

UNIVERSITY OF NAIROBI
THE DEPARTMENT OF DIPLOMACY AND INTERNATIONAL STUDIES

IMPLEMENTATION OF UN CYBER NORMS IN THE PROMOTION OF
INTERNATIONAL SECURITY:
A CASE STUDY OF KENYA.

TIMOTHY OTHIENO WERE

REG NO. R50/39051/2021

RESEARCH PROJECT SUBMITTED IN PARTIAL FULFILMENT OF THE
REQUIREMENT FOR THE AWARD OF
DEGREE OF MASTERS OF ARTS IN INTERNATIONAL STUDIES

December 2021



DECLARATION

A declaration is hereby made that this is my original research project and has not been submitted for any award in any other institution of higher learning.

Signature.......... Date..... 25 Nov 2021

Timothy Othieno Were

The research project has been submitted for examination with my approval as the University of Nairobi supervisor.

Signature.......... Date..........

Prof Ambassador Maria Nzomo, PhD

Supervisor

DEDICATION

This work is dedicated to my family, colleagues at the National Defence College, Karen course no. 23 of 2020/2021, Dr Kate Getao and Dr Martin Koyabe of the GFCE. I am grateful for their encouragement and support during this journey.

ACKNOWLEDGEMENT

This study would not have been possible without the guidance and direction of my supervisor, Prof. Maria Nzomo. I also acknowledge the valuable input of the Commandant National Defence College - Kenya, Lt Gen Adan Mulata, Maj Gen R A Elmi, Senior Directing Staff - Air, at the National Defence College, Senior Directing Staff, the entire faculty, and my fellow participants for the support and guidance in writing this paper.

LIST OF ABBREVIATIONS

AMISOM	African Union Mission in Somalia
AU	African Union
CA	Communications Authority of Kenya
CBMs	Confidence Building Measures
CCDCOE	Cooperative Cyber Defense Center of Excellence
COMESA	Common Market for Eastern and Southern Africa
DPA	Data Protection Act
GDPR	(European) General Data Protection Regulations
GGE	UN Group of Governmental Experts
ICANN	Internet Corporation for Assigned Names and Numbers
ICT	Information and Communication Technology
ICTA	Information and Communication Technology Authority
IRT	International Regime Theories
ITU	International Telecommunications Union
MIIYA	Ministry of ICT, Innovation and Youth Affairs
NATO	North Atlantic Treaty Organization
NC3	National Cyber Command Centre
OECD	Organisation for Economic Cooperation and Development
OSCE	Organization for Security and Co-operation in Europe
TESPOK	The Telecommunications Service Providers of Kenya
TT	Technology Transfer
UNIDIR	United Nations Institute for Disarmament Research
UNODA	United Nations Office for Disarmament Affairs
UNODC	United Nations Office on Drugs and Crime
UNOTC	United Nations Office of Counter-Terrorism
WSIS	World Summit on the Information Society

DEFINITION OF TERMS

Critical ICT Infrastructure – “an electronic communications network, information system or a group of information systems where an incident that occurs causes or may cause grave damage to national security, national economy or social well-being” - <https://www.vkontrole.lt/failas.aspx?id=3504>

Cyberspace – “the name given to the global and dynamic domain composed of the infrastructures of information technology - including the Internet - networks and information and telecommunications systems, has blurred borders, involving their users in unprecedented globalisation that provides new opportunities but also entails new challenges, risks and threats” - www.oecd.org

Digital Divide – “refers to the gap between demographics and regions that have access to modern information and communications technology (ICT) and those that do not or have restricted access. This technology can include the telephone, television, personal computers and internet connectivity” – techtargget.com.

