and individual in the protection against organized attacks capable of wreaking damage to economy of the world. Countries like South Africa has already created joint response mechanism called Computer Emergency Response Team(CERT), which comprises experts working together with law enforcement to handle computer security happenings[187]. In Namibia, government intends to establish necessary infrastructure starting with conducting capacity building workshops on cybercrime through public enlightenment programs, such as interactive session with the Bankers' Committee and government agencies, and associating with business sector in setting network security rules.

[186] Interview with Ms Elizabeth Kamutuezu, Acting Director, Policy and Regulations: Ministry of ICT. Interview conducted on 21 December 2016 in his office, Windhoek, Namibia.

[187] State Security Agency. Computer Security Incident Response Team (CSIRT). Pretoria, 2012

As it stands, many institutions in Namibia have adopted new technology but only few of them such as NAMPOL handles these incidences, in coordination with banks and few institutions country wide that have limited capabilities such as forensic laboratories. It requires that proactive measures to be applied against cybercrime, such as setting up of monitoring hubs to ensure cyber safety on the Internet. The absence of multi-agency collaboration and capacity in institutions is a huge setback and criminal are using this chance to attack other countries through Namibia, and also to drudge into local network. On 10 June 2010, a team of hackers by the fake name 'the Moroccan Exploiters Team' hacked into Namibian websites, shutting down sites, including that of the Parliament and Government Institutions Pension Fund (GIPF), placing their calling-card logo cover-page up, as a substitute of the local site homepage**.**[188] According to the crime squad**,** it the second time in a year that such outbreak happened on the same institutions.[189] This event can affect business country-wide and make investors are skeptical about the safety of information. Developing countries for example Namibia has to deploy the ITU toolkit in ensuring cybersecurity.

ITU toolkit is a applied tool designed to mitigate cybercrime which countries can use for the explanation of a cyber-security legal agenda and related laws. In addition, it supplements the effort of consultation, bringing together and team work amongst governments and the business sector, which are important if stakeholders are serious about tackling this elusive phenomenon. Those firms authorized to prove internet should be obliged to report any incursion they detect to the police. Since cybercrime is a worldwide problem, law enforcement agents in Namibia requires strong collaboration with major international security organizations for example the Federal Bureau of Investigation (FBI) and also INTERPOL to assist in investigation on cyber

[188] Graig, A. Namibia hacked again. (WHK; Informante, 10 June 2014), p 1.
[189] Namibian Police Crime report, Windhoek, Namibia. July 2010

criminality. It is mandatory that proper harmonization of possible measures, practices, and procedures be done for combating this problem. Harmonization of laws is necessary at all levels of society to encounter the challenges of technology internationally and its accompanying problems.

4.2 Research and Development (R&D)

Cybercrime is common to both developed less industrialized countries. Is happening fast and therefore need also fast action. It requires collaborations in R&D of all institutions locally, as it is happening in other countries in the world. However, its perseverance gives the imprint that developing countries for example Namibia, Botswana and Lesotho are less affected because the technology is not embraced as much as in industrialized countries such as USA, China and France. To substantiate that argument, the cyberattack that was carried out in May 2017, and which infected over 300 000 computers worldwide, have grave impact in developed countries for instance Russia, India and Taiwan, and was not even felt in developing countries.[190] The source of that attach could only be found through research laboratories in which developed countries invested heavily.

Meanwhile, effort being taken in Namibia includes the effort by the University of Namibia to develop courses on cybercrime in its curriculum. While it may take time to produce experts, the initiative is worth encouragement to reinforce the government agencies, financial and legal institutions to lessen cybercrime by all available means. This initiative calls for a multi-stakeholder investigation at national level. With regards to the practice and policy effects, the research provides the foundation for a rigorous effort on the part of private citizens and corporate

[190] Simon Choi. Worldwide cyberattack sparks fewer aftershocks than feared. Reuter. Seoul. (17 May 2017)

bodies, to report cybercrime cases and demand that government produce laws, policies and technologies to curb cybercrime.

4.3 Modern day approach to addressing cybercrime

Issues of coordination become crucial. To address the cybercrime challenges, it need a campaign planning at national level. Planning need coordination, distribution of responsibilities, and clear what role for each player. Campaign Planning (CP) is a new approach linked to specialized area of thinking. A good campaign planning is to give a timeline and start with action, it all depend on the context. It is significant to have different objectives for the one CP.

