UNIVERSITY OF NAIROBI

INSTITUTE OF DIPLOMACY AND INTERNATIONAL STUDIES

THE EMERGING ROLE OF CYBERSECURITY IN INTERNATIONAL PEACE: A CASE STUDY OF KENYA

WATSON KARUMA MUIRURI

R52/82685/2015)

SUPERVISOR

DR. PATRICK MALUKI

A RESEARCH PROJECT SUBMITTED IN PARTIAL FULFILMENT OF REQUIREMENT OF THE AWARD OF THE DEGREE OF MASTERS OF ARTS IN INTERNATIONAL STUDIES, UON, IDIS

NOVEMBER 2017

DECLARATION

I, Watson Karuma Muiruri hereby declare that this research project is my original work and has not been presented for a degree in any University other than this one.

Signed..... Date 14/12/17

Watson Karuma Muiruri

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

Signed..... Date 14/12/2017

Dr. Patrick Maluki

ACKNOWLEDGEMENTS

I would like to recognize the importance of my supervisor, Dr. Patrick Maluki, for his professional guidance through this entire process, thank you. I also thank my family, whose support and patience has been immense.

DEDICATION

This research project is dedicated to my father, the Late Humphrey G. M. Ngugi, who always encouraged me to fulfil my academic ambitions, and for inspiring me to never give up.

ABSTRACT

The purpose of this project is to get a better understanding of the new concept, and even threat to international peace and security, which is cybersecurity in East Africa most specifically Kenya. This study will focus on explaining what cybersecurity is and its relevance to modern international relations, most specifically; Kenya's reception or lack thereof cybersecurity.

Cybersecurity comes with it new dimensions of international relations conducted in virtual space but with serious implication in the real world e.g. intellectual property rights, cybercrime, identity theft, right to privacy, espionage as well as hacking.

Cybersecurity complicates international peace and security as it involves non-state actors e.g. multi-national corporations and even individuals such as Julian Assange of Wikileaks and American Robert Snowden.

The study look at the challenges of cybersecurity and the various ways of overcoming them especially in Kenya.

TABLE OF CONTENTS

DECLARATION i
ACKNOWLEDGEMENTS iii
DEDICATION iv
ABSTRACT v
LIST OF ABBREVIATIONS 4
CHAPTER ONE 6
1.1 Introduction 6
1.2 Background 7
1.3 STATEMENT OF THE PROBLEM 9
1.4 RESEARCH QUESTIONS 10
1.5 OBJECTIVES 11
1.5.1 Specific Objectives 11
1.6 JUSTIFICATION OF THE STUDY 11
1.7 LITERATURE REVIEW 13
1.7.1 Cybersecurity 13
1.7.2 Cybersecurity and international peace & security 17
1.7.4 Cybersecurity in Kenya 19
1.7.5 SUMMARY OF GAPS IN LITERATURE 22
1.8 THEORETICAL FRAMEWORK 23
1.8.1 Realism 23
1.8.2 Offensive Realism 24
1.8.3 Defensive Realism 26
1.9 HYPOTHESES OF THE STUDY 27
1.10 RESEARCH METHODOLOGY 28
1.10.1 Study Design 28
1.10.2 Study Site 29
1.10.3 Study Population 29
1.10.4 Sample Size 29
1.10.5 Data Collection Method 30
1.10.6 Validity and Reliability of instruments 30
1.10.7 Data Presentation and Analysis 30
1.10.8 Ethical Considerations 30

1.10.9 Scope and Limitation of the research 31
1.11 Chapter Outline 31
CHAPTER TWO 32
CYBER THREATS IN KENYA 32
2.0 Introduction 32
2.1 Background 33
2.2 Types of threat 35
2.2.1 Un-targeted attacks 36
a. Phishing 36
b. Water-holing 37
c. Ransomware 39
2.2.1 Targeted attacks 40
a. Spear-phishing 41
b. Distributed Denial of Service 42
2.3 Cases of Cyber Threats in Kenya 43
2.3.1 Early threats (2012 -2014) 44
2.3.2 Recent threats (2015 - 2017) 47
2.4 Conclusion 49
CHAPTER THREE 50
DEALING WITH CYBER THREATS AND ATTACKS IN KENYA 50
3.0 Introduction 50
3.1 Background 51
3.2 Domestic Cybersecurity policy 53
3.2.1 USA's Domestic Cybersecurity policy 55
3.3 Kenya's Cybersecurity policy 59
3.3.1 Kenya's Legal Framework of Cybersecurity 61
3.4 Conclusion 63
CHAPTER FOUR 65
CYBERSECURITY AND INTERNATIONAL PEACE 65
4.0 Introduction 65
4.1 Background 65
4.2 International Policy on Cybersecurity 69
4.2 USA's Foreign Policy on Cybersecurity 72

4.3 Kenya's Foreign Policy on Cybersecurity 74
4.4 Conclusion 75
CHAPTER FIVE 77
5.0 Introduction 77
5.1 Summary of the research 77
1. Securitization of the Cyberspace 79
a. Securitization Actor 80
b. Referent Object 81
c. Audience 81
2. Cyberspace as an emerging threat to the nation-state 82
a. Cyber Corporations 83
5.2 The Way Forward 84
Conclusion 85
APPENDICES 87
Appendix I 87
INTERVIEW GUIDE (SAMPLE) 87
Appendix II 89
QUESTIONNAIRE (SAMPLE) 89
BIBLIOGRAPHY 92
Other Resources 96

LIST OF ABBREVIATIONS

CERTs - Computer Emergency Response Teams

CFR - Council on Foreign Relations

CISPA - Cybersecurity Intelligence Sharing and Protection Act

CTSA - Cyber Threat Sharing Act

DDoS - Distributed Denial-Of-Service

DESA - Department of Economic and Social Affairs

EAC - East African Community

ECOSOC - Economic and Social Council

E-CSP - Electronic Certification Service Providers

GCA - Government Certification Authority

ICT - Information and Communication Technology

ICTA - ICT Authority

IFMIS - Integrated Financial Management Information System

ISP - Internet Service Providers

IT – Information Technology

ITU - International Telecommunication Union

KRA – Kenya Revenue Authority

M-PESA – Safaricom's Mobile – Money transfer

MS DOS - Microsoft Disk Operating System

NPKI - National Public Key Infrastructure

NSA - National Security Agency

NSA - US National Security Agency

NSCAP - National Security Cyber Assistance Program

OECD - Organisation for Economic Co-operation and Development

PCNA - Protecting Cyber Networks Act

RCA - Root Certification Authority

TESPOK - Technology Service Providers Association of Kenya

UN – United Nations

UNCITRAL - United Nations Commission on International Trade Law

UNCTAD - United Nations Conference on Trade and Development

WIPO - World Intellectual Property Organization

CHAPTER ONE

1.1 Introduction

Cyber security is a relatively new issue in international relations, and it is as enigmatic as it is complex, more so in Africa. To best understand the concept that is cyber security, one must know that it is an aspect of globalization and globalism. Keohane and Nye define globalism as the networks of interdependence across and between nation-states, where there is a flow of capital, goods, information and ideas as well as people. Globalization, they argue, is the increase of globalism.[1] This interdependence of the international realm is best exemplified by the cyber space, characterized by interconnectivity and flow of information, where free market thrives and promotion of liberal values has taken an integral place. The term cyberspace starts with the prefix 'cyber' which means electronic and computer related activities. Cyberspace can further be explained as a set of information systems that are connected together thereby allowing users, mostly human, to interact within the, and importantly, it is dependent of time.[2]

There is no one stakeholder in cyberspace but the government can provide the role of regulation and enforcement.[3] The interconnection between the end-users across the world is made possible by the internet, which is accessible via computers, televisions, and mobile phones; making it possible for a corporation to undertake daily operations from just about anywhere in the world or an army located in one part of the world to launch an attack against another located in another part of the world.

---

[1] Keohane, Robert & Nye, Joseph 1998. "Power & interdependence in the information age." Foreign Affairs; Sep/Oct 1998; Alumni - Research Library P. 81

[2] Ottis, R. & Lorents, P. (2010). "Cyberspace: Definition and Implications. In Proceedings of the 5th International Conference on Information Warfare and Security", Dayton, Ohio, US, 8-9 April. Reading: Academic Publishing Ltd.

[3] Kigen, P., C. Kisutsa, C. Muchai, K. Kimani, M. Mwangi & B. Shiyayo. 2014. "Kenya Cyber Security Report 2014: Rethinking Cyber Security – "An Integrated Approach: Processes, Intelligence and Monitoring."

1.2 Background

The International Telecommunication Union, reports that there were over 3.5 billion internet users in 2016, with over 7 billion people, which is 95% of the global population, enjoying mobile phone coverage and this has been occasioned by the drop in ICT prices globally.4 The role, then, of securing the cyberspace becomes a matter of state, and not the multinational corporations that are in it to exclusively make profits. Cybersecurity is simply the defence of all the computing hardware that include; computers, cellular devices, servers, systems, networks as well as information in the form of data, from attacks that can be described as malicious.[5] In January 2011, a major cyber-attack against the Canadian government's agencies were reported and they included attacks on a research agency for Canada's Department of National Defence also known as the Defence Research and Development Canada. This attack was so profound that it ended up seeing the Finance Department and Treasury Board, which is the country's most important economic agency, delink from the Internet to protect from further invasion and danger.[6] In October 2012, Russian cybersecurity provider Kaspersky Lab, uncovered a global cyber-attack whereby hackers had identified weaknesses in Microsoft Word and Microsoft Excel programs, and used it to steal or gather information and data. This attack, which was nicknamed 'Red October' targeted government embassies, research firms, military installations, energy providers, nuclear and other critical infrastructures in Eastern Europe, Kazakhstan, Belarus, Armenia, Estonia, among other former USSR states, Central Asia, parts of Western Europe and North America.[7]

---

[4] http://www.itu.int/en/mediacentre/Pages/2016-PR30.aspx retrieved 01/03/2017

[5] http://usa.kaspersky.com/internet-security-center/definitions/what-is-cyber-security#.VIRdSb_6_IU

[6] 'Red October' cyber-attack found by Russian researchers' www.bbc.com 14 January 2013

[7] Ibid.

According to the Norton Cybercrime report of 2012, 70% of South African internet users have been affected in one way or another, by cybercrime, with Africa's second-largest economy, Nigeria, infamous for its '411 scams', where criminals pose as wealthy account-holders who need help transferring funds.[8] The situation is so dire that reports indicate that cybercrime is increasing at a more rapid rate in Africa than in any other area in the world, for instance, South Africa, due to its internet and technological penetration is 3rd in the world behind Russia and China as far as the highest number of cybercrimes reported goes.[9] Cybercrime, in its various forms, continues to take a toll on the economies of these countries. Collectively, over $200 million was lost in 2011 in Kenya, Rwanda, Uganda, Tanzania and Zambia due to cyber-fraud targeting financial institutions. It is alleged, for instance in Zambia that some $4 million lost in 2013 through cybercrime was done so by Zambians and foreigners.[10]

In 2013, the Kenyan cyberspace recorded a growth of 108% in the number of cyber threat attacks which translates to 5.4million attacks up from 2.6 million attacks in 2012. These attacks were launched from Kenya and outside the country ranging from anonymous proxy server attacks, spamming, malware threats and even mobile fraud.11 In December 2014, 77 foreigners mostly Chinese nationals were arrested in Kenya's capital with what the police said were sophisticated telecommunication equipment. The nationals were accused of trying to hack or infiltrate M-

[8] Norton Cybercrime Report, September 2012, page 6 http://www.norton.com/2012cybercrimereport
[9] Symantec Corporation, Internet Security Threat Report 2013, 2012 Trends, Volume 18 (April, 2013). Available from www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf.

[10] Henry Quarshie and Alexander Martin-Odoom, "Fighting Cybercrime in Africa", Computer Science and Engineering, vol. 2, No. 6 (2012), PP. 98-100.
[11] Kigen, P., C. Kisutsa, C. Muchai, K. Kimani, M. Mwangi & B. Shiyayo. 2014. "Kenya Cyber Security Report 2014: Rethinking Cyber Security – "An Integrated Approach: Processes, Intelligence and Monitoring."

PESA system, cash machines and bank accounts.12 This specific case opened up a diplomatic exchange between the Chinese and Kenyan governments over the extradition of the arrested individuals with China saying Kenya was not the target of the hackers but Kenya insisting they should be tried locally.

Conflict is as old as humankind. It is in every aspect of human interaction, be it religious, economic or political. There is said to be conflict when two or more individuals or parties wish to carry out mutually inconsistent acts. These parties maybe as basic as individuals or as complex as groupings of people and states.13 The process of achieving cybersecurity can be a cause of conflict, while at the same time, achieving cybersecurity can be part and parcel of international conflict management with peace as the end goal. The United Nations acknowledges that cybersecurity is an emerging issue in international relations and therefore can, and has in counted situations, become a threat to international peace, stability and security as states seek advanced cyber-tools to either defend themselves or plan attacks on others. When the uncertainty about, which rules can be used to govern the cyberspace, and how states should approach and interact cordially in that space, then the risk of cyber-conflict increases. The United Nations Institute for Disarmament research, reported that over forty states have developed military cyber-capabilities, with 12 of the 40 doing so for offensive purposes.14

1.3 STATEMENT OF THE PROBLEM

It is evident that cybersecurity continues to be a growing concern, especially, as the world moves into a fully digitized space. The problems lie in the dynamic and fluid nature of the cyberspace

[12] "77 Chinese held in cyber bust" Daily Nation P. 4, December 3, 2014

[13] Nicholson, M. (1992) Rationality and the Analysis of International Conflict (Cambridge 12 University Press)
[14] UN Institute for Disarmament Research (UNIDIR), "The Cyber Index: International Security Trends and Realities," UNIDIR/2013/3 (2013).

which makes it open to all and its interconnectivity aspect makes it almost impossible to tether much to the chagrin of the nation-state. The cyberspace is in such a way that it is different to the traditional sphere of influence as exercised by the nation-state, in that this interconnectivity could see some computer servers in different countries making any cybersecurity issue an international concern. The quest for cybersecurity is likely to create conflict as a state deems another aggressive should a cyber-attack be launched from one to another or if a state interferes with another's cyberspace. Another way the quest for cybersecurity could threaten international peace is through cyber-attacks in the form of denial-of-service to sensitive institutions such as banks, which could directly affect a country's economy, then it is likely to lead to conflict in the international realm, as the victim of such attacks takes measures to ensure it is not attacked again. Kenya, like any other state, should be concerned with improving its cybersecurity because sensitive information falling on the wrong hands could threaten peace and lead to conflict. The cyberspace, has in recent times used by terror groups in the recruitment of supporters as well as a means of communicating to, not only, the members but also to spread terror offering a direct threat to peace and security.

1.4 RESEARCH QUESTIONS

1. What are the known and potential threats to Kenya's cybersecurity?
2. What measures are in place to deal with cyber-attacks on Kenyan systems?
3. Is Kenya making any efforts to ensure a peaceful international sphere vis-à-vis cybersecurity?

1.5 OBJECTIVES

The main aim of this study is to analyze the emerging role of cybersecurity in international peace and security.

1.5.1 Specific Objectives

1. To investigate Kenya's cyber security threats
2. To assess Kenya's policy on cybersecurity
3. To assess Kenya's foreign-policy on cybersecurity

1.6 JUSTIFICATION OF THE STUDY

This study is focusing on cybersecurity, which in itself involves the systems and relationship between systems and in this case Kenya's cyberspace and how secure it is and its relationship with other such systems locally and internationally. The Kenyan government has expressed and to some extent shown concerted interest in the utilization of the cyber-space to conduct its business in service delivery with the e-government the best example and use of IFMIS another. However, these systems have shown their susceptibility to infiltration such as IFMIS, which was used to misappropriate funds allocated to the Ministry of Planning and Devolution through the National Youth Service. The NYS deputy director then Adan Harakhe said that his IFMIS password was stolen and used to misappropriate over 600 million Kenya shillings.15 This study will then look at ways of formulating better policy, which in turn ensures there is an increased level of transparency, and improved monitoring.

This research will also seeks to find out how threats that are deemed domestic can have a domino kind of effect in international relations thereby creating conflict, which is a threat to peace. The

[15] http://www.capitalfm.co.ke/business/2015/11/e-government-tightens-noose-on-corrupt-rent-seeking-public-officials/

research is also expected to assist the Kenyan government in formulating policy on how business is conducted on the cyberspace without infringing on other states because currently there is little to no policy in most countries, and the use of international law may not necessarily be applicable in cyber-relations.

This research also seeks to provide scholarly material for academic purposes because cybersecurity is a relatively new term and have little to no information especially regarding Kenya.