Electronic Pearl Harbour – “the potential for an event that could compromise the operations of critical infrastructures across large areas of an organisation, community, state or nation” - <https://www.un.org/securitycouncil/ctc/sites/>

Techno Nationalism - “a mercantilist behaviour that links a nation’s tech capabilities and enterprise with issues of national security, economic prosperity, and social stability” - hinrichfoundation.com

ABSTRACT

Humanity has been transformed by development and innovation in the Information and Communication Technology (ICT) field. Indeed, we are now talking of the fourth industrial revolution driven by ICTs and the connectivity to Cyberspace. Cyberspace has been touted as one of the most significant intellectual challenges in the third millennium. It is not clear who is in charge and who will be in charge in the future. In the not too distant past, experts looked at cyber security as mainly a technical risk. Today, it is dealt with at the highest level of government as a critical national security challenge.

UN member states have gradually united around an agenda of responsible state behaviour in Cyberspace. International discussions point to “*cyber norms of behaviour*” as being appropriate means for directing the behaviour and actions of states in Cyberspace – with the aim is to increase predictability and stability and foster trust in the utilisation of ICTs and manage misunderstandings that may result in conflicts. Eight of the eleven norms could be considered positive duties – recommend states to take a particular action while three are negative, restraining specific behaviour. Protection of critical infrastructure and cooperation are covered by several of the norms, pointing to the emphasis laid by the UN Group of Governmental Experts.

This study examined Kenya’s implementation of the UN Cyber norms in promoting international security. The research study gap pointed to a lack of knowledge and non-adherence to the said norms. The existing literature addresses norm implementation in the context of the developing nations in the pre-COVID 19 era but hardly speaks to what is happening in the developing world. The study made the argument that the UN Cyber Norms promote international security by giving safeguards against cyber-attacks and fostering cyber security and stability. The study was steered by the International Regime Theories (IRT) that indicate that cooperation is possible in a setting with no higher authority to force the nations to cooperate.

This study found out that there is an increasingly critical role of information and communications technologies in the Kenyan national security, economy, critical infrastructures (such as finance, transportation, water and food supplies, public health, energy, emergency services) and civil society, more so in the post-COVID 19 dispensations. It also confirms that the Cyber Norms, if followed, would result in a more stable and safer Cyberspace, thus enhancing international security. There is a need to move from Norms to an actual convention anchored on International Law to address Cyberspace matters.

In terms of academic gain – there is a need to develop a theoretical framework to address the Cyberspace phenomenon, specifically cyber relations. Working together with the Private sector and Government Agencies, capacity building for cyber professionals needs to be fast-tracked. For Policymakers, identification, classification, and protection of critical information infrastructure are paramount, as is the enactment of the Critical Infrastructure Protection law. There is also a thin line between self-defence and interference with hostile nations’ critical infrastructure, as seen in the Kenya-Somalia tiff. Additional investment in cyber deterrence, expansion of the legal and policy framework, certification of ICT equipment, bilateral and multilateral cooperation as far as cyber relations are concerned (mutual legal assistance), national awareness campaigns and private sector disclosure of successful and attempted attacks must be ramped up significantly.

TABLE OF CONTENTS

DECLARATION	i
DEDICATION	ii
ACKNOWLEDGEMENT	iii
LIST OF ABBREVIATIONS	iv
DEFINITION OF TERMS	v
ABSTRACT.....	vi
TABLE OF CONTENTS.....	vii
TABLE OF FIGURES	ix
TABLE OF TABLES	ix
CHAPTER ONE	1
1.0 BACKGROUND OF THE STUDY	1
1.1 PROBLEM STATEMENT	5
1.2 RESEARCH QUESTIONS.....	7
1.3 OBJECTIVES OF THE RESEARCH	8
1.4 RESEARCH HYPOTHESES	8
1.5 JUSTIFICATION OF THE STUDY	9
1.6 LITERATURE REVIEW	10
1.6.1 NORMS	11
1.6.2 UN GROUP OF GOVERNMENTAL EXPERTS.....	13
1.6.3 UN GGE NORMS	15
1.6.4 NATO	20
1.6.5 INTERNATIONAL TELECOMMUNICATIONS UNION (ITU)	21
1.6.6 MULTILATERAL AND BILATERAL ARRANGEMENTS	22
1.6.7 PRIVATE SECTOR	24
1.7 THEORETICAL FRAMEWORK	26
1.8 METHODOLOGY OF STUDY	27
1.8.1 RESEARCH DESIGN	27
1.8.2 RESEARCH SITES	28
1.8.3 TARGET POPULATION.....	28
1.8.4 SAMPLE SIZE	29
1.8.5 SAMPLING TECHNIQUES	29
1.8.6 DATA COLLECTION	29
1.8.7 QUESTIONNAIRE	30
1.8.8 IN-DEPTH INTERVIEWS	30
1.8.9 DATA ANALYSIS.....	31
1.8.10 INSTRUMENT VALIDITY.....	31
1.8.11 INSTRUMENT RELIABILITY	32
1.8.12 LEGAL AND ETHICAL CONSIDERATIONS	32
1.9 LIMITATION AND ASSUMPTIONS.....	33
1.10 CHAPTERS OUTLINE.....	33
CHAPTER TWO - LEVEL OF AWARENESS OF EXISTING AND EMERGING THREATS IN CYBERSPACE GLOBALLY	35
2.0 INTRODUCTION	35
2.1 DEVELOPMENT OF CYBERCRIME	35
2.2 EMERGING THREATS.....	37
2.3 CRITICAL INFRASTRUCTURE THREATS	39