It is imperative to develop and define parameters to securitize networks and have points of monitoring for the success of CP. This will be complimented by specialists in both cybercrime and laws experts. The judiciary has to be aligned to this project because of the nature of its work. For example, the police evidence to be accepted in the court. As it stands, the courts are more independent, make room for criminal to escape punishment. There is a necessity for a national council to engage in budgeting to limit duplication by ensuring that resources are pooled in one vote and the equipment to be acquired and expert being prepared serves the whole country, not one department.

Realistically, cybercrime is a challenge that cannot be lectured in isolation. This rise the important issue of methodology on how to shared data so as succeed in the CP. Shared cyber data should be reliable and actionable, the challenge with cyber data is that it is illusive, meaning that it can be deleted and become difficult to trace.

Coordination is an important aspect of national CP to be carried out by the national designated body, a council, not a ministry. It should be established by policy of the government.

The function is multi sectoral as it is executed at national level. Coordination should also reach to other states and world organisations to address pertinent issues on bilateral and multilateral basis through diplomacy.

Most less industrialized countries are not in charge of their own security because they outsource consultant to install its communication systems and operate it without knowing who is connected, sometime the supplier keep the pin code. To make things worse they receive software and hardware equipment already prepared from the supplier, which could be installed with backdoor to guarantee that the someone has access to download the information anytime the internet is on and transmit all information to the supplier without user's knowledge. This does not only expose users but it encourages the supplier to continue supplying at a discount price a deal which African people always are like to hear. This can be addressed through capacity building. Software is easier to design and need to create capacity around this. Even within the framework of the architecture of the state, the definition of power is distorted. You cannot claim power if you cannot protect yourself.[191] It also matter how security sector work together. We create enabling environment to provide protection by creating relevant institution and infrastructure for other sector to complete their work, laws, links, etc.

Non state actor such as banks are far ahead in development, but they don't have authority and capacity to make public laws. The government is charged with the security responsibility by its citizen including the banks. It created laws to punish offenders without infringing in privacy. Ordinary people are dissatisfied with fraud and scam, they cry to the state not to the bank and if laws are not there, state fails in its obligations to create good living. Cybercrime is bad for economy as it can sway away potential investors with the consideration that there is lack of

[191] Muagiru, M. Lecture on Introduction to Crisis Management Campaign Planning, National Defence College, Kenya, 19.07.2016

protection. Capacity gap in institutions impede the security agencies to carry out their work, the exploitation of these gaps such as by Morrocan hacker group could be avoided. When policies made by global institutions have disastrous consequence, the agency is not accountable, there is a challenge of governance in Africa, where states ignore policies, conventions and agreement which they put forth. This is perhaps caused by international system as postulated in realist's views.

4.4 Conclusion

This chapter, dealt with the conclusions of the study. The researcher conducted as many experts as possible, which reinforce the validity of the findings. It shows that the absence of proper policies still challenge given that the envisaged cybercrime law has been debated without breakthrough for five (5) years now. It concludes that inadequate infrastructure such as network hubs and forensic laboratories impede the monitoring and controlling of the system. There is severe shortage of experts in public institution as compared to private institution such as banks. The other deficits are in intra and inter agency cooperation, the study found that only police and banks cooperate while other institution's contributions is minimal. The judiciary is not fully on board as it released criminals mostly on ground of technicalities, which, if it cooperates with other law enforcement, can make a difference. Finally, results were presented, followed by detailed interpretations of the findings to make sure that the research objective is achieved.

CHAPTER FIVE

CONCLUSION AND RECOMMENDATIONS

5.0 Conclusion

This chapter conclude the research work by pointing out the core finding and suggest solutions grounded on the Rational activity process by Cohen & Felson which posits that "crime occurs when a motivated offender comes into interaction with a appropriate target in the lack of a skilled custodian that could hypothetically thwart the offender from committing crime".[192] The study therefore concluded that:

First, this research brought to the fore factually that cybercrime is fast gaining grounds in Namibia. Nevertheless, there is lack of capacity to respond as the agencies responsible for coordinating the response and other mechanisms are yet to be instituted.

Second, the leading perpetrators are mostly non-nationals who have technical competence, experience and willingness to commit computer-related crimes. They established local contacts who they used as pawn controlled afar. The research establishes that Namibia is used as a passage country to penetrate the network of other countries.

Conspicuously, this could be addressed through the development of appropriate youth and community programs to tease out the technical competencies of the youth in the country.