1.7 LITERATURE REVIEW

Cyberspace is used interchangeably with virtual space, and to some extent virtual reality, and it is not a place with demarcated land and boundaries, but it has people who interact in this system and as such, conflict becomes inevitable; from an interpersonal level to state-state scale.[16] Cyberspace, then can be explained as a complex virtual environment brought about by the reciprocal action of people, computer software and services on the internet by the means of technological devices and networks, which are interconnected. There is no one stakeholder in cyberspace but the government can provide the role of regulation and enforcement.[17] According to the ITU, cybersecurity is no longer just about computer security but a matter of national concern and should be included in the national policy, and ultimately an international issue.[18]

1.7.1 Cybersecurity

Cybersecurity is comprised of various elements, which a state needs to focus on. First, on that list is critical infrastructure, which comprise the physical cyber-based systems whose reliability and security are key to governance and service delivery. Critical infrastructure forms the backbone of the cyberspace and it took some 25 countries for the Capstone's project by Dr. Engels to come up with a working definition. Countries, such as Finland, Korea, Russia and Brazil, are yet to out rightly come up with a clear outline of critical infrastructures. It is different in Norway, Germany, Norway, the United Kingdom and Switzerland, who have clear, detailed and specific definitions.[19] The public-private partnerships, as a way of combating cybersecurity threats exist in Switzerland, the Republic of Korea, and the UK but other countries seem to

[16] Gibson, W. (1984) *Neuromancer.* New York, Ace Books.
[17] Kigen, P., C. Kisutsa, C. Muchai, K. Kimani, M. Mwangi & B. Shiyayo. 2014. "Kenya Cyber Security Report 2014: Rethinking Cyber Security – "An Integrated Approach: Processes, Intelligence and Monitoring."
[18] http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf
[19] http://bush.tamu.edu/research/capstones/mpia/Engel_Spring2011.pdf

struggle security requirements and business efficiency is concerned.20 The critical infrastructure in the USA, for instance, dates back to 1962 when during the Cuban Missile Crisis, the National Communications System was created. It was necessitated by the 'call completion' problems where the US president then John F. Kennedy and Russian president Nikita Khruschev could not communicate adequately and could only use Radio Moscow. This was a system that laid the groundwork for establishing the current structure, which brings together various departments of government to handle a variety of issues from communicating in strategy to nuclear codes.21 In 2014, an anonymous group called 'Energetic Bear' believed to be based in Russia launched a cyberattack on the energy sector in the USA, whereby malware was used to take control of the SCADA in some companies thereby accessing and relaying sensitive data and information. A similar attack was launched in Germany, this time targeting a steel firm, where the attackers, using phishing, managed to access and gain control of various departments including the manufacturing plant, to the extent of shutting down a furnace, resulting to physical damage and losses in the process.22 Cybersecurity on critical infrastructure is so pertinent that the US government has allocated US $1.5 billion to it in 2017, and this will be used to strengthen the cyber-security of government departments as well as allow the collection and sharing of intelligence within government and across to the private sector. This comes in the run up to

[20] Ibid

[21] Critical Infrastructure Protection in Homeland Security: Defending a networked nation 2nd edition By Ted G. Lewis Published by Wiley

[22] https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/reports/critical-infrastructures-west-hemisphere.pdf

reports of hacking of the US federal government, where personal information of millions of employees was stolen, and Russia accused of interfering with the elections.23

A cyber-attack can be defined as any type of aggressive action taken by individuals or organizations targeting systems, networks, critical infrastructure, and even individually-owned and operated computer devices through malicious acts undertaken in anonymity in a bid to steal, alter, or destroy.24 Vulnerability of a cyberspace is that it can be used unfairly or adversely affected by natural hazards, accidents and even terrorism, all of which result in damage or harm to that system. Capability is defined as the volume and ability to launch an attack on a target and cause adverse effects. On the other hand, threat is defined as the purpose or aim and capability to adversely affect or cause harm or damage to the system by adversely changing its states. Risk, then, becomes the result of a threat with adverse effects to a vulnerable system.25 There are other scholars who offer more elaborate ways of dealing with software attacks in their literature. It can be argued that an integrated software security checklist involves; a software security checklist, a vulnerability matrix that categorizes vulnerabilities and exposure, a flexible modelling framework for verification of requirements, a property-based tester for testing vulnerabilities, a collection of security assessment tools.26 The Ponemon Institute, explains that

[23] https://www.scmagazineuk.com/trump-announces-15bn-for-cyber-security-and-critical-infrastructure/article/645005/

[24] Karnouskos, Stamatis. "Stuxnet worm impact on industrial cyber-physical system security." In *IECON 2011-37th Annual Conference on IEEE Industrial Electronics Society*, pp. 4490-4494. IEEE, 2011.

[25] Journal of Homeland Security and Emergency Management Volume 3, Issue 4 2006 Article 3 Cybersecurity: From Ad Hoc Patching to Lifecycle of Software Engineering Clyde G. Chittister Yacov Y. Haimes 2006 The Berkeley Electronic Press

[26] Gilliam, David P., Thomas L. Wolfe, and Josef S. Sherif, "Software Security checklist for the life cycle." Proceedings of the Twelfth IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE '03), IEEE Computer Society.

insider fraud occurs often and on average, organizations have had over 50 employee-related incidents of fraud in the past year.27

Other threats to cybersecurity include social engineering whereby victims are tricked into revealing confidential information, which could in turn be used for financial gains. Another threat is Phishing, which is short for 'password harvesting fishing' and it is a form of online identity theft where perpetrator pretends to be a financial institution, and sends emails asking for clarification of passwords and other information which is also used against the victim. SMS have also been used to phish in recent times. Spyware is another dangerous threat, which cyber criminals use to get into the victims computer without the victims' knowledge and steals information.28

Thirdly, a state endeavours towards a cyber-resilience, which is defined as the capability of an organization or government, which aids it to stand strong against negative impacts due to known, predictable, unknown, unpredictable, uncertain and unexpected threats from activities in cyberspace.29 Cyber-resilience involves the parties to do an evaluation in pre, during and post a cyber-attack or threat, and is usually carried out together with recovery making it a long-term strategy as opposed to a short-term event. Research shows that 80% of the United Kingdom's critical infrastructure is placed in private hands and in the last ten years there have been concerted efforts to make laws, which can avert the problem of resilience by creating mandatory legal obligations for service providers. This has brought about the birth of a new relationship involving intelligence, security and resilience in a complex state–private citizen partnerships.

---

[27] The Ponemon Institute, "The Risk of Insider Fraud: Second Annual Study." February 2013
[28] Shalhoub, Z.K. & Al Qasimi, S.L. Cyber Law and Cyber Security in Developing and Emerging Economies. 2010 Edward Elgar
[29] https://www.securityforum.org/news/cyber-resiliencebrand-reputation/

1.7.2 Cybersecurity and international peace & security

There is little literature linking cybersecurity to international conflict management directly but there exists literature on cybersecurity and international peace. The United Nations, in 2012 sanctioned a report on the use of ICT in international security, acknowledging the new threats to international peace where the states have powers and/or vulnerabilities as far as the cyberspace is concerned. The report, worked on by 15 experts drawn from the permanent states, together with Japan, Egypt, Germany, Argentina, Indonesia, Belarus, Canada, India, Estonia and chaired by Australia, focused on the urgent need to promote confidence-building in a bid to promote responsible behavior of States. 30 It primarily addressed how the UN can apply international law to states' behavior in the cyberspace. According to the report the lack of a universal legal framework was a sufficient breeding ground for the escalation of conflict and potential instability, in turn recommending that the principles as laid down by the UN Charter should also apply on the cyberspace, whereby states must respect territorial sovereignty and independence, reduced use of force instead using peaceful means as it happens in the 'real world'. The report recommended that states should refrain from creating cyber-weapons, which it acknowledged that the likelihood of this was increasing alarmingly, adding its creation should only be for peaceful purpose. Furthermore, the report elucidates the international conflict management mechanisms applicable in the cyberspace such states exchanging and sharing information as preventive diplomacy, use of regional organizations to improve investigative and mitigation mechanisms and increased cooperation.31

[30] UN General Assembly, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," A/68/98, June 24, 2013

[31] UN General Assembly, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," A/68/98, June 24, 2013

The UN has two distinguishable ways of approaching cybersecurity where one involves cyberwarfare; a combination of politics and military, and the other dealing with economics under cyber-crime. The Budapest Convention or the Convention on Cybercrime, is a product of such negotiations and talks, which produced the first international agreement that addresses the use of internet and computer crime. The Budapest Convention harmonizes national legal structures and promotes cooperation among nations.32 Furthermore, the ITU Secretary General is a proponent of cyber-peace, which can be defined as an attempt to make cyberwar null and void. As a matter of policy, the United States of America, blocks arms control on the cyberspace, which is fully supported by Russia, which in turn argues that it wants to develop international law in a bid to promote international peace and security.33

According to Russia, the main challenge of the International code of conduct for information security dwells on the legitimacy and applicability of international law; on how it can regulate the cases of aggressive use of ICTs for political and military ends. Under the auspices of the UN, the group of states recommended that dialogue among states on how the state uses ICT in a bid to reduce risk affecting the states collectively, and protect critical national and international infrastructures, should continue; it also recommended confidence building and measures of risk reduction, capacity building in countries that are less developed as well as finding common ground and relevant laws in the United Nations General Assembly resolution 64/25.34

According to USA, their reservations were based on the need to prevent authoritarian governments from censoring internet by legitimizing it under the UN's International code of

[32] Convention on Cybercrime, Budapest, 23 November 2001

33 Clarke, Richard A. and Robert Knake. Cyber War : The Next Threat to National Security and What To Do About It. Ecco, April 2010.

[34] Clarke, Richard A. and Robert Knake. Cyber War : The Next Threat to National Security and What To Do About It. Ecco, April 2010

conduct for information security but great leaps were made in the negotiations, which a majority of the states signed, including USA.35

The ITU, a treaty organization under the UN, was joined into the UN system as a Specialized Agency under article 57 of the UN Charter to deal with the practical aspects of cybersecurity. The ITU Secretary General submits threat assessment report every three months to the UN Secretary General, while at the same time maintaining a database of experts as a resource base in case of a cyber-attack and monitoring the Global Cybersecurity Agenda as a way of establishing an international framework for cybersecurity. The ITU seeks, with recommendations from the Global Cybersecurity Agenda, to develop model laws and legislation, which the member states can adopt under the guidance of the Budapest Convention, as well as a framework for national infrastructure protection. With this recommendations then the member states can formulate internationally harmonized laws. The ITU secretary general suggest a universal framework based on five principles to governments 'commitment; to give its citizens access to communication, to protect the citizens in the cyberspace, not to harbor cyber-terrorists or cyber-criminals in their territory, not to launch cyber-attacks against other states, and to work together under a framework that ensures peace in the cyberspace.[36]

1.7.4 Cybersecurity in Kenya

Kenya, just like most of the world, is steadily moving towards keeping up to date with the changing digital trends which in turn have come with their own cyber threats. Kenya lags behind in as far as scholars and experts seek to research and provide academic work towards

35 Nye Jr, Joseph S. —Cyberpower. Paper. Cambridge, Mass.: Harvard Belfer Center for Science and International Affairs, May 2010.

[36]Wegener, Henning. —Cyber Peacel, in The Quest for Cyber Peace. International Telecommunication Union and World Federation of Scientists, January 2011.

cybersecurity. In a bid to totally understand the concept of cybersecurity, we need to examine the various facets as well as numerous expert views of achieving cyber resilience. In this literature review, the study will examine literature on cyber-security assessments as well as specific studies and methods for analysing interconnectedness between sectors.

Kenya has made concerted efforts to identify while at the same time define Critical Infrastructure by presenting bills to parliament. The Critical Infrastructure Protection Bill set to be discussed in the national assembly before undergoing the law making process holds the proposals. The bill brings together five ministries dealing with crucial services, and they include ICT, Housing, Water, Transport and Energy, ministries. The bill advocates for the collective setting up, maintenance and protection of critical infrastructure under these ministries, which is at the moment done in an independent and uncoordinated way, which leads to essential service delivery being disrupted and losses incurred due to accidental damage. Furthermore, the bill seeks to ensure that this unit will work with the Inspector General of police to ensure security, improve cyber-surveillance and enhance protection against potential threats or other related terror activities.37 The bill further outlines the roles and responsibilities of the Critical Infrastructure Unit, which includes among others; to co-ordinate the planning, design, implementation and deployment of Critical Infrastructure in Kenya, to keep a register of the assets, to educate the public, to take necessary security measures for the assets' safety, and to take up a requisite insurance cover to protect the assets from any damage.38

[37] https://www.standardmedia.co.ke/mobile/?articleID=2000174969&story_title=state-to-set-up-unit-to-protect-critical-infrastructure By Paul Wafula | Wednesday, Sep 2nd 2015
[38] The critical infrastructure protection bill, 2015

In March 2017, reports in the media revealed that over 30 billion shillings was lost from the KRA through a syndicate of hackers both Kenyan and foreign.39 According to the reports, the hackers installed malware into the KRA systems where the accessed the servers and even stole the billions of shillings not only from KRA but also from banks and a supermarket. The reports further alleged that the syndicate was also involved in interference of the 2013 general elections whereby the electronic conveyance and collation of results was shutdown forcing the electoral body IEBC to resort to manual counting.40 Another example, KRA uses the Simba system, which allows a single point entry in custom clearance and declaration to payment. It was launched in 2005 to replace the Orbus system, because it is faster when it comes to clearing and it eliminates corruption, however the KRA employees are reported to disable it so that they can revert to the manual system, allowing tax evasion, and clearance of contraband. Even the ITMS which eases the filing of taxes with KRA has been a target.[41]

Early 2017, Kenya was among the countries that were attacked by the WannaCry virus, which affected over 300,000 users globally with warning that it could get worse. The ICT Cabinet Secretary Joe Mucheru confirmed this, warning that the threat of what he called cybercrime, is real, while at the same time the Communications Authority of Kenya warning Kenyans and explaining how the malware works.[42] An IT security report done by the Kenya National Bureau of Standards and CA and released in April 2017 indicated that

[39] https://www.standardmedia.co.ke/m/article/2001232241/how-kenyan-banks-lost-sh30-billion-in-two-years-to-tech-savvy-criminals

[40] http://www.nation.co.ke/news/Police-bust-ring-of-hackers/1056-3842558-11h7q5xz/

[41] Marete, G. (2011, June 5). Aeromarine. Retrieved March 18, 2017, from http://www.aeromarine.co.ke

[42] http://www.businessdailyafrica.com/corporate/Kenyan-firms-hit-by-ransomware-cyber-attack/539550-3928322-uwqsnq/ Retrieved on 17/05/2017

1.7.5 SUMMARY OF GAPS IN LITERATURE

The concept of cybersecurity maybe new to Kenya, which may explain the lack of sufficient literature to explain, and even, offer ways of strengthening against the new threat to international peace. However, the literature available is mostly from the developed states most specifically the United Stated of America, which is considered a frontrunner in cybersecurity. USA's experience in cybersecurity gives an opportunity to Kenyan scholars to learn from the available literature while at the same time discerning what is relevant to Kenyan needs and threats.

Former CEO of Google and currently chairman, Eric Schmidt points out succinctly that, "The Internet is the first thing that humanity has built that humanity doesn't understand, the largest experiment in anarchy that we have ever had".[43] Schmidt's argument aims at explaining how complex the cyberspace is, while at the same time predicting doom via anarchy. Many scholars are of the same argument in that they have almost always resigned the world's fate to the complex and ever-changing dynamics of the cyberspace. Nonetheless, it is important to note that, while the inter-webs are in indeed complex and dynamic, the threats or the reasons towards any form attack are almost static. Few scholars have argued along the lines of the reasons behind cyber-insecurity as a way of dealing with the threats to international peace and security as posed in the cyberspace. In understanding the motive of cyber criminals then can then provide an avenue to prevent future attacks and establish improved cyber-resilience. This study will attempt to bridge these gaps, with the aim of providing sufficient ways of dealing with the various threats to cybersecurity.

[43] http://www.business-standard.com/article/companies/4-ways-to-address-the-net-neutrality-issue-115071600492_1.html Mansi Taneja | New Delhi July 16, 2015

1.8 THEORETICAL FRAMEWORK

The issue of cybersecurity is more state-centric as many scholars argue with the threats to state security coming from non-state actors, which is different to the traditional international relations as we know it. The state in the cyber-age is faced with new challenges but its end remains the same as argued by realists. The different variants of realism; Offensive and Defensive, can best explain cybersecurity.

1.8.1 Realism

Realists focus their arguments on power, which they believe is the medium of exchange used in international politics. The world's super powers, such as the USA, pay close attention on how much economic and military power they have as compared others. Realism draws an international system highlighted competition, fear and conflict. Under this argument, realists do not recognize one authority, and view states as the core actors in the international system. Realism further argues that states are driven toward their own national interests, with their survival being the ultimate one.[44]

According to the principles of Realism as written by Hans Morgenthau, there is the tension between morality and political actions' requirements and it is here that assuring cybersecurity in Kenya comes to sharp focus. There is the moral issue of privacy among internet users getting privacy and the government listening in on phone calls and accessing information from its citizens. Realists in this case would argue that the state interests supersedes all else, sometimes even those of its own citizens. The realists can them argue that the presence and dominance of the individual in the cyber space is a direct threat to national security and thus deem this as a

---

[44] Freyberg-Inan, Annette What Moves Man: The Realist Theory of International Relations and Its Judgment of Human Nature, SUNY Press, 2004

weakening of state power. It is imperative to comprehend that according to realists the state seeks power and calculates its interests in terms of power.[45]

In as far as the issue of cybersecurity and the state, realists would argue that the international state is responsible for the conduct of the state on the international scene and not individuals behind computers and mouse clicks. What the cyberspace brings to international relations is a new height of uncertainty which some realists argue is another reason states go to war. In the cyber-age USA, Russia and China have often times accused each other of cyber-espionage and this can be a breeding ground for uncertainty and ultimately armed conflict.[46] Realists are not devoid some optimism as far as peace and cooperation in the international system is concerned. For classical realists, power is an end in itself; for structural realists, power is a means to an end and the ultimate end is survival. But in order to get a clear understanding of this side of the realists putting in mind all the suspicion among states in relation cooperating for peace and security scholars have come up with a distinction of realism; Offensive Realism and Defensive Realism – all with the national interests as a priority to taking any action in the international system.