2.4	ICT VULNERABILITIES.....	42
2.5	CHALLENGE OF ATTRIBUTION.....	43
2.6	SUMMARY.....	45
CHAPTER THREE - CONFIDENCE-BUILDING MEASURES FOR COLLABORATION AND COOPERATION		48
3.0	INTRODUCTION	48
3.1	CONFIDENCE-BUILDING MEASURES	48
3.2	COOPERATION AMONGST STATES AND PRIVATE SECTOR	49
3.3	PROTECTION OF CRITICAL INFORMATION INFRASTRUCTURES.....	53
3.4	SUPPLY CHAIN INTEGRITY.....	56
3.5	AUTHORIZED EMERGENCY RESPONSE TEAMS.....	58
3.6	CAPACITY BUILDING	59
3.7	SUMMARY.....	61
CHAPTER FOUR - KENYAN LEGAL AND POLICY FRAMEWORK AND ITS EFFECTIVENESS		66
4.0	INTRODUCTION	66
4.1	INTERNATIONAL LAW	66
4.2	INTERNATIONALLY WRONGFUL ACTS ATTRIBUTABLE TO STATES	67
4.3	RESPECT FOR HUMAN RIGHTS	71
4.4	LEGAL ENVIRONMENT	72
4.5	SUMMARY.....	75
CHAPTER FIVE – RESEARCH FINDINGS AND ANALYSIS.....		77
5.0	INTRODUCTION	77
5.1	FINDINGS.....	77
5.11	DEMOGRAPHICS.....	77
5.12	AWARENESS AND GLOBAL CULTURE OF CYBER SECURITY	79
5.13	COLLABORATION AND COOPERATION.....	84
5.14	LEGAL AND POLICY FRAMEWORKS	87
5.2	ANALYSES AND INTERPRETATION	91
CHAPTER SIX - CONCLUSION AND RECOMMENDATIONS.....		94
6.1	SUMMARY OF FINDINGS	94
6.2	DISCUSSIONS.....	94
6.3	CONCLUSION AND RECOMMENDATIONS.....	95
BIBLIOGRAPHY/REFERENCE.....		99
APPENDICES		106
APPENDIX 1: QUESTIONNAIRE.....		106
APPENDIX 2: KEY INFORMANT INTERVIEW GUIDE		112
APPENDIX 3: NACOSTI LICENSE.....		115
APPENDIX 4: TARGET INSTITUTIONS.....		117
APPENDIX 5: INTERNATIONAL CODE OF CONDUCT FOR INFORMATION SECURITY		118
APPENDIX 6: RESOLUTION 70/237.....		121
APPENDIX 7: RESOLUTION 55/63.....		124