Third, the research data also presented indicated that most cases go unreported due to inability to identify crimes, lack of appropriate instrument in the prosecuting process and some victims fear the humiliation. Namibia government is yet to create any law to specifically address

[192] Cohen, L. E., & Felson, M. Social change and crime rate trends: A routine Activity Approach. (American Sociological Review, 1979), p 40.

these forms of crime. The laws under which the suspects are charged are the existing conventional laws that over passed by time. Defense lawyers often win over when the trial presents poor evidence.

Fourth, the study shows a mismatch in the development of information technology between different ministries, offices, and agencies which eventually signifies lack of proper multi-sector collaboration. These institutions supposed to cooperate and share information and data on suspicious activities and then pass the information to the law enforcement, instead, it allows organized criminals to enter the system.

Fifth, it was established that Namibia lack expertise to produce cybercrime laws, which according to securitization process, is a necessity for managing cybercrime cases in the country. As per vision 2030, each government department is obliged to develop its human resource capacity to be able to achieve goals of the government by 2030. This task is rest with the Permanent Secretaries and Directors of government departments but it seems this directive is not being implemented. Government strength is formulating policies, but weakness in funding it. For example, how many % on national budget goes to fight cybercrime.

Sixth, the study discovered that conventional laws and policies are incapable to mitigate cybercrime cases. Therefore, it crucial to review it in order to include new technological changes.

At this point in time, there is no national structure to respond to cybercrime incidents in the country, but agencies such as police and banking institutions do it alone. There is no immediate local solution as department has not started to budget for cybercrime. Training program are run with donor funding. It should be clear that donor aid cannot address the problem wholly, it is only to give a tip, but the government should initiate action in coordination with other states, as per securitization theory.

Seventh, the study also established that cybercrime is not considered as a priority in several departments; hence, it is not even budgeted for as the securitization framework postulates. In this connection, it was observed from the study that some senior staffs in some ministries are aging and does not concentrate on future plans any more, but, yet, they could not groom youngsters because of fear that they will take their positions, and this makes the system vulnerable to cyber criminals. This state of stagnation is reducing the efficiency of government to effectively respond to crimes, while motivating criminals to perpetrate crimes.

Eighth, as show in the study, there are few modern infrastructure set-up and equipment to monitor cybercrime at the national level. Equally, there are few local experts to manage cybercrime, and according to the routine access approach, this state of affairs is an exposure to cybercriminals.

Ninth, it also come to light that no census was carry out in the country to understand the magnitude of cybercrime and be able to make appropriate policies and programs to mitigate it. Even within departments, only few had come up with policy and systems to monitor and detect these incidents. It seems there are no collaborations of all institutions in research and innovation in the country.

Tenth, cybercrime is happening fast, similarly, the response need also to be proportional, however, the research established that there is no strong teamwork between different institutions in the country, both government and, business and individual to report cybercrime. The plan to set up a National Computer Crime Resource Centre, which should comprise experts and professionals to establish rules, regulations and standards for network security protocols, is set to be in place after the laws is passed.

Eleventh, the country seemed to depend on buying computer from the market on-shelf, which comes with backdoor system. These programs are dangerous because when the computer is switched on, it exposes all information to the criminals on-line.

Twelfth, the study established that there is a misalliance of IT facilities in offices, ministries and Agencies, such that it makes communication between departments difficult. Vision 2030 specified that every department is responsible to develop its staffs and infrastructure to make its input to the development of the country, including information sharing. Therefore, it should be understood that one department's output is the other' input. For instance, the receiver if revenue detect crime incident, it reports to the anti-corruption commission, who take it to the police, who take it to court of law. As a result, if one sector in the chain is broken, then both the initiator and the finisher will fail, hence, the importance of inter-agency cooperation in combating cybercrime. There is more time wasted in the process.

Factually, it requires a paradigm shift for those entrusted with management responsibility, because if development plans are not implemented, then these officials should pave the way for those energetic people who can make a difference. The study also establishes that there is no adequate national framework and infrastructure for the protection and management of electronic payment fraud and other cybercrimes. This calls for urgent Government action through law enforcement to commit resourced on this project address this impasse.

5.1 Recommendations

Government should set-up a strategic national coordinating body, as a matter of urgency, whose tasks will be to;

- Manage anti-cybercrime matters including budgeting, organizing experts training, handling cybercrime reports, coordinating with other states and international organizations in order to share the available resources while addressing the shortage of experts in the country.

- As Information Technology cut across all sectors of the economy, and the fact that this created another challenge of cyber warfare. This brought about an urgent need for local capacity in terms of experts and infrastructure that can respond to such situation. Therefore, the government should seriously look into developing such capacity.