1.8.2 Offensive Realism

John Mearsheimer is one of the leading offensive realists who argue that it is good strategic sense for states to gain as much power as possible and, if the circumstances are right, to pursue hegemony. Mearsheimer, further argues that states should always be looking for opportunities to gain more power and should do so whenever it seems feasible. States should maximize power,

---

[45] Keohane R.O. and Nye, J.S. Power and Interdependence 3rd ed. Longman Classics 1977

[46] Herz, J.H., Political Realism and Political Idealism: A Study in Theories and Realities (Chicago:University of Chicago Press, 1951)

and their ultimate goal should be hegemony, because that is the best way to guarantee survival.[47] In relation to cybersecurity, and according to the offensive realists' arguments, then the state should seek to collect as much information as it can whether from other states as does the USA via the *Wikileaks* or from its citizens, again as USA was accused in the *Wikileaks*. The state, according to offensive realists, should know what its real or perceived enemies are up to and ensure the information collected makes it powerful such as the collection of information through a centralized governments' record system which tracks down citizen's economic activities and to some extent the socio-cultural activities.

Offensive realists understand that threatened states usually balance against dangerous foes, but they maintain that balancing is often inefficient, especially when it comes to forming balancing coalitions, and that this inefficiency provides opportunities for a clever aggressor to take advantage of its adversaries.[48] Offensive realism, depicts an international system characterized by unending conflict and strife. Fear and uncertainty will rationally drive states to maximize their relative power, with the ultimate goal being the attainment of regional hegemony.[49] It is this argument, then that would lead states to accumulate military power to outdo their perceived or real enemies and collection of information via the cyberspace offer that avenue as the international system expands in that sphere where information is the currency. On this, the offensive Realists argue that in order for a state to maximize its power, it must improve its military advantage over others. The result is a constant race to develop both offensive and

[47] John J. Mearsheimer: An Offensive Realist Between Geopolitics & Power, Institut for Statskundskab, Københavns Universitet, 2003
[48] Ibid.
[49] John Mearsheimer, "The False Promise of International Institutions," International Security, Vol. 19, No. 3 (Winter 1994-1995), p. 10.

defensive military capabilities. Unsurprisingly, this structure leaves little opportunity or hope for cooperation between states.[50]

1.8.3 Defensive Realism

Defensive realists led by the likes of Kenneth Waltz argue against states attempts to maximize their measure of world power, because the international system has a way of punishing them should they endeavour towards gaining too much power. These scholars point out that the international system offers strong impulses to accrue more increments of power, while at the same time maintaining that it is imprudent to pursue hegemony; and they describe this as the worst form of overexpansion. They further argue that states, should not maximize power, but should instead strive for an 'appropriate amount of power', a level of restraint that is critical to survival in the international system. These class of realists add that balancing will inevitably occurs should any state become too powerful, whereby other super powers will enhance their military capabilities and unite into a balancing alliance that will leave the aspiring hegemon at least less secure, and maybe even destroy it. [51] Most of the advanced nations in cybersecurity have seen the reason behind cooperating to defend themselves against the threats such as Australian police arresting a cyber-criminal for his activities affecting the USA and Britain or Sweden and Norway shutting down *Piratebay* servers which carry free content and allow free downloads from companies belonging to their allies.

---

[50] [50] John Mearsheimer, "The False Promise of International Institutions," International Security, Vol. 19, No. 3 (Winter 1994-1995), p. 10

[51] Waltz, Kenneth. 1979. Theory of International Relations. New York: Random House.

Realists under this category, also argue that, even when victory is in the offing, it does not pay: the costs are more than the benefits whereby nationalism makes it is especially difficult, and sometimes impossible, for the vanquisher to subdue the defeated.[52]

As applied in this study, realism holds that the state should be the center of focus as far as cybersecurity is concerned because the individual involved in the cyberspace belong to specific states and these particular states are powerful and the citizens are answerable to them. In as much there is freedom in the cyberspace, the state's interests are paramount and any threat, perceived or real should be dealt with by the state. This theory will further augment the reason for this study which seeks to empower the state/government in dealing with the threats to cybersecurity and ultimately ensuring international peace and security. The theory offers a solution in obtaining cybersecurity, which involves a carefully crafted out balance to ensure the state/government pursues its interests by collecting information but also ensuring that this pursuit of hegemony is not deemed as suspicious such that in its pursuit it also cooperates with others in a bid to protect its interests and preventing conflict with other states.

1.9 HYPOTHESES OF THE STUDY

1. State's quest for cybersecurity increases the likelihood of an insecure international system.
2. States can use a secure cyber space as a tool in international conflict management.

[52] Ibid.

1.10 RESEARCH METHODOLOGY

1.10.1 Study Design

This research will approach a government office where sensitive but not necessarily secret information is likely to flow from one department to another. In this office the researcher will seek access to the staff from all departments – Finance, IT, security, janitorial services, and Human Resource. The investigators will interact with the government staff to observe how they relate in the cyberspace. The investigators will look at what websites, computer applications and programs the staff use and for what reason. The investigators will ask the participants to declare their levels of competence and skill as far as the use of computers is concerned.

In addition to this the investigators ask the IT department to explain what security measures are taken to ensure airtight connection to the information collected. The investigators will further ask the participants to account for the number of machines; computers, laptops and mobile phones connected to the networks and how the departmental passwords work.

1.10.2 Study Site

This study site is Nairobi, which is the capital city of Nairobi and the center of governance for Kenya. Nairobi holds the central government offices and private companies.

1.10.3 Study Population

This study will focus on staff in a government office employed by the central government, county governments and the corporate sector. The study will also focus on the banking and finance sector, to investigate the threats and measures taken to mitigate cyber-attacks. The study will also focus on the general public, who are the users and/or beneficiaries of e-government in Kenya.

1.10.4 Sample Size

The researcher will select 50 respondents from at least two departments in the central government, a further 50 from the county governments and 50 more from the private sector. The general public, which is also part of this study, will be sampled as exemplified below;

POPULATION	SIZE
Ministry of Foreign Affairs	50
Public	50
Media	50
Corporate	50

1.10.5 Data Collection Method

This research will utilize interviews and questionnaires to collect the much-needed data from the government offices as well as the private sector. The questionnaires will ensure a sense of privacy of information, whereas the interviews will promote openness.

1.10.6 Validity and Reliability of instruments

There are quite a number of private organizations which have invested heavily in ensuring their cyberspaces are well protected and secure and the respondents from the private sector, where such measures have been taken will be the control sample. States where cybersecurity have previously been a threat such as the USA or Britain or Germany can also provide control sample. Using these as the control, the researcher will collect and collate the data from the citizens and the government and contrast for the findings.

1.10.7 Data Presentation and Analysis

For the quantitative data analysis, the researcher will use two software programs ATLAS.ti and SPSS. For the qualitative data analysis, the researcher will identify the main themes which include patriotism and cybersecurity awareness and assign code X and Y, respectively to them. After that the researcher will classify the results from the questionnaires and interviews to the codes before integrating this into a table for further analysis.

1.10.8 Ethical Considerations

The researcher will seek permission to access the information required for this study. However, this will be limited to declassified information, which is accessible to a few people but not the general public and for this the researcher is ready to sign a contract of non-disclosure, approved by the security agencies. More so, the researcher will seek a research permit from National Commission for Science, Technology and Innovation.

1.10.9 Scope and Limitation of the research

This research pertains information that some departments maybe unwilling to divulge and this may limit my study during the collection of data and publishing of the report.

1.11 Chapter Outline

The first chapter is a proposal on how to do this particular research, and it started with introducing and giving a background of what the study will focus on. The chapter also deals with a review of the literature and the gaps in the literature before explaining the content of the study through the lenses of realists. The chapter also explains how the research will be carried out, from data collection and collation before reporting on the same. Chapter two will be an investigation of the link between cybersecurity and international conflict management. In chapter three, the researcher will investigate Kenya's cyber threats whereas chapter four will be an assessment of how Kenya uses the cyber space to resolve conflict and if that is possible.

CHAPTER TWO

CYBER THREATS IN KENYA

2.0 Introduction

A cyber threat can be defined as any malicious act that attempts to gain ingress to a computer or a network or information system without permission from the owners. These malicious acts are offensive in nature and may usually involves stealing, altering or destroying of information.[53] A broader definition of a cyber threat explains it as any situation or event that is likely to adversely impact operations at an organization be it the mission, normal function, image, or even the reputation, as well the organization's assets, or individuals. It further explains that this can be done via modification of information, unauthorized access, disclosure, denial of service and destruction. The definition also includes the likelihood or potential for a source of the threat to exploit a particular information system vulnerability, doing so successfully.[54] These threats can be classified either as natural e.g. when cyber infrastructure is damaged by a thunderstorm, or manmade where this paper will focus on. Manmade threats can further be categorized either as accidental whereby human error, software and/or hardware faults are occasioned, or intentional; done by an outsider or an insider. Microsoft uses a different approach to classifying threat; spoofing is whereby an individual user pretends to be a different user by falsifying data to gain illegitimate access

[53] Lewis, James. (2002). Center for Strategic and International Studies. Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats. Washington, D.C. USA.
[54] http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf Retrieved 28/06/2017

and advantage to the other's program and/or network, rejection from a system, tinkering, leaking or releasing private information, denial of service and elevation of privacy.[55]

2.1 Background

Cyber threats are as old as the computer itself. In the early 19th century Charles Babbage created was is believed to the 1st mechanized computer and is considered the father of the computer.[56] It is this technology many years later that the modern electronic digital computer is founded on, which John Vincent Atanasoff is credited with for his work in the 1930's. The earliest computer networks were used by the military in the 1950s both in the USA and Soviet Union before a commercial airline reservation system was created in the 1960s, and then the internet protocol was created in 1972 after which computer technologists worked on increasing the internet speeds.[57]

The connectivity and improved speeds meant that the computers and the computer systems and networks were susceptible to attacks and access without permission. The first attack on computers was done by a virus called Brain in 1986, which was written by two Pakistani brothers, Basit and Amjad Farooq Alvi. This computer virus affected the boot sector of media formatted under MS-DOS and it needed the replacement of the boot sector with a copy of the virus. The brothers insisted that their intentions were not malicious despite their actions affecting hundreds of computers in the UK and USA; adding that they had written the sector in a bid to protect their medical software from being stolen.[58]

---

[55] https://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx Retrieved 28/06/2017

[56] *Halacy, Daniel Stephen (1970). Charles Babbage, Father of the Computer. Crowell-Collier Press.*

[57] *Mollenhoff, Clark R. (1988). Atanasoff: Forgotten Father of the Computer. Ames, Iowa: Iowa State University Press*

[58] *Avoine, Gildas; Pascal Junod; Philippe Oechslin (2007). Computer system security: basic concepts and solved exercises. EFPL Press. Pp. 20.*

The second attack on a network was the Morris Worm in 1988, which Robert Tappan Morris, a university student, was behind. The Morris Worm spread via the internet was several dozen lines of code that replicated immensely and spread to hundreds of computers forcing them to crash. Citing the US Computer Fraud and Abuse Act, Morris was convicted making the act, arguably, the first piece of legislation regarding cybersecurity.[59] In the 1990s internet became popularized and then commercialized when a browser Mosaic, was invented; meaning that people could browse the World Wide Web where the users would transfer files as well as read text in line with images. The browser was followed by the creation of drawing and animation tools, which revolutionized the browsers, while at the same time opening up computers to the threat of hackers who could use the tools such as Macromedia Flash to remotely take control of computers via the internet due to the add-ons which posed serious security shortcomings. The Melissa and ILOVEYOU viruses are examples of viruses that infected millions of computers worldwide, where email systems failed, but the people behind them are said to have little to no strategic mission or financial motivation. However, the advent and spread of these threats brought about the development of antivirus technology in bid to identify the viruses before they became a threat, while at the same time informing computer users, both corporate and personal, of the risks they can expect in the cyber world.[60] The early 2000s saw the birth of even more powerful cybersecurity challenges as Distributed Denial of Service attacks entered the fray. DDoS attacks simply knocks out websites rendering them offline by directing as much traffic, mixed with worms, as possible to a computer or server thereby overwhelming the entire system; sometimes done by

[59] *Dressler, J. (2007). "United States v. Morris". Cases and Materials on Criminal Law. St. Paul, MN: Thomson/West.*
[60] *Clark, Jim (1999). Netscape Time. St. Martin's Press.*

individuals seeking vulnerabilities that can be exploited and it is these earliest attacks that form the basis of modern day security technology in a bid to prevent data theft and destruction.[61]

Importantly, in 2003 the amount of data created then, surpassed all the information created in the entire human history meaning that the internet was growing at a very fast rate, gradually becoming the centre of commerce, trade and culture globally, while at the same time the devices that could access internet continued to grow, providing more access points to potential attacks. Such devices included mobile phones and the Apple iPhone's arrival in 2007 opened up the smartphone arena as Google's Android operating system was introduced in the market heralding a period of snooping and spying. In 2010, the US department of defence commissioned a report on cyber-security to better understand the concept, however the team of computer scientists under the name JASON reported that the cyberspace is very complex to the extent that it exceeds human understanding and that it is very unpredictable.[62]

2.2 Types of threat

An important feature in understanding cyber threats is that they transform on daily basis as attackers attempt to be a step ahead and users progressively seek to protect themselves from such attacks i.e. the more the sophisticated cyber security systems endeavour to be, the more sophisticated the attacks become. In this paper, the threats will be classified into broad categories; un-targeted attacks and targeted attacks.

---

[61] *Lee, Newton (2013). Counterterrorism and Cybersecurity: Total Information Awareness. Springer.*
[62] *Grossman, Elaine (2009). "JASON Panel Offers Secret Nuclear Warhead Upkeep Recommendations". Global Security Newswire.*

2.2.1 Un-targeted attacks

Untargeted attacks are first, intentional, and secondly, indiscriminate in nature in that they are directed at any and/or every user and/or device. The attackers' hope is that the would-be victims are vulnerable in one way or the other and in doing so, causing damage to the users devices and systems. This form of attack is the most common and widespread and they are intended to cause damage without being directed to a particular user. The main examples of these untargeted attacks include; worms, viruses, and malware, which are transmitted through the internet either through emails or advertisements. According to CNN, in 2014 over 300 million new forms of malware were created and transmitted across the cyberspace and here are some of the most common:-[63]

a. Phishing

Phishing can be defined as trying to obtain delicate and private date which can include; credit card details and passwords for malicious reasons such as stealing money or information and the attackers do so by pretending to be a trustworthy user.[64] Another definition of phishing is an online con game where phishers steal identities by using fake websites and spam mail to coerce users into divulging sensitive information, which the phishers then use to defraud the users or sell the private information on the black market for profit. Phishers usually send spam email to millions of unsuspecting users claiming to be a trusted and well-known organization, often including logos and company name. The Phishers use business language

[63] https://www.ncsc.gov.uk/content/files/protected_files/guidance_files/common_cyber_attacks_2016.pdf Retrieved on 03/07/2017

[64] *Ramzan, Zulfikar (2010). "Phishing attacks and countermeasures". In Stamp, Mark & Stavroulakis, Peter. Handbook of Information and Communication Security. Springer.*

to create a false crisis in order to get the information they need from the unsuspecting users and they do so by directing the user to a face website, which they use to retrieve the sensitive information.[65]

In 2003, eBay customers were sent emails that their accounts had been compromised and that the company was closing them down to ensure safety of both the customers and the company. The email was a perfect copy of the company's style of correspondence, from the company colors, font, logo and even language. However, the email included a hyperlink, which was disguised as the actual eBay web page and it is where the customers were instructed to give afresh their details, which included name, address, credit card data, social security numbers, date of birth and even next of kin's details. The unsuspecting and concerned customers rushed to send out the details to the phishers. This a classic example of phishing and the US Federal Trade Commission reported that in 2003, over 9 million Americans had fallen victim to identity theft through phishing and this had seen over 48 billion dollars lost by businesses and financial institutions with customers losing about 5 million dollars.[66]

b. Water-holing

Water-holing describes what happens in the animal kingdom, whereby the hunting animals go to the watering hole or water source such as a river, to hunt prey. In cybersecurity studies, the analogy is drawn in that the attacker plants malware in an organization, group or region's most accessed website in a bid to profile the users before testing the website's vulnerabilities

[65] https://us.norton.com/cybercrime-phishing retrieved on 03/07/2017
[66] http://www.computerworld.com/article/2575156/security0/phishing.html retrieved on 03/07/2017

in order to access sensitive information from the users.[67] Furthermore, water-holing can be defined as a fortuitous or calculated affront on sanctioned, websites that are linked either geographically or topically, that an attacker believes users of a targeted organization or government will visit. This type of un-targeted cyber-attack makes it hard for the attackers to be discovered and is commonly used in large scale against financial institutions, government and defence agencies.[68]