TABLE OF FIGURES

Figure 1 Experts' Countries (Source, Digital Watch 2021)	15
Figure 2 Escalation of cyber events and applicable legal frameworks and opportunity space for cybersecurity norms (Source Microsoft Corporation, 2015)	25
Figure 3 Significance of target vs. sophistication of attacker (Source Sales, 2013).....	70
Figure 4 Respondents' Gender Distribution (Source Author,2021).....	78
Figure 5 Respondents' Level of Education (Source Author, 2021)	78
Figure 6 Respondent's Role in Cyber Security (Source Author, 2021)	78
Figure 7 National Cyber Strategy Implementation (Source Author, 2021).....	83
Figure 8 Alignment of National Cyber Strategy with Regional and International Initiatives (Source Author, 2021)	84
Figure 9 Public-Private Cooperation (Source, Author 2021)	84
Figure 10 Collaboration Arrangements (Source Author, 2021)	85
Figure 11 Network and Processes of International Cooperation (Source, Author 2021)	86
Figure 12 Government - Industry Collaboration for Policy Development (Source, Author 2021)	87
Figure 13 Level of Understanding of Cybercrime Issues (source, Author, 2021).....	89
Figure 14 Adequacy of Legal Codes and Authorities in addressing challenges of cyber space (Source, Author 2021)	89

TABLE OF TABLES

Table 1 Importance of Cyber Security in various sectors (Source, Author 2021).....	79
Table 2 Sector Legal Framework (Source Author, 2021).....	88

CHAPTER ONE

1.0 BACKGROUND OF THE STUDY

Our lives have been eternally changed by Information and Communication Technology (ICT). We now enjoy increased productivity, innovation and sharing of ideas. Humanity has been transformed – indeed, we are now talking of the fourth industrial revolution that ICTs and the connectivity to cyberspace drive. On the dark side of Cyberspace, both non-state and state actors utilise it as a launchpad for aggressive behaviour with a view to crippling critical infrastructure (physical and virtual), destroying, altering or stealing data and undermining institutions and governments. There exist records of several international incidents with devastating consequences.

At the end of January 2003, resolution 57/239 of United Nations entitled “Creation of a global culture of cybersecurity” was agreed upon by the General Assembly asking owners and operators of internet systems and technologies to take cognisance of the cyber security risks as far as their roles were concerned, and asked relevant international organisations and the Member States to develop a culture of cybersecurity.¹

Following this, there has been a push for guidance by global rules-based arrangements to direct behaviour in Cyberspace, with discussions taking place over the last ten years. UN member states have progressively united around a structure of accountable state behaviour in cyberspace that is still evolving. The norms have been established by Groups of Governmental Experts (GGE) appointed by the UN with incremental reports adopted in 2010, 2013, and 2015 – and affirmed by the general

¹ Maarten Van Horenbeeck, Ed., “Cybersecurity Culture, Norms and Values: Background Paper to the IGF Best Practices Forum on Cybersecurity.,” *Internet Governance Forum Best Practices Forum on Cybersecurity* (2018).

assembly. The program “supports the international rules-based order, affirms the applicability of international law to state-on-state behaviour, faithfulness to voluntary norms of responsible state behaviour in peacetime, and the development and implementation of practical confidence-building measures to help reduce the risk of conflict stemming from cyber incidents.”²

As a responsible state that upholds global rules-based order, Kenya appreciates its duty in preserving the gains of an open, unrestricted, and safe cyberspace - for the foreseeable future. This study analyses the country’s compliance to the framework and its contribution to promoting Kenya’s ability to offer protection to its ICT space from considerable negative, unsettling, or otherwise destabilising cyber activity as it facilitates international security.

The current technological age is referred to as the “Fourth Industrial Revolution (4IR)” that is demonstrated by the amalgam of the physical and biological to the digital realms, in addition to the increasing application of emerging technologies, for instance, blockchain, robotics, artificial intelligence, 3D printing, cloud computing, advanced wireless systems and the Internet of Things (IoT), to mention but a few - ushering in a new age of innovative development and growth.³

Nevertheless, this adoption of 4IR also comes with disruption with uncertain consequences for the world. Serious cyber-attack incidents have shaken several states globally, most notably Estonia (2007), Georgia (2008), Iran (2010), and even the USA has had several attacks. Like other modes

² “USA and 26 Countries Issue Joint Statement on Responsible Behaviour in Cyberspace 23” (Digital Watch-Geneva Internet Platform, September 2019), <https://dig.watch/updates/usa-and-26-countries-issue-joint-statement-responsible-behaviour-cyberspace>.