- In addition, all structures of OMA to acquire own experts and an office dealing with anti-cybercrime matter within their structure, which will then coordinate with the national bodies.

- It is also recommended that the government introduce retention policy with incentives in order to keep young and aspiring engineers in the service because these people are attracted by incentive, to understudy foreign experts.

- The study recommended a multi-sectoral approach to educate youth in order to produce local expert that will drive the national campaign towards self-sufficiency. The exercise should include employees of government departments, financial institutions, internet service providers and internet businesses.

- For individual citizens, technology to be included in school curriculum to focus on sensitization of online conduct and measures to identify forms and behavior of perpetrators, and to prepare learners psychologically to deal with this phenomenon.

- Businesses, on the other hand, need to strictly develop appropriate policies governing online conduct and technical security measures to protect organizational information systems and networks.

- Further, government should introduce retirement packages to attract aging and ineffective officials into retirement and give a chance to younger and energetic people who understand technology better.

- On lack of legal expert on cybercrime, it is recommended that Namibia utilize the opportunity provided for by ITU (HIPSSA project) to be assisted to enact and enforce cybercrime laws, and to design systems that have specified security standards.

BIBLIOGRAPHY

Alam, S.M. "Globalization and its Discontent: The Dialectics of World Development and the Emergence of New Social Movement," *Journal of Developing Societies* (2003).

Alweendo, T. *Report on Financial Crime in Namibia – Evidence, Economic Effects and Countering Mechanisisms*. (paper presented in a workshop on cybercrime, 20 June 2007, Windhoek: Safari Hotel.)

African Union. AU Convention on Cyber Security and Personal Data Protection, 2014, Art 27(a & c)

African Union. Draft African Union Convention, Part III, Chapter V, Section II, Chapters 1 and 2

Avevor, I., K. Offei, E. Nketiah, F. T. Nartey, E. Boryor, S. Abubakar & O. Sakawa. Cybercrime and Criminality in Ghana. (*Journal of Information Technology Impact, 2011)*

Balzacq, T., S. Léonard and J. Ruzicka. Securitization' revisited: Theory and cases. The Institute for Strategic Research (IRSEM); University of Namur. 2015

Barry B. and R. Little. International Systems in World History. Remarking the Study of International Relations, (NY, 2000)

Battersby, P. Globalization. An Agenda in Steger, M., Battersby, P. and Siracusa, J. (Eds), *The SAGE Handbook on Globalization*, (SAGE Publication, London, 2014).

Bednarz, A. Profiling cybercriminals: A promising but immature science. (2004) Retrieved from http://www.networkworld.com/sup p/ on 12/10/2016

Ben, I and L. Tabansky. "An Interdisciplinary Look at Security Challenges in the Information Age," Military and Strategic Affairs no. 3 (2011), p. 24

Birchfield, R. Cyber Threats and Data Privacy Management. New York, 2013 pp.46-51.

Bolton, J. "*Beyond the Axis of Evil: Additional Threats from Weapons of Mass Destruction*," (Washington, D.C, 2002)

Brenner, S. Defining cybercrime: A review of state and federal Law. In R. D. Clifford (Ed.), *Cybercrime: The Investigation, Prosecution, and Defense of a Computer-Related Crime*. Durham, NC: Carolina Academic Press. (2006). p. 394

Burg, D. PwC's Global and U.S. Advisory Cybersecurity Leader, 2014

Burke RH (2009) An Introduction to Criminological Theory. Oxon, England: Taylor & Francis.

Buzan, B. O. Wæver and J. Wilde. Security: A New Framework for Analysis. Boulder, Colorado: Lynne Rienner, 1998

Buzan, B. *People, Fears and States: An Agenda for International Security Studies in the Post-Cold War Era*, (Boulder, CO: Lynne Rienner Publishers, 1991)

Canham, R. *Interagency coordination and rapid community growth*. University of Arizona.1999

Chowbe V, S. Legal Control of Cyber Crime in India; Problems and Prospects (India, 2015)

Cohen, L. E. & Felson, M. Social change and crime rate trends: A routine Activity Approach. American (Sociological Review, 1979).
Commonwealth of Independent States Agreement, Art. 1(a)

David S. Wall. Cybercrimes: The Transformation of Crime in the Information Age (Cambridge: Polity, 2007)

Defence Centre of Excellence. Estonia: Tallinn, 2013, p16

ECOWAS Draft Directive, Art. 17 (Facilitation of access of minors to child pornography, documents, sound or pornographic representation). and, Pocar, F., New challenges for international rules against cyber-crime. European Journal on Criminal Policy and Research, 10(1), 2004.