In 2009, there were water-holing attacks on Google, Yahoo, Juniper Networks, Morgan Stanley, Symantec, Rackspace and Adobe Systems, which were christened Aurora and is reported to have links to the People's Liberation Army based out of Beijing, China. The Aurora attacks were designed by the attackers to retrieve valuable information and files from the compromised machines by planting malware which took command and control.[69] In December 2012, the website of the Council on Foreign Relations was attacked probably because it is a foreign policy and foreign affairs resource-rich think-tank used by educationists, business people, government officials and journalists. The attackers penetrated the CFR's website server in New York and used the infected computer system to launch attacks on CFR members and others who visited the site. The attack saw malicious content being hosted on the website using a computer program, Adobe Flash to launch the attack against the 8.0 version of Internet Explorer, which was vulnerable. According to various security experts some of who investigated the attack, it is believed that the attack was

[67] *Haaster, Jelle Van; Gevers, Rickey; Sprengers, Martijn (2016). Cyber Guerilla. Syngress. Pp. 57.*
[68] https://threatpost.com/large-scale-water-holing-attack-campaigns-hitting-key-targets-092512/77045/ Retrieved on 03/07/2017
[69] https://threatpost.com/inside-aurora-google-attack-malware-011910/73395/ Retrieved on 03/07/2017

launched by Chinese hackers and immediately the Federal Bureau of Investigations were alerted in order to carry out investigations.[70]

c. Ransomware

Ransomware is the use of malicious code and software by cybercriminals to launch an attack that involves the inaccessibility of the device. The difference between ransomware and other attacks is that the attackers give instructions on how to unlock the device after a fee has been paid, thus the name ransomware. The motive is purely monetary usually paid in a virtual currency such as bitcoin for anonymity and should the individual user fail to pay the ransom in time, some of these malware have a 'time-bomb', which eventually destroys the files. The attackers may lock the screen or a more sophisticated method would involve the encryption of the users' files rendering them inaccessible.[71] The attack is launched using a legitimate file probably such as a removable disks e.g. hard drives and USB drives, pop-up, or an email and once downloaded, infects the computer system rendering it useless; the malware may come with the instructions or the attacker can remotely start sending messages to the individual. The Cryptolocker is one such example of the ransomware, which targets close to 100 file extensions, including .doc, .img, .av, .src, .cad on not only home computers but also financial bodies, government agencies, academic institutions and health institutions.[72]

Reveton is one example of ransomware, which has attacked computers across the United States of America and it involves a Trojan installing itself on a vulnerable user's computer making it freeze before a message claiming to be from the Federal Bureau of Investigations

[70] http://freebeacon.com/national-security/chinese-hackers-suspected-in-cyber-attack-on-council-on-foreign-relations/ Retrieved on 03/07/2017

[71] *Young, A.; M. Yung (1996). Cryptovirology: extortion-based security threats and countermeasures. IEEE Symposium on Security and Privacy. pp. 129–140*

[72] *Jack Schofield (2016). "How can I remove a ransomware infection?". The Guardian.* Retrieved 28 June 2017

popping up on the screen accusing the user of breaching the law and in order to unlock the device, one has to pay a fine.[73]

Another example of ransomware is those attacking cellular phones and is called mobile ransomware, which include Fusob, Svpeng, Pletor and Small. Fusob is most common and can be traced back to April 2015, which coincides with the huge and growing demand for mobile telephony. In Europe, Fusob usually detects the language the mobile user communicates in and targets those that do not use post-Soviet languages; using a website or application and locks it demanding about 200 dollars. Small, on the other hand, avoids Russia, Kazakhstan and Ukraine but works in a similar way as Fusob drawing a conclusion that they are country specific.[74] There is another version of Fusob, which targets English-speaking countries in USA and UK using a pornographic video clip and once a mobile user clicks on it for the player, downloads the malware, which takes over the mobile device and in turn demanding about 200 dollars for the release. It also comes with a timer, which ensures the victim sends the ransom faster, failure to which data is destroyed.[75]

2.2.1 Targeted attacks

Targeted attacks are more intent and focused on a specific victim for specific interests be it business or government, making it more damaging than un-targeted attacks. The attackers perform their due diligence, seeking out vulnerabilities on how and when best to launch the

[73] https://www.f-secure.com/v-descs/trojan_w32_reveton.shtml Retrieved 28 June 2017
[74] https://blog.kaspersky.com/mobile-ransomware-2016/12491/ Retrieved on 04/07/2017
[75] *"Mobile ransomware use jumps, blocking access to phones". PCWorld. IDG Consumer & SMB. Retrieved 04/07/2017*

attack with the mission to either destroy data and software or steal information to gain an upper hand on the victim or cyber-espionage. Targeted attacks may include the following:

a. Spear-phishing

Spear phishing is a more direct and targeted form of phishing whereby a vulnerable user is presented with an email that perceived to be from an individual or business one is familiar with but once clicked, attackers gain access to the computer and files seeking financial information, passwords, account numbers and other personal and private details.. It is classified as a targeted attack because the attacker appears or actually knows the users name, and email address and often send very personalized messages to the vulnerable user. A user is likely to become a target because of the information he or she puts in the internet e.g. in the social network, where the attacker can easily access the personal information, including the friends list, where one can gain access to personal information. On a larger scale an attacker can easily target an employee of a financial organization, government agency or business via an email, which when opened within the network allows the phisher to easily gain access. Government sponsored hackers or hacktivists usually use this form of attack to either take control of websites, access classified information, destroy data, seek financial gain or espionage.[76]

In 2011, RSA Security was a target of spear-phishing which started with an email sent to four employees of the firm with an attachment claiming to be a recruitment plan and once

[76] https://us.norton.com/spear-phishing-scam-not-sport/article Retrieved on 04/07/2017

one of the workers clicked the hackers gained back-end access to the network by exploiting a vulnerability on Adobe Flash. The cyber criminals stole information security products.[77]

b. Distributed Denial of Service

A Distributed Denial of Service or DDoS attacks is a variant of a Denial of Service attack whereby a lot of attacking computers overwhelm a target by creating bogus traffic. DDoS attacks are performed by botnets, which direct millions of infected computers to participate in the attack unwittingly. A botnet, which is derived from 'robot' and 'network', can be defined as a number of devices connected via the internet where each is running one or more web robots.[78] DDoS are unique and special in the sense that attacker can launch a large-scale mission because of using numerous computers, which become the attackers' slaves, a feature that also makes such attacks hard to detect because it is near impossible to locate the attacking computer amongst the millions of machines used in the attack, which could be scattered across the globe. The use of many computers also makes the attack hard to be detected because the traffic is recognized as legitimate, hence cannot be rejected by the target computer. More so, once the attack is initiated, it becomes very hard to shut it down because this would require shutting down all the machines under the control of the attacking machine. DDoS attacks usually target financial or public organizations for political, personal reasons or extortion reasons in a bid to stop the attack, which, should they continue would result to loss of time, productivity and money.[79]

DDoS attacks have become very common in the 2000s with a cyber group called Anonymous becoming synonymous with this method of cyber-attack. In 2012, Anonymous

[77] https://www.wired.com/2015/04/hacker-lexicon-spear-phishing/ Retrieved on 04/07/2017
[78] https://usa.kaspersky.com/resource-center/threats/botnet-attacks Retrieved on 04/07/2017
[79] https://www.paloaltonetworks.com/cyberpedia/what-is-a-ddos-attack Retrieved on 04/07/2017

built its own botnet by calling upon users who were against the American governments fight against online piracy, to offer their computers to launch a DDoS attack. Once the botnet was up and running, Anonymous disabled a number of US government websites among them the Justice Department, the FBI, the White House, as well as American enterprises such as the Motion Picture Association of America, the Recording Industry Association of America, Universal Music Group, and Broadcast Music, Inc. DDoS attacks have been used in cyber warfare such as was the case in 2008 in the South Ossetia war, whereby the government of Georgia websites were allegedly disabled by cyber criminals based out of Russia but were hired by the Russian security services. These attack preceded Russia military attacks in Georgia.[80]

2.3 Cases of Cyber Threats in Kenya

The Kenyan Government continues to ensure that most if not all of its sectors are up to date in terms of technological advancements, which has been outlined clearly in the Vision 2030 strategy to economic growth, whereby it is classified one of eight enablers of achieving the goals.[81] In this regard, cyber criminals are full aware how important the use of the cyberspace is to Kenya and are likely to use it against the Kenyan government and its various sectors for either political reasons or simply extortion. Cyber security in Kenya continues to grow in leaps and bounds citing the rapid growth in sophistication by the cyber criminals who in 2012 were more opportunistic and applied un-targeted attacks but within four years became more skilled, focused and targeted – attacking financial institutions and even government agencies. Indeed, Kenya falls 4th in Africa in terms of the number of cybercrime cases

[80] https://www.paloaltonetworks.com/cyberpedia/what-is-a-ddos-attack Retrieved on 04/07/2017

[81] http://www.vision2030.go.ke/enablers-macros/ retrieved 05/07/2017

reported; behind Algeria, Egypt and South Africa, which can mostly be attributed to the rise of number of people connected or using the internet, which is slightly above 20 million, attracting both domestic and international cyber criminals. The Technology Service Providers Association of *Kenya* or *TESPOK*, says that most of the attacks launched from outside Kenya more often have come from China, United States, Korea, Brazil and South Africa.[82]

2.3.1 Early threats (2012 -2014)

This period had a number of threats top among them insider threats whereby current employees of organizations, business and government use their user rights for unauthorised access to the systems, either for personal gain or for sale. According to the cybersecurity report of 2014, the number of botnet attacks increased from 900,000 in 2012 to 1,800,000 in 2013 marking a by 100% increase, and this was attributed to the faster internet speeds in Kenya and the rapid growth in internet use in the country. Another threat was in the form of theft of Internet Telephony, which grew by 73% to 780,000 attacks up from 450,000 attacks in 2012 as Kenyan organizations reported that they had been hacked and that their internet systems were used to make long distance calls, which were costly in the long run due to the huge internet bills incurred. Similarly, malicious activity on the internet in Kenya grew which was shared amongst spamming, malware and botnets.

In 2012, 103 government websites were hacked and disabled by a hacker based in Indonesia under the name Direxer, who is believed to have been part of a cyber-crime group called the Forum Group, where Direxer was given the tutorials on how to launch the attack. Some of

[82] http://www.serianu.com/downloads/KenyaCyberSecurityReport2016.pdf retrieved 05/07/2017

the websites attacked included; the administration police, business license, immigration, housing, industrialization, IFMIS, public health, Nakuru County and treasury among others.[83] The attack is believed to have been opportunistic and untargeted and similar attacks followed in 2013 and 2014 to include political messages such the one on the ministry of transport in 2014, where the attackers said that it was a cyberwar for Muslims. However, more targeted attacks became more prevalent such as one in July 2014, where the Kenya Defence Forces twitter account was hacked and misleading messages tweeted in regards to Kenya's military presence in Somalia.[84]

There were targeted attacks, as well, during this period such as the attack on the 29th of July 2013, whereby a DDoS attack on a Kenyan Internet Service Provider saw an increased data rate that reached 1629 mbps, which ultimately slowed down the internet speeds for about 8 minutes thereby denying its customers access to the internet during the time.[85]

Cyber terrorism also came to the fore during this period especially as the Kenyan military occupied the war torn Somalia in the fight against the terror group Al Shabaab. In this period, there were violent and physical attacks on Kenya, which Al Shabaab took responsibility for and used the social media to do so, as well as hacking Kenyan government websites to pass their messages. Al Shabaab used a twitter handle @ HSMPress to claim responsibility and spread their messages across the world despite internet being banned in Somalia, meaning they were using internet from a different country, and this was credited to its growing base as it recruited via social media. Cyber terrorism also prospered during this time as Kenyan

[83] http://www.cio.co.ke/news/main-stories/103-Government-of-Kenya-websites-hacked-overnight Retrieved 05/07/2017
[84] http://allafrica.com/stories/201407210683.html Retrieved 05/07/2017
[85] http://www.tespok.or.ke/reports/Q3-2013/Cyber%20Threat%20Trends%20Report_Q3.pdf Retrieved 05/07/2017

citizens sent out messages of fear causing panic and passing information, which the terror group used to effectively plan attacks.[86]

During this period it is estimated that Kenya lost over 2 billion shilling annually because of cyber fraud, which was accentuated by the rise of online and mobile banking. The financial institutions received the biggest blows as banks lost money via online fraud, electronic funds transfer, credit card fraud, identity theft and loan fraud.[87]

The Slammer Worm, which was commonly used in 2003 to cause denial of service on internet hosts to generally slow down the internet traffic and was known to infect over 70,000 computers in a time of ten minutes, was also a bug used by hackers in Kenya over the period. The worm, which used Microsoft's SQL Servers slowed down the internet by collapsing numerous routers which caused loss of time and money in Kenya.[88] The Slammer Worm was at least ten year old when it became a cyber threat to Kenya in this period and this goes to show how vulnerable Kenya was citing user ignorance or ineptitude opening up an avenue for cyber security firms to establish business and organizations to understand the importance of cyber security.[89]

[86] http://www.theeastafrican.co.ke/news/How-cyber-crime-complicates-war-on-terror/2558-2422854-13ja90iz/index.html Retrieved on 05/07/2017
[87] http://www.serianu.com/downloads/KenyaCyberSecurityReport2014.pdf Retrieved on 05/07/2017
[88] http://www.spamfighter.com/News-18517-In-Kenya-Cyber-attacks-and-E-threats-Surged-Sharply-says-TESPOK.htm Retrieved 05/07/2017
[89] http://www.businessdailyafrica.com/corporate/Cyber-crimes-open-window-for-IT-firms/539550-1998058-4amfcd/index.html Retrieved on 05/07/2017

2.3.2 Recent threats (2015 - 2017)

This period not only saw an increased frequency in the cyber-attacks but also in the sophistication nature of the newer attacks, which were more focused and targeted mainly on business enterprises and government agencies; and, importantly, most of these attacks were launched by home grown cybercriminals who were becoming more skilled as cybersecurity improved. During this period, cyber-attacks in Kenya mainly revolved around ransomware, database transaction manipulation and social engineering with financial loss via cyber-crime pegged at $175 million in 2016.[90]

In early 2017, there was a global ransomware called WannaCry, which attacked over 300,000 users running their computers on Microsoft Windows, which was the virus's target. Over 80% of Kenyan organization run on this system and they automatically became susceptible and vulnerable to WannaCry. It was reported widely that about 19 firms fell victim to the cyber-attack with two multinational corporations allegedly losing data most likely because they failed to pay the ransom or run out of time.[91] In a separate attack eight Kenyan institutions, telecommunication companies and government agencies were also reportedly attacked by an invisible memory malware, which is very hard to detect and is used to steal passwords and financial data.[92]

In another study conducted by Kaspersky Lab, it was discovered that a malware from a group calling itself Lazarus was found in financial institution and crypto-currency businesses in Kenya. The group of hackers breach the system remotely through a webserver or water-

[90] http://serianu.com/downloads/KenyaCyberSecurityReport2015.pdf Retrieved on 05/07/2017
[91] http://www.nation.co.ke/news/14--cases-of-ransomware-attacks-in-Kenya/1056-3930394-8eq5g4z/index.html Retrieved on 05/07/2017
[92] https://moneyandmarkets.co.ke/kenyan-banks-among-victims-fileless-malware-attacks/ Retrieved on 05/07/2017

holing the system upon invite from a staff member of a target institution and once the hackers gain access they create a backdoor and bypasses before they can steal money from banks or information and data.[93] Other malware attacks that were common in this period include; Sality, which allows computers to be controlled remotely and the malware to download additional malware, Virut, which is a botnet used in DDoS attacks, data theft and spam distribution and is usually spread using removable drives and compromised websites, and Mazben, which targets Windows operating systems, where the attacker can remotely send spam messages to other systems and computers.[94]

As far as database transaction manipulation is concerned 2017 saw Kenya report the largest loss via hacking when a 28 year old man Alex Mutungi Mutuku was arrested and charged with hacking the Kenya Revenue Authority systems and causing a loss of about 4 billion Kenya Shillings. According to the police, he was part of an international hacking group, which conducted its attacks between 2015 and 2017.[95]

Social Engineering has also become prevalent especially in the mobile money transfer age, whereby customers lose money from their mobile phones. This cybercrime involves the criminals who have been reported to be in prison, calling mobile-phone users claiming they have sent money to them wrongly and requesting for a reversal. The criminals then withdraw or forward the money before the victim can report to the mobile-service provider for a reversal. The cybercriminals can also phish for usernames, identity numbers, passwords and

[93] http://aptantech.com/2017/04/lazarus-group-malware-samples-were-detected-in-it-networks-of-kenyan-firms-kaspersky/ Retrieved on 06/07/2017
[94] http://www.biztechafrica.com/article/cybercriminals-target-african-countries-ransomware/12064/ Retrieved on 06/07/2017
[95] https://www.standardmedia.co.ke/business/article/2001233552/man-charged-with-hacking-kra-and-causing-sh4b-loss Retrieved on 06/07/2017

PIN numbers in a bid to steal from the unsuspecting victims. Another form of social engineering sees the attackers send text messages to vulnerable mobile phone users claiming they have won and need to send money in order for them to receive the cash prizes. The unsuspecting victims thereby lose the money and never really get to get the cash prize as promised in the text message.[96]

2.4 Conclusion

The above section delved on the most common cyber threats that exist globally and in Kenya. Importantly, the dynamic feature of the cyberspace is especially influential in moulding the cyber threats, which morph according to the cybersecurity options that are created for protection and prevention. In this section, it is clear to point out the technological vulnerabilities that exist in Kenya despite the technological advancements and internet-penetration; this is exemplified by the malware attack that affected Kenyan systems despite there being a solution to it ten years earlier. The ransomwares that have attacked Kenya appear to most likely persist and could be greater in magnitude due to the inadequacies especially in Kenyan government, which has seemed to move over 50% of its service delivery to the cyberspace. With the world becoming one global village via the cyberspace in the coming years an American, German or Chinese cyber threat will immediately become a Kenyan problem as experienced with the ransomware WannaCry and for this the Kenyan government needs to address cybersecurity in its domestic policy. The next chapter reviews Kenya's domestic policy in relation to what the rest of the world is doing to address the cyber threats.