³ Njuguna Ndung’u and Landry Signé, “The Fourth Industrial Revolution and Digitization Will Transform Africa into a Global Powerhouse,” *Foresight Africa 2020* (Washington DC: The Brookings Institution, January 8, 2020), <https://www.brookings.edu/research/the-fourth-industrial-revolution-and-digitization-will-transform-africa-into-a-global-powerhouse/>.

of war, cyber technology can be deployed against military facilities/forces and target noncombatant civilians. ICT has come up with a new method of fighting that has proven exceptionally difficult to contain, let alone overcome.⁴ Furthermore, as a result of this, the developed world seems to be preparing for possible fallout.

The 2010 disclosure of *Stuxnet* as one of the world's earliest cyberweapons that attacked the Iranian nuclear enrichment industry complex has raised concerns about whether the computer world can act as a deterrent to stop nuclear proliferation. This development has exposed the susceptibilities of industrial setups worldwide and alerted industrialists, governments and academicians to “position cyberspace within the international political system and explore ways to deal with its associated challenges”. It should be noted that for every cyber-attack, the attacker risks supplying missiles to the enemy as a design to work out their cyber weapons.⁵

The USA Policy Review indicates that: “Cyberspace touches virtually everything and everyone. It provides a pedestal for innovation and prosperity and the means to improve general welfare around the globe. However, with the broad reach of a loose and lightly regulated digital infrastructure, great risks threaten nations, private enterprises, and individual rights.”⁶ The US Cyber Command’s primary mission is the protection of the USA’s military cyber networks, but they are also ready to spring offensive cyber-attacks on prospective adversaries. The attacks can potentially reach out

⁴ B. M. Mazanec, *Cyber War: International Norms for Emerging-Technology Weapons* (Nebraska: Potomac Books, 2015).

⁵ J. Kremer and B. (Eds.) Müller, *Cyberspace and International Relations: Theory, Prospects and Challenges* -, 2014, Editors: www.springer.com.

⁶ Office of the Press Secretary, “Remarks by The President on Securing Our Nation’s Cyber Infrastructure” (White House, Washington DC, May 29, 2009), <https://obamawhitehouse.archives.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure>.

from cyberspace into the physical world, resulting in disruptions including; weapons malfunction, high voltage transmission lines, electrical generators and gas pipeline explosions, train derailments and aircraft crashes, funds ‘disappearance’ - “This is likely to be the twenty-first-century warfare.”⁷

In its policy outlook, the United Nations Economic Commission for Africa concludes that “measuring the magnitude of challenges posed by lack of adequate cyber defence is complex.” Cyberattacks are, unsurprisingly, transnational. Tackling them, therefore, necessitates coordinated and single-minded policies. The wide array of the issues and the diversity of dimensions, including political, sociocultural, economic and financial, scientific and technological, underline the complexity of cybersecurity.⁸

There has been an accord towards “norms of responsible state behaviour in cyberspace” through consensus by the UN-backed Group of Governmental Experts (GGE) in the meetings held in 2015 and earlier in 2010, 2013. The norms reached by consensus are an essential “contribution to establishing how international law applies in cyberspace.” Cyberspace is a vital element of protecting critical infrastructure and a crucial foundation for online electronic social and economic activity. States must reiterate their dedication to open, free, secure and peaceful cyberspace.

International discussions point to “cyber norms” or “cyber norms of behaviour” as an appropriate means for directing the behaviour and activities of state actors in cyberspace to increase

⁷ R. Clarke, “War from Cyberspace,” *National Interest*, December 22, 2009, <https://nationalinterest.org/article/war-from-cyberspace-3278>.