European Commission. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (Brussels, 2013).

European Union Agency for Network and Information Security. *An evaluation Framework for National Cyber Security Strategies, 2014*

Finnie, T., T. Pete, and J.N. Jarvis, (Eds). *The Future Challenges of Cybercrime: Volume 5 Proceedings of the Futures Working Group.* (Quantico, Virginia 2010).

Gerald, G. Contemporary theories of liberalism: Public Reason as a Post-Enlighten Project (London: Sage, 2003)

Gercke, M. *Understanding cybercrime: Phenomena, Challenges and Legal Response*: Geneva: ITU Publication. Vol. 6, (2012) p.36

Gilpin, R. *The Challenge of Global Capitalism*, (Princeton, N.J.:

Glyn, E.A. Computer Abuse: The Emerging Crime and the Need for Legislation. 1983

Goldman Sachs. “e-Commerce expected to accelerate globally in 2014”, Equity Research, New York: The Goldman Sachs Group, Inc., 5 March 2013. And’ e-Marketer, “e-Marketer in review – key 2013 trends, coverage areas and platform growth”, Newsroom, 4 September 2013.

Goodman, M. *Interpol’s Role in Fighting High Tech Crime*. (Geneva, 2006), p13

Grabosky, P. Organized crime and national security (Report No. 2014/40). Canberra, Australia: Regulatory Institutions Network, 2014

Graig, A. Namibia hacked again. (Informante, 10 June 2014)

Grindle, M. S. “Ready or Not: The Developing World and Globalization,” in J S. Nye and J D. Donahue, (Eds), *Governance in a Globalizing World*, (2010) pp. 184–188.

GRN. Results of National Statistics 2011. Statistics Office

Grobler, M., S. Flowerday, R von Solms, and H. Venter. “*Cyber Awareness Initiatives in South Africa: A National Perspective*”, (Pretoria, 2011)

Guanci, R. J. Unrestricted Warfare: The Rise of a Chinese Cyber-Power. (Seton Hall University, 2014). Paper 488

INTERPOL. Third INTERPOL Symposium on International Fraud, Paris 11-13 December 1979

ITU. “ICTs facts and figures 2013” and, ITU Telecommunication Development Bureau (Geneva, 2008).

ITU. Understanding Cybercrime: A guide for Developing Countries, 2011

Jaishankar, K. Expanding Cyber Criminology with an Avant-Garde Anthology. In: Jaishankar, K., (ed.) Cyber Criminology: Exploring Internet Crimes and Criminal Behaviour. Boca Raton, FL: CRC Press, Taylor & Francis Group, 2011

Karamchand, V. An Overview Study on Cybercrimes in Internet. *Journal of Information Engineering and Applications,* Vol 2, (2012).

Keohane, R, O. and J S. Nye. “Introduction,” in J. S. Nye and J. D. Donahue, (Eds), *Governance in a Globalizing World*, (Washington, D.C.: Brookings Institution Press, 2010)

Kigerl, A. Routine Activity Theory and the Determinants of High Cybercrime Countries. Social Science Computer Review, 2012

Koops, B. J. The Internet and its Opportunities for Crime. In: Herzog-Evans, M., (ed.)

Lampe, K. 'Not a process of enlightenment: the conceptual history of organized crime in Germany and the United States of America'. *Forum on Crime and Society* Vol. 1 No. 2, (December 2001)

Lee, A, L and T. Brewer, (Eds). Smart Grid Cyber Security Strategy and Requirements. USA. *National Institute of Standards and Technology report, 2009.*

Levine, J. H. *Introduction to Data analysis: The Rules of Evidence*. Macintosh. (USA: New Jersey, 1996)

Lynn, D. E. Globalization's Security Implications. *Issue paper*, Rand. California (2013).

Mahajan, V. *Chinese Anti-Satellite Means: Criticality and Vulnerability of Indian Satellites*. (CLAWS Journal, New Delhi, 2016)

Maughan D. The need for a national Cybersecurity Research and Development Agenda. (Communications of the ACM, 2010)

Mbokazi, S. SA credit card fraud losses rise to R454m. SABRIC, (*Independent Newspapers, Nov 25, 2014)*

Melissa E. Hathaway, "Falling Prey to Cybercrime: Implications for Business and the Economy," ch. 6, in Securing Cyberspace: A New Domain for National Security (Queenstown: Aspen Institute, February 2012).