[96] http://www.kachwanya.com/2014/03/11/m-pesa-fraud/ Retrieved on 06/07/2017

CHAPTER THREE

DEALING WITH CYBER THREATS AND ATTACKS IN KENYA

3.0 Introduction

The cyber space is as dynamic as it is fluid; it changes on a daily basis almost taking the form of the various personalities that are behind every click of the button and in this regard the cyber criminals tend to be a step ahead of the security measures, which have to improve accordingly especially because cyber-attacks are also very unpredictable.[97] Cyber-attacks are directed towards individual users, organizations, businesses and government agencies and whereas the measures to deal with these threats may differ, there needs to be a monitoring authority with legal backing in order to handle not only the crime but also the underlying elements of cybercrime that have seen criminals walk scot free. Post-industrialization came the information age, which has seen almost every aspect of society rely on the cyber space for every interaction and transaction thereby giving rise to cybercrime, which deals with theft or destruction of information.[98]

In this chapter, we look at the front line measures taken individual users, organizations, businesses and government agencies in dealing with cyber threats and attacks, as well as various domestic policies that have been drafted in regards to dealing with this new international relations issue.

---

[97] Glenny, Misha; Glick, Bryan; Hyppönen. Mikko H.; Wainwright, Robert(2010), Cybercrime, cybersecurity and the future of the internet, Session Handouts, Global Economic Symposium 2010 (GES), 27-29 September 2010, Istanbul, Turkey

[98] Ibid.

3.1 Background

Cyber security are measures taken to protect a system against a cyber threat or attack and these measures change according to the threat i.e. there is no one magical solution for all cyber-attacks or threats. This transformation of cyber-attacks and consequently cyber security can be traced back to 1971 when a researcher Bob Thomas created what is believed to be the first computer virus, whereby he learnt that traces of a computer could be left across a larger network via a self-replicating mechanism and affecting the TENEX operating system. This worm was aptly called Creeper due to its mode of transmission and left a message, 'I'M THE CREEPER: CATCH ME IF YOU CAN'. In 1972, Ray Tomlinson then used a similar self-replicating system to create the Reaper, whose work was to follow the Creeper and delete it, making this the first anti-virus software.[99] In 1986, the concept of cyber security took a more advanced position from the previously academic approach when a German computer programmer Marcus Hess hacked about 400 computers including the mainframes at the headquarters of the US Department of Defence better known as the Pentagon, via the internet with the sole aim of exchanging the information to Russia for monetary gain. Even as Hess became known as a digital spy, Russia and the USA took it upon themselves to delve and dedicate resources to cybersecurity.[100]

Policy can be defined as administrative decisions whereby if they are domestic, they pertain such decisions that are applicable within a nation's border whereas a business policy relates to decisions within a business organization. It can also be described as a guideline, principle,

---

[99] Metcalf, John 2014. "Core War: Creeper & Reaper" retrieved on 29/07/2017

[100] Ramirez, Jessica (8 March 2010). "The History of Computer Hacking". Newsweek. *Retrieved 29/07/2017*

law and even a strategy, which can be used to find a solution to a problem once enforced or implemented they help address pertinent issues involving an organization or a nation. In business organizations a cybersecurity policy is embedded in the IT or information security policy whereby an organization clearly defines how it intends to protect its information assets and information systems, while at the same time ensuring compliance with legal and regulatory needs, as well as maintaining an environment that supports the guiding principles. A good information security policy has clear objectives, top among them protecting the organization, employees, suppliers, customers, from damage and loss of information.[101]

Domestic policy regarding cybersecurity has become a priority because it encompasses all aspects of governance from social, economic, military, diplomatic, legal and law-enforcement as well as technical. Domestic policy on cybersecurity is now seen as a sovereignty issue due how wide-reaching the issue has become and they ensure proper and smooth governmental coordination while at the same time encouraging public-private partnership and cooperation. The policy must ensure fundamental values like freedom of speech and privacy are promoted and protected. However, for any policy to sufficiently meet all these needs and the threshold in the modern world, continued research is imperative on the part of national governments if they are to keep up with the changing trends.[102]

The first cybersecurity legislation and by extension, policy, was the Computer Fraud and Abuse Act, which was enacted by the US Congress in 1986, after the Comprehensive Crime Control Act of 1984 was amended and prohibits accessing a computer or a computer system

[101] https://www.sagedatasecurity.com/blog/seven-characteristics-of-a-successful-information-security-policy Retrieved on 25/07/2017
[102] Ibid.

without authorization. This law was used for the first time, during the case against the creator of the Morris Worm, Robert Morris, in 1988.[103] Two important actions arose from the Morris Worm case; first, the US government formed the Computer Emergency Response Team, which later became, the US-CERT, and secondly, the rise of antivirus as the threats and attacks became more potent, dangerous and widespread.

These domestic policies on cybersecurity or cybersecurity strategy are created in a bid to protect individual users, organizations and the society or country as a whole because any lapses or failures no longer affect these distinct users alone but ultimately all aspects of governance and thus the need for governments to establish potent policies. Furthermore, these policies are geared towards strengthening the same aspects of governance they are dedicated to protect.[104]

3.2 Domestic Cybersecurity policy

Cybersecurity policy has become a matter of national priority in many countries with the more developed states taking an advanced role as compared to the developing countries and this can be attributed to technological advancement across the international spectrum. Cybersecurity is special in that it involves all aspects of governance in any country, and thus it should essentially seek to include not only legal, intelligence and military, but also economic, educational, social, and diplomatic aspects while at the same time putting into consideration the important matter of sovereignty.[105]

---

[103] Mello, Susan M. (1993) *Administering the Antidote to Computer Viruses: A Comment on United States v. Morris* 19 Rutgers Computer & Tech.

[104] http://www.oecd.org/sti/ieconomy/security.htm Retrieved on 29/07/2018

[105] Ibid.

A functional domestic Cybersecurity policy should have four pertinent elements as exemplified by 8 countries in the Organisation for Economic Co-operation and Development (OECD) in the UK, USA, Germany, Australia, France, Canada, Japan and the Netherlands, with Spain and Finland following the same shared principles and commonalities thereafter. These countries came up with domestic cybersecurity policies that ensured enhanced governmental co-ordination at policy and operational levels, strengthened partnership between government and private corporations, improved international cooperation, and respect of fundamental rights or upholding fundamental values. In addition to these elements, the countries ensure that their sovereignty is not compromised, while putting into consideration the dynamic nature of the cyberspace and thus applying flexibility in the policy making and implementation. These countries, from the onset, set out to draft policies that concentrated but not limited to the following areas; priority was given to government security, protection of critical infrastructure, cybercrime fight, raising awareness, educating all stakeholders and response measures and mechanisms. These examples of OECD countries can be augmented by what the respective countries have done as far as domestic cybersecurity policy or strategy is concerned. The United Kingdom, for example, developed a strategy starting in 2009 by changing her traditional approach to national security, whereby cybersecurity was the major driving force, in its 2010 National Security Strategy and the Strategic Defence and Security Review. At the same time, France developed its policy under the Defense and security of information systems, which produced the White Book on Defense and National Security, and this also put into account the changing trends, among them cybersecurity, in the international environment. The E-Security National Agenda of

Australia is another example of the domestic cybersecurity policy, whereby cybersecurity was accorded top priority.[106]

3.2.1 USA's Domestic Cybersecurity policy

The Morris Worm case ruled under the Computer Fraud and Abuse Act, is believed to be the 1st form of cybersecurity legislation in the USA. Over the years such crimes have not only evolved but also legislation, and consequently domestic policy has come to the fore to ensure a safe and secure cyberspace, with presidents such as Barrack Obama coming out very strongly to ensure that. USA has arguably the highest internet connectivity which means that there is also increased vulnerabilities, which may come in the form of identity theft, data breaches, hacking, cyber-attacks and even cyber bullying. The Stuxnet virus, for example was used to destroy Iran's nuclear program by causing the nuclear reactors to spin so fast that they destroyed themselves; the leaks by intelligence officer Edward Snowden, and the infamous hack by Chinese cyber criminals on US government offices are examples of events that provided not only a learning curve but also a turning point to USA policy on cybersecurity.[107]

The Protecting Cyber Networks Act (PCNA) (H.R. 1560) of 2015 is one such act that deals with cybersecurity in the USA, and it seeks to utilize a public-private partnership approach, whereby private companies can share cyber threat indicators with each other and voluntarily, with the federal government, while at the same time ensuring privacy and civil liberties are

[106] http://www.oecd.org/sti/ieconomy/security.htm Retrieved on 29/07/2018
[107] Purser, Steve (2014). "Standards for Cyber Security". *IOS Press*.

protected.[108] The PCNA provides for the government to use the shared information only for cybersecurity reasons, which in turn helps the government in response to cyber-attacks, investigation, prosecution and mitigation of cybercrimes.[109] There have been changes on the original PCNA, whereby in 2015, President Barrack Obama signed for the establishment of the Cyber Threat Intelligence Integration Center which would serve as a support program for the National Cybersecurity and Communications Integration Center. It is important to note that PCNA does not allow the sharing of information or access to the data with any entity outside the federal government. PCNA, while voluntary only allows the sharing of limited information to ensure the protection of privacy and it does so by prohibiting the government from forcing private entities from sharing the information, requiring that the private companies remove any personal and private information before sharing it with the government, which should double check for the same before sharing it with any other government department. The act does not allow sharing of information and data for non-cyber reasons between private-private and has strict restrictions on the use, retention, and searching of any data voluntarily shared and to ensure all the above are followed, The Privacy and Civil Liberties Oversight Board has to write a biennial report.[110]

The Cyber Threat Sharing Act 2015 (CTSA) was introduced to the US Senate, as a bill, by Senator Thomas R. Carper, who intended to establish a bill that allows private entities to share cyber threat information better, with other private businesses and the government.

---

[108] https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/new%20bill%20summary%20pdf.pdf Retrieved on 30/07/2017

[109] Fischer, Eric. "Cybersecurity and Information Sharing: Comparison of H.R. 1560 (PCNA and NCPAA) and S. 754 (CISA)." Report to Congressional Committees. Congressional Research Service, November 6, 2015. Federation of American Scientists Project on Government Secrecy. https://www.fas.org/sgp/crs/misc/R44069.pdf.

[110] Ibid.

Under this act the Department of Homeland Security was at the center of information sharing and allows the government to share both unclassified and classified cyber threat data with industry. The Cybersecurity Intelligence Sharing and Protection Act (CISPA) was then introduced and sought to involve legislative language and citizen privacy in cybersecurity legislation. It also protected private companies in order to garner support but its language was still vague and did not get the support of President Obama and therefore did not become law.[111] However, the legislative process and attention from the US presidency saw most of the elements of these bills and acts find their way into the Cybersecurity Information Sharing Act (CISA) and the Cybersecurity Act of 2015.

The Cybersecurity Act of 2015 ensures that private companies have the option of sharing information about potential cyber threats with the federal government, and even provide legal protection to these companies to act as an incentive to encourage more information to be shared between private and public entities. Furthermore, the two objectives of this act is to protect the privacy of American citizens while at the same time protecting and encouraging private business in the sharing of the cyber threat information, and all this is to be done through the Department of Homeland Security, which could initiate the information sharing. The Act also gave the president powers to appoint another federal agency to conduct this business when necessary.[112] The Act sought to increase cooperation between the private entities, who own and control most of the critical network infrastructure, and the

[111] Fischer, Eric. "Cybersecurity and Information Sharing: Comparison of H.R. 1560 (PCNA and NCPAA) and S. 754 (CISA)." Report to Congressional Committees. Congressional Research Service, November 6, 2015. Federation of American Scientists Project on Government Secrecy. https://www.fas.org/sgp/crs/misc/R44069.pdf.

[112] Gregory S. McNeal (2014). "Controversial Cybersecurity Bill Known As CISA Advances Out Of Senate Committee". Forbes. Retrieved 30/07/2017

government, representing the public; and this was supported by major companies as such as Verizon, AT&T, and Boeing. However, civil liberty groups and technology companies such as Apple, Twitter, Microsoft, and Google were opposed to the Act citing vagueness of the language in regards to the privacy of individual information and the specific circumstances under which the government would be able to access private information.[113] The Department of Homeland Security released guidelines on the Act, which assures the protection of individual information as well as incentives to the private companies to encourage the sharing of information with the government and this was all geared towards national security, which had become a priority under President Obama. President Obama went further, in his attempt, to ensure that the American citizens were catered for in the Cybersecurity Act, by releasing the Cybersecurity National Action Plan in 2016, which sought to improve knowledge of the citizens and the critical infrastructure of the government. It is not legislation but a plan to educate the citizens about their personal cyber threats through Awareness Campaigns and also modernizing technology used by the federal government, and to achieve this the president increased the budget allocation from $5 billion to $19 billion as well as the appointment of a 12-member committee, drawn from various technological backgrounds for advisory purposes.[114]

---

[113] Barb Darrow (24 Sep 2015). "Apple, Microsoft, others slammed for supporting cybersecurity bill". Fortune. Retrieved 30/07/2017

[114] Fischer, Eric. "Cybersecurity and Information Sharing: Comparison of H.R. 1560 (PCNA and NCPAA) and S. 754 (CISA)." Report to Congressional Committees. Congressional Research Service, November 6, 2015. Federation of American Scientists Project on Government Secrecy. https://www.fas.org/sgp/crs/misc/R44069.pdf.
[114] Gregory S. McNeal (2014). "Controversial Cybersecurity Bill Known As CISA Advances Out Of Senate Committee". Forbes. Retrieved 30/07/2017

3.3 Kenya's Cybersecurity policy

Kenya's domestic policy on the various aspects of governance are guided by the head of state, who decides or lays out the direction he/she believes is best suited for the country. The president cannot influence every single decision from research, development and to implementation but the appointments of the people in charge and the agencies created are majorly a reflection of the political will. For instance Kenya's cybersecurity strategy or policy falls under Ministry of Information Communication and Technology, most specifically the Information and Communication Technology Authority, which is a State Corporation established in 2013. The ICT Authority is mandated with the responsibilities of rationalizing and streamlining the management of all Government of Kenya ICT functions as well as supervising the government's electronic communication and the promotion of ICT literacy and innovation. The ICT Authority serves a number of functions among them; setting and enforcing guidelines for the infrastructure, human resources, procedures as well as providing systems and technology to public offices and public service, manage all ICT staff in the public service, regulate ICT is used in the public service, promotion of e-government services, among other functions.[115]

The ICT Authority drafted the national cybersecurity strategy 2014, which recognized Kenya's growing reliance on the cyberspace for most aspects of life and governance especially with the laying of the fiber-optic, and the anticipated threats that come with it, from Nation states, criminal organizations, and hacktivists. Therefore the national cybersecurity strategy 2014 was created in order to ensure that the country could respond

[115] http://icta.go.ke/who-we-are/ Retrieved 30/07/2017

adequately to these threats so that national priorities remain on course with the vision 2030, and is even termed as a priority item in the list. The strategy outlines four objectives, top among them the enhancement of Kenya's cybersecurity by protecting the critical infrastructure by increasing security and resilience in order to offer protection to government, its population and corporations against any cyber threats. To achieve this, the Kenyan government through the ICT Authority analyses the current environment in relation to the government's aspirations before working towards bridging the gap between the current state and the aspirations in order to develop cybersecurity regulations, policy and legal framework. The other objective is to create cybersecurity awareness among Kenyans in order to build capability and develop Kenya's workforce to address cybersecurity needs and plan to achieve this through agreements with other governmental departments and organizations, the private sector as well as the academic world. The third objective is to encourage and promote the sharing of information and working together by developing a detailed framework in order to utilize all available resources, to cut down on conflict and duplication of roles and labour; to achieve this the Kenyan government intends to create required laws, regulations and policies, involve various stakeholders, while at the same time to create a balanced information security, privacy concerns and economic priorities. The fourth objective is to provide national leadership by creating and harmonizing the application of national cybersecurity strategy and master plan.[116]

Kenya's cybersecurity strategy is multi-layered with each layer seeking to augment the next and ultimately ensure the government realizes its vision, goals and objectives. The outer

[116] http://icta.go.ke/who-we-are/ Retrieved 30/07/2017

most layer comprises operations, infrastructure, resilience, awareness and training and communications and outreach. Under these all issues involving threat intelligence, malware analysis, critical infrastructure protection, business impact analysis, disaster recovery, internal and external stakeholder engagement and capacity building. Once these issues are addressed then they pave way for organization, governance and risk management, legal and regulatory affairs and then strategy and planning.[117]

3.3.1 Kenya's Legal Framework of Cybersecurity

The national cybersecurity strategy has seen an advancement in the approach to cybercrime, especially locally by seeking to improve existing legislation in a bid to ensure a safe and secure cyberspace, where a majority of activities are carried out. The Kenya Information and Communications ACT, CAP 411A was amended by The Kenya Information and Communication (Amendment) ACT, 2012/2014/2015, and is best suited to deal with various issues of cybersecurity but not in its entirety. In the 2013 amendments the Communication Authority of Kenya was established and the term cybersecurity was defined as the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment. The Act demands that before a telecommunications operator such as Safaricom, Airtel or Orange can sell a SIM card, the individual must provide full names, identity card and even address, which serves as the first step in dealing with cybercrime, whereby the SIM user is liable to any crime committed using the SIM card. The law further stipulates that any individual who gains unauthorized access or attempts to secure such access to a protected system is liable on conviction to a fine, imprisonment or both.

[117] Ibid.

Such access is defined as inputting, acquisition, alteration, deletion or suppression of data in a system. The act further states that a Communications and Multimedia Appeals tribunal is to be set up in order to deal with such cases.[118]

The legislation also allows for the formation of the National Kenya Computer Incident Response Team Coordination Center (KE-CIRT/CC), which was set up in order to coordinate response and manage cybersecurity incidents in Kenya and to collaborate with relevant stakeholders locally, regionally and internationally. The KE-CIRT/CC is supposed to be the trusted point of contact and should offer advice on cybersecurity matters in Kenya. Its other main functions include: gathering and circulation of technical information such as incidents that affect computer security, conducting research and analysis on computer security, creating and maintaining awareness on cybersecurity-related activities as well as capacity building in information security and, facilitating the development of a National Public Key Infrastructure (NPKI).[119] The KE-CIRT/CC was actively involved in creating awareness when the Petya Ransomware v0.3 was affecting machines whereby it warned Kenyan users on what to look out for and how to protect their systems from the malware.[120]

The NPKI project is carried out under the Ministry of ICT through and together with the Communications Authority of Kenya and the ICT Authority (ICTA) and is provided under the Kenya Information and Communications Act, 1998, to refer to the establishment of online identity through a system of creating, storing and distributing digital certificates.

[118] http://kenyalaw.org/kl/fileadmin/pdfdownloads/AmendmentActs/2013/KenyaInformationand Communications_Amendment_Act2013.pdf Retrieved on 01/08/2017
[119] http://www.ke-cirt.go.ke/index.php/about-us/ Retrieved on 01/08/2017
[120] http://www.ke-cirt.go.ke/index.php/petya-ransomware-v0-3-national-ke-cirt-cc-report/ Retrieved on 01/08/2017

NPKI comprises of a Root Certification Authority (RCA), which is managed by the CA as a regulatory function, and the Government Certification Authority (GCA), an Electronic Certification Service Providers (E-CSP) which is managed by the ICT Authority. This ensures that all the basic fundamentals of cybersecurity such as privacy, integrity, and authenticity are protected within the confines of the law.[121]

3.4 Conclusion

This chapter delved into domestic policy on cybersecurity starting with its definition before looking at broad examples of such, and then specific examples, whereby USA was used due how advanced their cyberspace is, before looking into Kenya's case. Kenya is still in the nascent stages but not immune to cybercrime and therefore its policy remains vague and borrows heavily from the more advanced states. The United States of America has shown that a powerful leadership is crucial in the establishment of a potent domestic policy, one that ensures the citizens are safe and secure, and their information is kept private, while at the same time keeping government procedures free from interference. However, there is the thin line between protecting the state and ensuring privacy for individual users and private corporations, and thereby conflict arises. American corporate have deemed the cybersecurity act as intrusive and state-centric, and similar conclusions can be drawn from the Kenyan case, whereby the cybersecurity is more or less geared to protect the government's information and data and not necessarily the citizens directly. Pertinently, the dynamic characteristic of the cyberspace means that domestic policy and legislation should also morph to accommodate the ever changing nature of technology and the various cybercrime that follows. USA, just like Kenya, continues to amend the laws in order to match up with

[121] http://www.ke-cirt.go.ke/index.php/services/national-pki/ Retrieved on 01/08/2017

the changing trends in cybercrime. States cannot exist in isolation and therefore need to establish a foreign policy that compliments its domestic policy is imperative and the next chapter will delve into that.

CHAPTER FOUR

CYBERSECURITY AND INTERNATIONAL PEACE

4.0 Introduction

The cyberspace has introduced a new frontier for international relations and as such cybercrime threatens international peace and security. This interconnectedness of the international realm is best exemplified by the cyber space, characterized by interconnectivity and flow of information, where free market thrives and promotion of liberal values has taken an integral place. Cyberspace, then can be explained as a complex virtual environment brought about by the interaction of people, software and services on the internet by the means of technology devices and networks connected to it. There is no one stakeholder in cyberspace but the government can provide the role of regulation and enforcement.[122] Conflict is as old as humankind. It is in every aspect of human interaction, be it religious, economic or political. There is said to be conflict when two or more persons or parties seek to undertake acts which are mutually inconsistent. These parties maybe as basic as individuals or as complex as groupings of people and states.[123] The process of achieving cybersecurity can be a cause of conflict, while at the same time, the existence of cybersecurity can be part and parcel of international conflict management.

4.1 Background

There exists numerous challenges in the cyberspace especially in its governance. The traditional international relations is mostly between states, whereby the state provides for

[122] Kigen, P., C. Kisutsa, C. Muchai, K. Kimani, M. Mwangi & B. Shiyayo. 2014. "Kenya Cyber Security Report 2014: Rethinking Cyber Security – "An Integrated Approach: Processes, Intelligence and Monitoring."

[123] Nicholson, M. (1992) Rationality and the Analysis of International Conflict (Cambridge 12 University Press)

national security over land, air and sea; but the cyberspace is a virtual realm, mostly organized under private corporations who are the internet service and crucial internet-related services providers such as Amazon, Microsoft, Google, Apple. The role of the state in as far as the cyberspace is concerned is very vague and undefined due to the lack of physical borders and boundaries, and the fact that individual use is an expression of civil liberties, therefore the government need to find the right balance between ensuring national security without affecting entrepreneurship or infringing on human rights. To this end the government need to seek a collaborative approach, not only with the private corporations but also with other states to ensure security in the cyberspace.[124]

States also engage in cyber warfare, whereby governments can attack, retaliate or use coercion and North Korea exemplifies this. According to various media reports, North Korea has a special cell in its spy agency called Unit 180 and is used to launch cyber-attacks on financial networks in the USA and South Korea. In 2016, a hacking group, based in North Korea, called Lazarus conducted a cyber heist against Bangladesh central bank where over $80 million was lost and before that, in 2014, Sony Picture's studio was also attacked and private information leaked as well as movies leaked resulting to the loss of millions of dollars. This web further enjoins Malaysia, which is reported to host the IT firms that are used in the cybercrime because of fast and reliable internet connections.[125]

---

[124] https://www.extension.harvard.edu/inside-extension/how-cyberspace-transforming-international-security Retrieved 02/08/17

[125] http://www.reuters.com/article/us-cyber-northkorea-exclusive-idUSKCN18H020 Retrieved 02/08/17

In the cyber age USA and Russia remain at loggerheads over alleged interference, sometimes state-sponsored, other times individuals based in either state. One such case is that of Russia-linked cyber-criminal Alexsey Belan who, in 2013, was accused and sought for launching assaults on US networks using thousands of hacked computers. According to the FBI, Belan was used to steal information from over 500 million Yahoo email accounts by hacking into the National Security Agency. The USA say Belan escaped European agents traps with the help of Russia and even China, who they accuse of providing immunity in exchange for the cyber expertise and skills.[126] The Edward Snowden case is another apt example of the USA-Russia cyber feuding, whereby the former American CIA employee and when working as a contractor for the National Security Agency, copied and leaked classified information , which showed an unholy union between the US government, telecommunication companies and European government. In 2014, Snowden left the USA for Hong Kong, from where he leaked the information before flying to Moscow, where he was stranded at the airport before Russia gave him asylum, which was extended to 2020 in 2017. The US government have a warrant of arrest on Snowden for espionage and theft of government property.[127]

Snowden's case shows what thin a line exists between the state, private corporation and individual users; the state labelled Snowden a dissident, whereas individual internet users glorified him as a whistleblower. The leaks revealed that the US government had an established surveillance system in collaboration with Google and Yahoo, which are private

[126] https://www.csmonitor.com/USA/2017/0628/How-Russia-and-others-use-cybercriminals-as-proxies Retrieved on 03/08/2017

[127] Finn, Peter; Horwitz, Sari (2013). "U.S. charges Snowden with espionage". *The Washington Post*. Retrieved on 03/08/2017

internet companies; it was a similar case in Britain, where the government had surveillance on its citizens. There were reports of deeper surveillance through popular internet-based applications and companies such as Xbox Live and World of Warcraft. Snowden's case spurred a diplomatic tussle not only between USA and her allies against Russia but also against Bolivia, whereby President Evo Morales was denied entry into the France, Spain and Italy airspaces for allegedly trying to transport Snowden from Russia to Bolivia to offer asylum; upon landing in Austria, the plane was reportedly searched.[128] Whereas the various states were vilifying Snowden for his leaks, he was receiving accolades for whistleblowing; he was named runners-up Time's Person of the year in 2013 behind the Pope, he received Germany's whistleblower prize in 2013 among others for his expose.[129]

Snowden, worked with Chelsea Manning during his contractual work with NSA and Manning also leaked information using Wikileaks, which was founded by Australian Julian Assange. Manning may have been arrested and released in the USA, but Assange remains in asylum protection at the Embassy of Ecuador in London as he is wanted for an alleged sexual assault, which happened in Sweden. Wikileaks is an organization, which releases leaked information accessed through hacking and by 2015, it had leaked over 10 million documents including government cables and the infamous Guantanamo files. Wikileaks also leaked information, allegedly after Russian cybercriminals hacked Democratic Party servers, that the former US secretary of state Hillary Clinton had used her personal email for official communication, which was a source of great debate during the US elections in 2016. For this

[128] Finn, Peter; Horwitz, Sari (2013). "U.S. charges Snowden with espionage". *The Washington Post*. Retrieved on 03/08/2017
[129] Ibid.

Assange was termed as a 'terrorist' by the American government and his activities 'illegal' by his home government in Australia but celebrated by citizens of the world what they term as promoting human rights by exposing the truth.[130]

4.2 International Policy on Cybersecurity

There has been concerted efforts to have some form of order on the cyberspace and inevitably it has been state-led with even the United Nations involved in the process, citing the growing opportunity not only for growth and development but also crime and aggression, and therefore seeks global cooperation. In 2011, the UN's Economic and Social Council (ECOSOC) together with the Department of Economic and Social Affairs (DESA) and the International Telecommunication Union (ITU) organized the "Cybersecurity and Development Event" in New York, USA and it involved high ranking officials in these agencies as well as member states, private sector representatives and civil society. The event discussed how to build awareness at the international policy level picking out the challenges facing cybersecurity. They also identified the best practices and initiatives from across the world and explored the options available to tackle cybercrime by managing the risks involved through increasing interconnectivity. It was pointed out that the huge difference and disconnect between the developed and developing countries could lay serious challenges in future, where weak legal systems in the developing countries could offer loopholes to cyber

[130] Carr, David and Somaiya, Ravi, (2013) "Assange, back in news, never left U.S. radar", *The New York Times*. Retrieved 03/08/2017

criminals who would launch attacks easily and freely, and therefore a partnership was necessary to avert this, by providing expertise and security knowhow.[131]

In 2013, a Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security pointed out that International cooperation was a sure way of reducing risk and enhancing security in the world by establishing standard patterns, regulations and principles of responsible behaviour by States, voluntary measures to increase openness, credence and trust among States and capacity-building measures. The Group recommended the use of international law as prescribed under the UN Charter to maintain peace and stability, adding that the issue of state sovereignty in relation to ICT is applicable as afar as the critical infrastructure within its territory is concerned.[132]

In 2015, a Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security examined current threats and potential threats in order to build on what the previous group had accomplished. The Group acknowledged the need for international cooperation and went a step further to define the norms and principles recommending that states should ensure no harmful ICT practices targeted to other states, are conducted in the territories, calling for prosecution of such criminals and cyber terrorists while at the same time guaranteeing privacy and freedom of expression.[133] Furthermore, the group spelt out how all this can be achieved; states should

[131] http://www.un.org/en/development/desa/news/ecosoc/cybersecurity-demands-global-approach.html

[132] http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98 Retrieved on 03/08/2017

[133] http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174 Retrieved on 03/08/2017

not impede or damage the other's critical infrastructure, states should not aim at each other's computer emergency response teams, states should collaborate with other nations to investigate cyberattacks, and states should carry responsibilities for any action that emanate from their territory.

Fast forward to 2017 and the global arena is still discussing how to safeguard the cyberspace and yet again it is the state that is at the forefront, especially so because of the ravaging malware WannaCry, which was attributed to North Korea and the Russian hackers on the US Democratic National Committee (DNC) and Petya/NotPetyta attacks on Ukraine. In the wake of these events, states took it upon themselves to create treaties based on cybersecurity. China and Canada signed one such agreement, purely covering economic cyber espionage, where both states pledged launch state-sponsored cyber-attacks against each other in attempts to steal trade secrets. China, which has been considered by many other states as an aggressive cyber participants has also gone ahead to sign more agreements with the USA, UK, Australia, the G7, and the G20.[134]

USA sought to end the 2016-2017 Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security process citing deficiencies of how international law should be applied in the cyberspace, specifically those governing states' exercise of their inherent right of self-defense, and the law of State responsibility, including countermeasures.[135]

---

[134] https://www.cfr.org/blog/development-cyber-norms-united-nations-ends-deadlock-now-what Retrieved on 03/08/2017

[135] https://www.state.gov/s/cyberissues/releasesandremarks/272175.htm Retrieved on 03/08/2017

4.2 USA's Foreign Policy on Cybersecurity

There are two major approaches towards Internet governance; first, a multi-stakeholder approach, which involves a collaborative and cooperative approach between private industry and national governments to promote open and free internet with optimum accessibility. The multilateral approach focuses on state-to-state agreements without the inclusion of the private industry thereby advocating for control and monitoring of the Internet with strict access points.[136] As it is applicable in domestic policy, international policy is molded according to the presidency and once the USA elected a new president Donald Trump, she decided to withdraw from the discussions pertaining international policy on cybersecurity.

The USA also approaches foreign policy on cybersecurity from two perspectives; Defensive and Offensive Measures, which oscillates between a state protecting itself and launching an attack. The Cybersecurity Act of 2015 defines defensive measure as an effort and/or activity, instrument, and signature, technique used in the detection, or mitigation against an identified or suspected threat or security vulnerability. USA seeks to use the defensive measures in order to promote partnerships not only with private industry but also with other states in order to mitigate and prevent attacks. Proponents of USA's Cybersecurity Act of 2015 argue that the defensive measures are a crucial component to national security and is exemplified under the National Security Cyber Assistance Program (NSCAP) run by the National

---

[136] Marg, Max. "The Future of the Internet: Who Should Govern It and What Is at Stake for You? A Multistakeholder Dialogue." Thinktank. Internet Democracy Project, n.d. https://internetdemocracy.in/events/the-future-of-the-internet-who-should-govern-it-andwhat-is-at-stake-for-you-a-multistakeholder-dialogue/ Retrieved on 03/08/2017

Security Agency (NSA). The National Security Cyber Assistance Program seeks to detect any intrusion, respond to incidents, assess any vulnerabilities and test penetration, and it does so by accrediting qualified service providers such as Lockheed Martin Corporation, CrowdStrike and FireEye/Mandiant. Outside the Cybersecurity Act of 2015, which supports the defensive approach, the Department of Defense pushes for another strategy, which is offensive in nature but aptly named as 'active defense' which seeks to integrate the various elements in order to share information, capabilities, and anticipate threats.[137] USA under President Obama used the active defense strategy against Iran when USA planned a cyber-attack over Nuclear Deal negotiations whereby USA was ready and willing to launch a cyber-attack on Iran should it have failed to comply with the demands not to weaponize their nuclear power. From this we can draw that USA continuously have surveillance on other nation states and indeed are willing to launch a cyber-attack if and when need be.[138] For this other states such as Russia perceive defensive measures as offensive and in 2015 had a budget to respond to these perceived USA offensive strategy and appear to light the embers of the Cold War. Russia cannot be blamed for the perceptions because defensive measures are kept secret and the fear of the unknown can be deemed as passive aggression and it arguably so because in 2010 USA'S Department of Defense created the CyberCom, which is a cyber command center comprised of air, land, and sea departments, all dealing with

[137] https://jsis.washington.edu/wordpress/wp-content/uploads/2016/06/Task-Force-E-Report-2016-Beyer.pdf Retrieved on 04/08/2017
[138] Ibid.

cybersecurity, with the prospect of creating an entire arm of military to deal with cybersecurity.[139]

4.3 Kenya's Foreign Policy on Cybersecurity

Kenya's foreign policy is largely aligned to her colonial master, Britain and has not really changed from independence but with the emergence of China a major economic and political force in the global arena, Kenya, like most African countries appear to be leaning East in terms of policy.[140]

According to Kenya's foreign policy under President Uhuru Kenyatta, it is directed towards achieving various national objectives. The top most priority is to protect Kenya's sovereignty and territorial integrity and for this cybersecurity plays an important role,[141] which is the reason the state has taken concerted steps to place cybersecurity under the state specifically under the Ministry of ICT, department of defense and Interior security. For this reason, as drawn from other state's examples, there is a challenge of infringing on the rights of its citizens; and this is exemplified by reports that the Kenyan government was planning to monitor and run surveillance through Kenyan telecoms. In relation to the UN Charter and the Group of Experts, Kenya works towards the promotion of sub-regional and regional integration and cooperation, which would be essential to achieve a secure cyber space.