Menges, W. *Court Orders Removal of Facebook Smut - AllAfrica.com*. The Namibian. P.5. 25 January 2015.

Ministry of ICT. Communication Act, 2009.

Muraranganda, E. Cyber criminals on borrowed time. Windhoek. Namibian Sun. (27 February 2015)

Mvula, E. Establishing and Strengthening the National System of Innovation. Paper presented at a workshop in Windhoek, June 2015.

NAMPOL Crime Report, Windhoek, December, 2015.

National Assembly. Constitution of the Republic of Namibia, 1990

Notification National Cybersecurity Policy. (India Ministry of Information and Communication Technology, 2013)

Oman. Royal Decree No 12/2011 issuing the Cybercrime Law; Philippines, Cybercrime Prevention Act, 2012

Parulekar, D. Strategic national measures to combat cybercrime: Perspective and learnings for India, (August 2015)

Powell, B. Is Cybercrime a Public Good? Evidence from Financial Service Industry. (*Journal of Law and Economy*. 2005).

Rawls. J. Political Liberalism. (New York: Columbia University Press, 1996)

Richardson, C. Cyber criminals demand a modern approach to security. The Dominion Post. (2015) Retrieved on 29 September 2016 from http://www.stuff.co.nz/technology/digitalliving/64625717/.

Riptech. *Riptech Internet Security Threat Report*. Riptech University: USA; Arizona obtained on 4 July 2016 from

Rishi. R. Strategic National Measures to Combat Cybercrime: Perspective and learnings for India, 2015

Rosenbach, E. and R. Belk. U.S. Cybersecurity: The Current Threat and Future Challenges. In N Burns and J Price (Eds) *Securing Cyberspace – A New Domain for National Security*. (Washington, DC: 2012)

Salifu, A. The impact of internet crime on development, (*Journal of Financial Crime*, 2008).

Sandema, R. Head of NAMPOL Anti-Money Laundering Unit (WHK. interviewed 21 July 2013)

Schjolberg S and S. Ghernaouti-Hélie. *A Global Protocol on Cybersecurity and Cybercrime*, (Oslo, 2009)

Schjolberg, S. The History of Global Harmonization on Cybercrime Legislation - The Road to Geneva. 2008

Schmidt, W.E. Legal Proprietary Interests in Computer Programs: The American Experience. Jurimetrics Journal, 1981

Scott, J. *Understanding Contemporary Society: Theories of the Present*. New York. Sage Publications (2013).

Shinder D. L. and M. Cross. *Scene of the Cybercrime* (Burlington, MA: Syngress, 2008).

Statement at UN Security council, SC/9867, February 2010

Sterling, C. Crime Without Frontiers: The Worldwide Expansion of Organized Crime and the Pax Mafiosa. New York: 1995.

Taureck, R. Securitization theory and securitization studies. Journal of International Relations and Development. Warwick, 2006

The Rise of a Chinese Cyber-Power. (Seton Hall University, 2014)

Thorel, R.J. Cyber Threat. Paper presented at the workshop of Shield Africa, Gabon. Libreville (May 2015)

Thucydides in Zalta, E. Political Realism in International Relations, (Stanford University, 2010). http://plato.stanford.edu/entries/realism-intl-relations/#pagetopright
Transnational Criminology Manual. Nijmegen, Netherlands: WLP, 2010

UN. Comprehensive Study on Cybercrime. (United Nations Office on Drugs and Crime. Vienna, 2013)

United Nations, 1994. UN Manual on the Prevention and Control of Computer Related Crime.

United Nations. 2004. Convention against Corruption, Art 15

United Nations. A more secure world: Our shared responsibility, Report of the High-level Panel on Threats, Challenges and Change, 2004, p 2
United Nations. Namibia: Situation Analysis (United Nations in Namibia and Government of Namibia

Victor, D. 'Globalization and the Study of International Security', Journal of Peace Research, Vol. 37, No. 3, 2000

Wafula, P and P. Alushulu. *State Defends Plans to Snoop on Kenyans.* (The Standard, 18 February 2017)

Wall, D S. *Cybercrimes: The Transformation of Crime in the Information Age* (Cambridge: Polity, 2007).

Yar, M. Cybercrime and Society: Crime and Punishment in the Information Age (London: SAGE Publications, 2006).

Yar, M. The novelty of 'cybercrime': An assessment in light of routine activity theory. European Journal of
Criminology, 2005