---

[139] Olenick, Doug. "U.S. Cyber Command Sets Priorities for the Nations Defense." SC Magazine, September 9, 2015. http://www.scmagazine.com/news/cyber-command-capabilitiesshould-be-integrated-into-us-cybersecurity-efforts/article/437636/. Retrieved on 04/08/2017

[140] https://theforeignpolicyanalyst.wordpress.com/tag/kenya-foreign-policy/ Retrieved on 04/08/2017

[141] http://www.mfa.go.ke/wp-content/uploads/2016/09/Kenya-Foreign-Policy.pdf Retrieved on 04/08/2017

Indeed, UNCTAD and the East African Community (EAC) Task Force on Cyber laws, have been working legal frameworks for e-commerce seeking to harmonize cyber laws and regulations and in 2009, the EAC adopted Africa's first modern and effective regional harmonized framework for cyber laws.[142] This by extension covers the third objective of Kenya's foreign policy, which is directed at enhancing regional and global peace as, the EAC cyber laws, for instance were drafted in line with international norms and principles.[143]

4.4 Conclusion

This chapter dealt with the international policy and foreign policy as far as cybersecurity is concerned. The chapter started by broadly looking at the current state of affairs at the international arena, most specifically the UN and its work on cybersecurity and it is suffice to conclude that it has pooled experts on the field together with nation-states to try and come up with international law in line with its Charter. However, research and experience shows that the Nation-state has become skeptical about how to deal with each other on the cyberspace thereby risking conflict that may spill from the cyberspace and into the physical world. States such as the USA and Russia, as they did during the Cold War, appear to be preparing for a cyber war despite diplomatic statements claiming they support a secure cyberspace. The developed countries also appear to be at advanced stages of creating a foreign policy that is commensurate with the threats and challenges, both potential and actual, that may exist in the cyberspace. However, the developing countries, most specifically Kenya appear to lagging behind in including a plausible outlook of cybersecurity in her foreign policy and this can be

[142] https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Harmonizing%20cyberlaws%20-%20East%20Africa%20Community%20.pdf Retrieved on 04/08/2017

[143] Ibid.

attributed to the approach of security, which remains traditional. As far as infringing on human rights is concerned vis-à-vis upholding the powers of the state, there seems to exist an agreeable consensus that the state is right and might; to take charge of cybersecurity.

CHAPTER FIVE

5.0 Introduction

In the course of this research there certain elements that have emerged; there seems to be an emergence of a securitization of the cyberspace, the emerging threat to the nation-state and a combination of the two, which has now become a threat to international peace and security bordering anarchy. Furthermore, the different level of development amongst the states in the international arena also offers serious challenges in achieving peace and security and Kenya, as part of the case study is an example of one such state that is playing catch up with the more developed countries as far as cybersecurity is concerned.

5.1 Summary of the research

The research project set to investigate the various threats that exist in the cyberspace and how nation-states, in this case, Kenya is interacting with others. Using realism as the guiding theory of this research it is evident that the state continues to exact its authority in the cyber space despite numerous challenges, which include the threat towards peace and security in the international system.

Chapter two specifically discussed the various and most common cyber threats which not only affect other states but specifically Kenya. The chapter took a progressive approach in the attempt to clearly understand how the threats have transformed from mere guesswork, in terms of password-guessing to more complex and intent-driven activities. In the Kenyan example, the chapter outlined the historical background of the various threats that have been prevalent in the country, while at the same time contrasting it to what exists in the more advanced societies, ultimately meaning that they could eventually be future threats to Kenya.

This chapter observed that the threats have now mostly become global, in that, contrary to the past, when these attacks mostly attacked the specific and the more advanced states, the threats have become more potent and large scale. This, then means that a USA, China or Australian threat can and is, easily a Kenyan threat.

Chapter three addressed the measures taken to counter these threats from the basic IT policies in organizations to anti-viruses installed in computers as well as legislation and domestic policy regarding cybersecurity. It is important to note that, the cyberspace and indeed cybersecurity is less than five decades old and therefore, nation-states continuously and progressively adjust their laws as it does with updating security features such as antiviruses due to the dynamic and fluid nature of the cyberspace. The chapter traced back the oldest form of legislation dealing with cybersecurity, whereby it borrowed from existing laws before new laws were enacted and even amended to ensure they suit the cyberspace and its ever-changing nature. The chapter also looked at domestic policy of the USA to fully understand the influence of a president in determining the direction a country takes in order to ensure cybersecurity for a country's citizens. Whereas the US domestic policy on cybersecurity is succinctly written, Kenya, it was observed, appears to be vague and very, if not entirely state-centric in its nature despite explaining that it exists in order to improve the lives of Kenyans.

Chapter four faced similar challenges, as far as Kenya is concerned, there is little to no information on Kenya's foreign policy on cybersecurity, which in itself is a risk, citing the interconnected nature of the cyberspace. However, citing Kenya's precedence to follow its colonial masters in line with the United Nations, there exists examples and paths that Kenya

can follow in order to achieve a foreign policy that is not only protective of its people but also the state. The UN has had major efforts to draft an international policy on cybersecurity, which has involved all the stakeholders involved, from the states, corporations and civil groups but as the clock ticks and more elaborate work and details required emerge, some states have appeared to either ignore the international policy or offer impediments to the work.

From the research in this paper there are important elements that emerge; and that are important in understanding how cybersecurity influences international peace and security. They include:-

1. Securitization of the Cyberspace

In 2012, US President Barrack Obama wrote that no entities had managed to destroy seriously or disrupt America's critical infrastructure networks. But foreign governments, criminal syndicates and lone individuals were probing USA's financial, energy and public safety systems every day, adding that cyber threats are one of the most alarming economic and national security tests facing USA. He wrote this as he sought to push for proper and strong legislation regarding cybersecurity, which he felt would strengthen USA's defence, especially digitally.[144] This is a perfect example of securitization of the cyberspace whereby securitization is constructed to include both traditional and modern aspects of security. Through the lenses of Ole Wæver et al, under the securitization theory, there is not distinct difference between real threat and perceived threat; and threat is dependent of the specific

[144] https://obamawhitehouse.archives.gov/the-press-office/2012/07/19/op-ed-president-obama-taking-cyberattack-threat-seriously Retrieved 09/08/2017

subject.[145] Ole Wæver et al specifically define the act of securitization as process that ranges from one subject to another through which understanding is constructed within a state to view something as an existing threat to a valued referent object, and to enable a call for urgent and exceptional measures to deal with the threat.[146] The group points out three elements that define securitization; securitization actor, referent object and an audience.

a. Securitization Actor

As far as cybersecurity is concerned the securitization actor is the state and/or state actors, whose role is to initiate and guide the transformation of a subject into a security matter. Ole Wæver et al say that the in order for the actor to securitize a subject, the process must be accompanied by a speech-act, which is a forte of state actors among them the president.[147] US President Obama's declaration that the threat of cyber-attack is one of the greatest challenges to security the USA faces, is one such example of how a state actor in this case the president uses speech to initiate the securitization process and action, by progressively seeking to enact legislation to securitize the cyberspace. This has further been internationalized under the UN, where the Group of Experts drawn from various states have sought to define the threat of cyber-attacks as a threat to international peace and security.[148]

Kenya is no exemption to the securitization of the cyberspace, whereby the national cybersecurity strategy 2014 was created in order to ensure that the country could respond

[145] Buzan, Barry, Ole Wæver, and de Wilde, Jaap, (1998) Security: A New Framework for Analysis. Boulder: Lynne Rienner Publishers.
[146] Buzan, Barry, Ole Wæver, and de Wilde, Jaap, (1998) Security: A New Framework for Analysis. Boulder: Lynne Rienner Publishers
[147] Ibid.
[148] https://obamawhitehouse.archives.gov/the-press-office/2012/07/19/op-ed-president-obama-taking-cyberattack-threat-seriously Retrieved 09/08/2017

adequately to these threats so that national priorities remain on course with the vision 2030, and is even termed as a priority item in the list.[149]

b. Referent Object

The referent object refers to that subject that the securitization actors needs to transform from just an ordinary matter to that of security concern and attention, and in this case it is the cyberspace.[150] Most nation-states have pointed out the cyberspace and all the activities within it as a number one priority citing the important role it has come to play in governance. Almost all governance, economic and social activities revolve around and within the cyberspace and it is no wonder US President Obama intimated that all American lives revolve around the cyber networks and thus the need for the US Senate to pass the cybersecurity act in order to protect the American citizens.[151] This is also applicable in the Kenyan case, with Kenya's National Cybersecurity Act solely dedicated to ensure the country achieves its Vision 2030 by eliminating all threats.[152]

c. Audience

The audience refers to the population that is required to be convincing of the vulnerability of the referent object, and the necessity of extraordinary measures in order to protect it.[153] In the case of cybersecurity, the audience is the national population or citizens of the individual state and this can extend globally to citizens of the world who have been convinced that the cyber-attack threat is potentially very dangerous.

---

[149] http://icta.go.ke/who-we-are/ Retrieved 30/07/2017
[150] Buzan, Barry, Ole Wæver, and de Wilde, Jaap, (1998) Security: A New Framework for Analysis. Boulder: Lynne Rienner Publishers
[151] https://obamawhitehouse.archives.gov/the-press-office/2012/07/19/op-ed-president-obama-taking-cyberattack-threat-seriously Retrieved 09/08/2017
[152] Ibid.
[153] Ibid.

2. Cyberspace as an emerging threat to the nation-state

The basic principles of realism uphold that the state is the central actor in international relations by emphasizing the persistent role of sovereignty and territoriality whereby the state is in a continuous fight for survival through the balance of power characterized by its military capabilities within the international system.[154] Under this theory, the state, which is viewed as the monopoly of force, seeks to increase its military capabilities and in doing so creates an anarchical international system.[155] Anarchy as Fearon explains causes commitment problems to alternatives in that whoever strikes first may have an upper hand and maybe compelled to do so seeking that advantage.[156] Another commitment problem of anarchy is the issue of declining versus rising state, whereby the declining state may wage way before it is discovered it is declining and in an attempt to avoid the slip or decline as it were, and in contrast the rising state may wage way to test its capability or to exact its hegemonic status. Anarchy according to Fearon, leads to war when one state's effort to make itself more secure is deemed a threat by other states, when it feels more insecure, especially in the absence of a central authority.[157]

In light of this, realists will continue to view states as the key legitimate and central actors within the international system despite the emergence of strong non-state actors such as giant corporations who wield cyber power and even cyber-criminal and even cyber terrorists who continue to challenge the state and its power in the international system.

---

[154] Waltz, Kenneth N. (2001), Man, the State and War: A Theoretical Analysis, 3rd edn. (New York: Columbia University Press).

[155] Bull, Hedley (1961), 'Disarmament and the Balance of Power', in Lawrence Freedman (1994), ed., War (Oxford and New York: Oxford University Press), Pp. 297-303.

[156] *Fearon, James.(1995) "Rationalist Explanations for War". International Organization.*

[157] Gilpin, Robert (1983), 'Hegemonic War and International Change', in Lawrence Freedman (1994), ed., War (Oxford and New York: Oxford University Press), pp. 94-95.

a. Cyber Corporations

The cyberspace is run as a business where corporations such as Internet Service Providers carry out the role. Uniquely so, the cyberspace is a combination of physical and virtual elements; the physical properties involve the economic laws and the political laws of sovereign states represented by governmental laws and control, and the virtual elements are economic networks, and political practices that make government jurisdictional control difficult. The corporates fall in the virtual sphere, in the sense that they do not want governmental guidance and control, while at the same time being run as businesses, which comply with laws of the nation-state.[158]

The push and pull between the State and corporations is best exemplified by the case between the US Government and Apple Inc., whereby the FBI needed the mobile technology firm to help its investigators access the phone used by a terrorist Syed Rizwan Farook, who had committed a mass shooting in San Bernardino, California, USA. Apple Inc.'s reason given for denying FBI access to the phone was that the request and/or its approval to do so infringed on human rights, specifically free speech, which is characterized by the password to access the phone. Apple Inc., also added that by handing over the bypass for the phone's password would be create a precedence whereby other nations would request the same in consequent cases, especially in China which is the second highest consumer of Apple Inc.'s product, the iphone; the company insists that it was not a business decision. The State argued that this was necessary in the fight against terrorists but other technology companies

[158] Nye, Joseph. (2016) 'The Regime Complex for Managing Global Cyber Activities'. Who Runs the Internet? The Global Multi-stakeholder Model of Internet Governance: Vol. II Centre for International Governance Innovation and the Royal Institute of International Affair. Ottawa, Canada

followed suit with the likes of Facebook, Amazon, Microsoft and Google filing lawsuits.[159] There have been instances whereby corporations carry out acts in cyberwarfare upon the request of a nation-state, either by being on a government contract or by more autonomous actions under the government's blessing.[160] Large multinational corporations have also found themselves on both sides during a cyber conflict, such as was the case in 2010 when Google's Chinese subsidiary was permanently moved from Mainland China to Hong Kong, after Chinese-originated cyber-attacks against Google and other U.S. corporations.[161]

Kenya has not been devoid such instances where the state is challenged by corporations; in 2017, the government through the Communication Authority of Kenya ordered telecommunications companies to give access in order for them to listen to calls, read text messages and review mobile money transactions; all done by a contracted company. There was a huge public outcry led by media houses, civil groups and even, hacktivists who hacked into CA's website to leave a message demanding the respect of human rights.[162]

5.2 The Way Forward

Kenya's case is not unique as far as cybersecurity and the challenges that come with it are concerned; the distinct feature is the level at which its technological advancements have reached and what aspects of daily life relies on the cyberspace. In relation to how Kenya relates with other nation-states in matters cybersecurity remains vague but need to be addressed;

---

[159] *United States v. Apple Inc.*, U.S. 12 Civ. 2862 (2013).

[160] Drew, C. and Markoff, J.,(2009) "Contractors Vie for Plum Work, Hacking for U.S.," The New York Times, May 30, 2009.

[161] Drummond, D.,(2010) "A new approach to China: an update," Google Official Blog.

[162] http://www.nation.co.ke/news/Government-likely-to-start-phone-tapping/1056-3816372-m5vnfx/index.html Retrieved on 08/08/2017

1. Kenya needs an elaborate Cybersecurity Act that explicitly outlines how the cyberspace is organized and run in Kenya; This can only be achieved if the government uses a multi-stakeholder approach, ensuring that a majority of stakeholders among them users, corporations, law enforcement and legal agencies are all involved.
2. Kenya should cooperate with other nations in a bid to ensure peace and security not only within her borders but also as a way of ensuring any outside threat can be handled under such an agreement.
3. Kenya can also explore a regime approach, as the hegemon in order to serve her interests adequately in a union of states that are within the same level of development. The East African Community is one such avenue, where Kenya as more advanced state can take charge of the process.
4. Kenya needs to seek diplomatic assistance from the more advanced states albeit cautiously to ensure her sovereignty is not compromised.
5. Kenya needs to broaden her technological knowhow whereby over 80% of its population have some basic knowledge of using technology.

Conclusion

This research had two suppositions; that states quest for cybersecurity can increase the likelihood of an insecure international system and that states can use a secure cyber space as a tool in international conflict management. It is evident that the securitization of the cyberspace is in itself a cause for alarm and that indeed a nation-state in its quest to achieve cybersecurity is bound to be perceived as aggression. From this research project, it is evident that even a defensive approach to achieving cybersecurity is still perceived as offensive; duly

so because most international policies by the states are secret in nature and other states seek to outdo the other. Here a matter of strategy and tactics come into play, whereby the state continues to grow its military capabilities by advancing in technology. Kenya like other less developed nations can and have been used as havens for cyber criminals thereby creating diplomatic tension between nations. A state's quest to achieving cybersecurity single handedly would also mean infringing on other states thereby creating an unstable international system. Therefore the idea of a state working together with others to achieve a secure cyber space is a form of international conflict management, which states should explore in a bid to ensure peace and security in the international system. The UN, as it is its role, has shown serious effort to ensure a peaceful international system through a collaborative approach, which involves as many of its members as possible, but just like its traditional core objectives there exists challenges.

APPENDICES

Appendix I

INTERVIEW GUIDE (SAMPLE)

I. Known and potential threats to Kenya's cybersecurity (Managerial staff in the population)

1. How would you describe your cyber knowledge, poor, good or very good?
2. Do you know the various threats to cybersecurity in your department?
3. Do you use untrusted/blocked websites with departmental computers and mobile phones? Yes or No.

   If yes, kindly list the websites.
4. Do you think these websites expose the department to cyber threats? Yes or No.

If yes, kindly elaborate on this

5. Do you share work related information with people working outside your office?

II. Measures in place to deal with cyber-attacks (IT Staff in the population)

1. What measures are in place to protect from cyber-attacks?
2. Does the department offer basic cyber skills to all employees?
3. What are the procedures in place once a cyber-attack is identified?
4. Has anyone been held accountable for leaked information? Yes or No.

   If yes, please elaborate

III. Efforts Kenya is making to ensure international peace in the cyberspace (Ministry of Foreign affairs officials)

1. Do you think proper cyber-security measures can be followed? Yes or No.

If yes, kindly explain how.

2. Do you think social media should be controlled in Kenya? Yes or no.

   If yes, kindly elaborate

3. Is there a foreign policy on cybersecurity in Kenya?
4. Do you think Kenya needs a dedicated foreign policy on cybersecurity?

Appendix II

QUESTIONNAIRE (SAMPLE)

Instructions: Please put a tick ☑ in the box next to the answer of your choice or write in the space provided as the case maybe.

Sex

Male ☐ Female ☐

Age

☐ 18-25 ☐ 26-35 ☐ 36-45 ☐ 46-55

Level of Education

☐ High School ☐ Diploma ☐ Degree ☐ Masters

☐ PhD

PART I (Potential Threats)

1. What technological device do you connect to the office network with?

   ☐ Computer ☐ Laptop ☐ Tab ☐ Mobile Phone

2. How many hours a day are you online?

   ☐ 1-2 ☐ 3-4 ☐ 4-5 ☐ Over 6 hours

3. Do you share your password with anyone?

   Yes ☐ No ☐

4. Do you ever leave your device unattended?

   Yes ☐ No ☐

5a. If yes, for how long?

5. Do you use company devices outside the office?

Yes ☐ No ☐

6. Has any suspicious person approached you about your work online?

Yes ☐ No ☐

7a. If yes, who?

7b. If yes, did you report?

Yes ☐ No ☐

PART II (Dealing with cyber attacks)

7. How many times do you change your network password?

☐ Often ☐ Occasionally ☐ Rarely ☐ Never

8. Who do you report to when faced with technological challenges?

☐ Workmate ☐ Superior ☐ IT department ☐ Other

If other, please specify who?

9. Do you know what to do if company devices are stolen?

Yes ☐ No ☐

10. Would you know a cyber-threat if you encountered one?

Yes ☐ No ☐

PART II (Cybersecurity for international peace & security)

11. Can war be caused by conflicts in the cyberspace?

Yes ☐ No ☐

12. Should the government control social media and websites?

Yes ☐ No ☐

13. Should the government block terror group sites and social media pages?

Yes ☐ No ☐

14. Do you know Kenya's foreign policy on cyber-related issues?

Yes ☐ No ☐

15. Do you think a safe and secure cyberspace leads to a peaceful world?

Yes ☐ No ☐

16. Is cybersecurity achievable?

Yes ☐ No ☐

If other, please suggest how?

BIBLIOGRAPHY

Avoine, Gildas; Pascal Junod; Philippe Oechslin (2007). Computer system security: basic concepts and solved exercises. EFPL Press.

Bull, Hedley (1961), 'Disarmament and the Balance of Power', in Lawrence Freedman (1994), ed., War (Oxford and New York: Oxford University Press), Pp. 297-303.

Buzan, Barry, Ole Wæver, and de Wilde, Jaap, (1998) Security: A New Framework for Analysis. Boulder: Lynne Rienner Publishers

Carr, David and Somaiya, Ravi, (2013) "Assange, back in news, never left U.S. radar", *The New York Times*.

Clark, Jim (1999). Netscape Time. St. Martin's Press.

Clarke, Richard A. and Robert Knake. Cyber War : The Next Threat to National Security and What To Do About It. Ecco, April 2010.

Critical Infrastructure Protection in Homeland Security: Defending a networked nation 2nd edition By Ted G. Lewis Published by Wiley

Dressler, J. (2007). "United States v. Morris". Cases and Materials on Criminal Law. St. Paul, MN: Thomson/West.

Drew, C. and Markoff, J.,(2009) "Contractors Vie for Plum Work, Hacking for U.S.," The New York Times, May 30, 2009.

Drummond, D.,(2010) "A new approach to China: an update," Google Official Blog.

Fearon, James.(1995) "Rationalist Explanations for War". International Organization.

Finn, Peter; Horwitz, Sari (2013). "U.S. charges Snowden with espionage". *The Washington Post*.

Fischer, Eric. "Cybersecurity and Information Sharing: Comparison of H.R. 1560 (PCNA and NCPAA) and S. 754 (CISA)." Report to Congressional Committees. Congressional Research Service, November 6, 2015. Federation of American Scientists Project on Government Secrecy. https://www.fas.org/sgp/crs/misc/R44069.pdf.

Freyberg-Inan, Annette What Moves Man: The Realist Theory of International Relations and Its Judgment of Human Nature, SUNY Press, 2004

Gibson, W. (1984) *Neuromancer.* New York, Ace Books.

Gilliam, David P., Thomas L. Wolfe, and Josef S. Sherif, "Software Security checklist for the life cycle." Proceedings of the Twelfth IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE '03), IEEE Computer Society.

Gilpin, Robert (1983), 'Hegemonic War and International Change', in Lawrence Freedman (1994), ed., War (Oxford and New York: Oxford University Press).

Glenny, Misha; Glick, Bryan; Hyppönen. Mikko H.; Wainwright, Robert(2010), Cybercrime, cybersecurity and the future of the internet, Session Handouts, Global Economic Symposium 2010 (GES), 27-29 September 2010, Istanbul, Turkey

Gregory S. McNeal (2014). "Controversial Cybersecurity Bill Known As CISA Advances Out Of Senate Committee". Forbes.

Grossman, Elaine (2009). "JASON Panel Offers Secret Nuclear Warhead Upkeep Recommendations". Global Security Newswire.

Haaster, Jelle Van; Gevers, Rickey; Sprengers, Martijn (2016). Cyber Guerilla. Syngress..

Halacy, Daniel Stephen (1970). Charles Babbage, Father of the Computer. Crowell-Collier Press.

Henry Quarshie and Alexander Martin-Odoom, "Fighting Cybercrime in Africa", Computer Science and Engineering, vol. 2, No. 6 (2012).

Herz, J.H., Political Realism and Political Idealism: A Study in Theories and Realities (Chicago:University of Chicago Press, 1951)

Jack Schofield (2016). "How can I remove a ransomware infection?". The Guardian.

https://www.f-secure.com/v-descs/trojan_w32_reveton.shtml

John J. Mearsheimer: An Offensive Realist Between Geopolitics & Power, Institut for Statskundskab, Københavns Universitet, 2003

John Mearsheimer,(1994) "The False Promise of International Institutions," International Security, Vol. 19, No. 3.

Journal of Homeland Security and Emergency Management Volume 3, Issue 4 2006 Article 3 Cybersecurity: From Ad Hoc Patching to Lifecycle of Software Engineering Clyde G. Chittister Yacov Y. Haimes 2006 The Berkeley Electronic Press

Karnouskos, Stamatis. "Stuxnet worm impact on industrial cyber-physical system security." In *IECON 2011-37th Annual Conference on IEEE Industrial Electronics Society*, pp. 4490-4494. IEEE, 2011.

Keohane R.O. and Nye, J.S. Power and Interdependence 3rd ed. Longman Classics 1977

Kigen, P., C. Kisutsa, C. Muchai, K. Kimani, M. Mwangi & B. Shiyayo. 2014. "Kenya Cyber Security Report 2014: Rethinking Cyber Security – "An Integrated Approach: Processes, Intelligence and Monitoring."

Lee, Newton (2013). Counterterrorism and Cybersecurity: Total Information Awareness. Springer.

Lewis, James. (2002). Center for Strategic and International Studies. Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats. Washington, D.C. USA.

Marg, Max. "The Future of the Internet: Who Should Govern It and What Is at Stake for You? A Multistakeholder Dialogue." Thinktank. Internet Democracy Project, n.d. Mello, Susan M. (1993) *Administering the Antidote to Computer Viruses: A Comment on Metcalf, John 2014. "Core War: Creeper & Reaper"*

Mollenhoff, Clark R. (1988). Atanasoff: Forgotten Father of the Computer. Ames, Iowa: Iowa State University Press

Nicholson, M. (1992) Rationality and the Analysis of International Conflict (Cambridge 12 University Press)

Nye Jr, Joseph S. —Cyberpower. Paper. Cambridge, Mass.: Harvard Belfer Center for Science and International Affairs, May 2010.

Nye, Joseph. (2016) 'The Regime Complex for Managing Global Cyber Activities'. Who Runs the Internet? The Global Multi-stakeholder Model of Internet Governance: Vol. II Centre for International Governance Innovation and the Royal Institute of International Affair. Ottawa, Canada

Olenick, Doug. "U.S. Cyber Command Sets Priorities for the Nations Defense." SC Magazine, September 9, 2015. http://www.scmagazine.com/news/cyber-command-capabilitiesshould-be-integrated-into-us-cybersecurity-efforts/article/437636/.

Ottis, R. & Lorents, P. (2010). Cyberspace: Definition and Implications. In Proceedings of the 5th International Conference on Information Warfare and Security, Dayton, OH, US, 8-9 April. Reading: Academic Publishing Limited.
Purser, Steve (2014). "Standards for Cyber Security". *IOS Press*.

Ramzan, Zulfikar (2010). "Phishing attacks and countermeasures". In Stamp, Mark & Stavroulakis, Peter. Handbook of Information and Communication Security. Springer.
Red October' cyber-attack found by Russian researchers' www.bbc.com 14 January 2013

Shalhoub, Z.K. & Al Qasimi, S.L. Cyber Law and Cyber Security in Developing and Emerging Economies. 2010 Edward Elgar
The Ponemon Institute, "The Risk of Insider Fraud: Second Annual Study." February 2013
UN General Assembly, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," A/68/98, June 24, 2013
UN Institute for Disarmament Research (UNIDIR), "The Cyber Index: International Security Trends and Realities," UNIDIR/2013/3 (2013).
Waltz, Kenneth N. (2001), Man, the State and War: A Theoretical Analysis, 3rd edn. (New York: Columbia University Press).
Waltz, Kenneth. 1979. Theory of International Relations. New York: Random House.

Wegener, Henning. —Cyber Peacel, in The Quest for Cyber Peace. International Telecommunication Union and World Federation of Scientists, January 2011.

Young, A.; M. Yung (1996). Cryptovirology: extortion-based security threats and countermeasures. IEEE Symposium on Security and Privacy.
Ramirez, Jessica (8 March 2010). "The History of Computer Hacking". Newsweek.
Marete, G. (2011, June 5). Aeromarine. http://www.aeromarine.co.ke

Barb Darrow (24 Sep 2015). "Apple, Microsoft, others slammed for supporting cybersecurity bill". Fortune.

Other Resources

"Mobile ransomware use jumps, blocking access to phones". PCWorld. IDG Consumer & SMB.

'Hackers Struck Computers In Canadian Government.' page A8 February 18, 2011 The New York Times

"77 Chinese held in cyber bust" Daily Nation P. 4, December 3, 2014

Convention on Cybercrime, Budapest, 23 November 2001

http://allafrica.com/stories/201407210683.html

http://aptantech.com/2017/04/lazarus-group-malware-samples-were-detected-in-it-networks-of-kenyan-firms-kaspersky/

http://bush.tamu.edu/research/capstones/mpia/Engel_Spring2011.pdf

http://freebeacon.com/national-security/chinese-hackers-suspected-in-cyber-attack-on-council-on-foreign-relations/

http://icta.go.ke/who-we-are/

http://icta.go.ke/who-we-are/

http://kenyalaw.org/kl/fileadmin/pdfdownloads/AmendmentActs/2013/KenyaInformationandCommunications_Amendment_Act2013.pdf

http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf

http://serianu.com/downloads/KenyaCyberSecurityReport2015.pdf

http://usa.kaspersky.com/internet-security-center/definitions/what-is-cyber-security#.VlRdSb_6_IU

http://www.biztechafrica.com/article/cybercriminals-target-african-countries-ransomware/12064/

http://www.businessdailyafrica.com/corporate/Cyber-crimes-open-window-for-IT-firms/539550-1998058-4amfcd/index.html

http://www.businessdailyafrica.com/corporate/Kenyan-firms-hit-by-ransomware-cyber-attack/539550-3928322-uwqsnq/

http://www.business-standard.com/article/companies/4-ways-to-address-the-net-neutrality-issue-115071600492_1.html Mansi Taneja | New Delhi July 16, 2015
http://www.capitalfm.co.ke/business/2015/11/e-government-tightens-noose-on-corrupt-rent-seeking-public-officials/
http://www.cio.co.ke/news/main-stories/103-Government-of-Kenya-websites-hacked-overnight
http://www.computerworld.com/article/2575156/security0/phishing.html retrieved on 03/07/2017
http://www.itu.int/en/mediacentre/Pages/2016-PR30.aspx
http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf
http://www.kachwanya.com/2014/03/11/m-pesa-fraud/
http://www.ke-cirt.go.ke/index.php/about-us/
http://www.ke-cirt.go.ke/index.php/petya-ransomware-v0-3-national-ke-cirt-cc-report/
http://www.ke-cirt.go.ke/index.php/services/national-pki/
http://www.nation.co.ke/news/14--cases-of-ransomware-attacks-in-Kenya/1056-3930394-8eq5g4z/index.html
http://www.nation.co.ke/news/Government-likely-to-start-phone-tapping/1056-3816372-m5vnfx/index.html
http://www.nation.co.ke/news/Police-bust-ring-of-hackers/1056-3842558-11h7q5xz/
http://www.oecd.org/sti/ieconomy/security.htm
http://www.reuters.com/article/us-cyber-northkorea-exclusive-idUSKCN18H020
http://www.serianu.com/downloads/KenyaCyberSecurityReport2014.pdf
http://www.spamfighter.com/News-18517-In-Kenya-Cyber-attacks-and-E-threats-Surged-Sharply-says-TESPOK.htm
http://www.serianu.com/downloads/KenyaCyberSecurityReport2016.pdf
http://www.tespok.or.ke/reports/Q3-2013/Cyber%20Threat%20Trends%20Report_Q3.pdf
http://www.theeastafrican.co.ke/news/How-cyber-crime-complicates-war-on-terror/2558-2422854-13ja90iz/index.html
http://www.un.org/en/development/desa/news/ecosoc/cybersecurity-demands-global-approach.html

http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98

http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174

http://www.vision2030.go.ke/enablers-macros/

https://blog.kaspersky.com/mobile-ransomware-2016/12491/

https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/new%20bill%20summary%20pdf.pdf

https://internetdemocracy.in/events/the-future-of-the-internet-who-should-govern-it-andwhat-is-at-stake-for-you-a-multistakeholder-dialogue/

https://jsis.washington.edu/wordpress/wp-content/uploads/2016/06/Task-Force-E-Report-2016-Beyer.pdf

https://moneyandmarkets.co.ke/kenyan-banks-among-victims-fileless-malware-attacks/

https://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx Retrieved 28/06/2017

https://obamawhitehouse.archives.gov/the-press-office/2012/07/19/op-ed-president-obama-taking-cyberattack-threat-seriously

https://obamawhitehouse.archives.gov/the-press-office/2012/07/19/op-ed-president-obama-taking-cyberattack-threat-seriously

https://theforeignpolicyanalyst.wordpress.com/tag/kenya-foreign-policy/

http://www.mfa.go.ke/wp-content/uploads/2016/09/Kenya-Foreign-Policy.pdf

https://www.sbs.ox.ac.uk/cybersecuritycapacity/system/files/Harmonizing%20cyberlaws%20-%20East%20Africa%20Community%20.pdf

https://threatpost.com/inside-aurora-google-attack-malware-011910/73395/ Retrieved on 03/07/2017

https://threatpost.com/large-scale-water-holing-attack-campaigns-hitting-key-targets-092512/77045/

https://us.norton.com/cybercrime-phishing retrieved on 03/07/2017

https://us.norton.com/spear-phishing-scam-not-sport/article

https://usa.kaspersky.com/resource-center/threats/botnet-attacks

https://www.cfr.org/blog/development-cyber-norms-united-nations-ends-deadlock-now-what

https://www.csmonitor.com/USA/2017/0628/How-Russia-and-others-use-cybercriminals-as-proxies

https://www.extension.harvard.edu/inside-extension/how-cyberspace-transforming-international-security
https://www.ncsc.gov.uk/content/files/protected_files/guidance_files/common_cyber_attacks_2016.pdf
https://www.paloaltonetworks.com/cyberpedia/what-is-a-ddos-attack
https://www.sagedatasecurity.com/blog/seven-characteristics-of-a-successful-information-security-policy
https://www.scmagazineuk.com/trump-announces-15bn-for-cyber-security-and-critical-infrastructure/article/645005/
https://www.securityforum.org/news/cyber-resiliencebrand-reputation/
https://www.standardmedia.co.ke/business/article/2001233552/man-charged-with-hacking-kra-and-causing-sh4b-loss
https://www.standardmedia.co.ke/m/article/2001232241/how-kenyan-banks-lost-sh30-billion-in-two-years-to-tech-savvy-criminals
https://www.standardmedia.co.ke/mobile/?articleID=2000174969&story_title=state-to-set-up-unit-to-protect-critical-infrastructure Paul Wafula | Wednesday, Sep 2nd 2015
https://www.state.gov/s/cyberissues/releasesandremarks/272175.htm
https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/reports/critical-infrastructures-west-hemisphere.pdf
https://www.wired.com/2015/04/hacker-lexicon-spear-phishing/
Norton Cybercrime Report, September 2012. http://www.norton.com/2012cybercrimereport

Symantec Corporation, Internet Security Threat Report 2013, 2012 Trends, Volume 18 (April, 2013). Available from www.symantec.com/content/en/us/enterprise/other_resources/bistr_main_report_v18_2012_21291018.en-us.pdf.

The critical infrastructure protection bill, 2015
United States v. Apple Inc., U.S. 12 Civ. 2862 (2013).
United States v. Morris 19 Rutgers Computer & Tech.