⁸ UN Economic Commission for Africa, “Tackling the Challenges of Cybersecurity in Africa. Policy Brief. No. 002, 6 p” (UNECA, 2014), <https://repository.uneca.org/handle/10855/22544>.

predictability and stability, foster trust in the utilisation of ICTs, and manage misunderstandings that may result in conflicts. The norms, in addition, could form guides that shape foreign and domestic policy and allow for robust bilateral and multilateral engagements.⁹

1.1 PROBLEM STATEMENT

Apart from the great opportunities offered by cyberspace, it also creates severe threats to non-state and state actors. Therefore, to prevent conflicts that would disrupt international security and peace, behaviour in cyberspace has to be checked. Cyber activities run on the internet, which needs norms given that the internet is not maintained, developed, managed or governed by a single stakeholder alliance, nor is it under state jurisdiction. This results in a lack of policy authority and jurisdictional ambiguity, best sorted out by norms.

Cyberspace has been touted as one “of the greatest intellectual challenges in the 21st century” since there is ambiguity about who is in charge and who will be in control in the future. It is further noted that “theories of International Relations are not able to grasp the entirety of cyberspace, but as previously experienced during history, each paradigm has its added-value to the dilemmas of the future of cyberspace.”¹⁰ At the beginning of the twenty-first century, cyber security was viewed as a technical issue, but today, it is deliberated at the highest echelons of government. It is regarded, rightly, as a fundamental national security challenge.¹¹

⁹ Finnemore M, Sikkink K., “International Norm Dynamics and Political Change,” *International Organization* 52 (1998): 887–917.

¹⁰ B. Feledy, “Challenges of Theoretical Approaches to Cyber Security Theorizing Security in the Eastern European Neighbourhood: Issues and Approaches,” *Academia.Edu*, 2018, 147–63.

¹¹ R. S. (Ed.) Dewar, *National Cyber Security and Cyber Defence Policy Snapshots* (Zurich: Centre for Cyber Security Studies, 2018).

The massive April 2007 cyber-attack wreaked havoc on Estonia. As one of the most networked countries globally, the tiny Baltic Sea state depends on ICT for tax, banking and financial services, the electoral process and general e-governance. The country was unable to communicate or transact business for weeks. The attack was not formally attributed, but observers noted that it came after announcing the intention of getting rid of a 1947 monument dating back to the Soviet-era capital, Tallinn.¹²

Challenges arise alongside growth in ICT uptake and increasing exposure to cyberspace. Such a threat stems from increased technological vulnerabilities. It requires urgent diplomatic and policy action and attention, mainly the probability of cyberattacks by state and non-state actors. Cybercriminals are beginning to wake up to the fact that Africa is a treasure field with vulnerable systems running emerging and nascent economies. Complex emergent matters include increased malicious deployment of ICTs by organised criminal groups, including terrorists, money launderers and traffickers of narcotics, human and wildlife trophies.

Kenya has a plethora of players in the public and private sectors that have adopted ICTs. Still, all have different cyber security arrangements and enforcement regimes that exploit gaps to impact international and national security.

Taking cognisance of this, the UN GGE and other organised groups have agreed on a normative framework on the use of ICTs to address the cyber insecurity phenomenon. The norms implementation requires collaboration and cooperation between the state actors and the other

¹² Kelly A. Gable, "Cyber-Apocalypse Now: Securing the Internet against Cyberterrorism and Using Universal Jurisdiction as a Deterrent.," 2010, <https://www.thefreelibrary.com/Cyber-apocalypse+now%3a+securing+the+Internet+against+cyberterrorism...-a0219374102>.

stakeholders from academia, civil society, private sector, and other experts. There has been an explosion of norms from varied sources with different levels of backing from their sponsors – this is likely to result in conflicts as well as gaps, more so since many norms developed by small closed groups do not inspire confidence and legitimacy.

Therefore, the motivation of this study is to look at the utilisation of the Cyber Norms to promote international security and the reasons for the apparent inadequate application of the UN-backed Cyber Norms. Secondly, it examines the existence of the requisite reciprocal arrangements, both in-country and with the international arena, to guarantee the formation of stable, secure and predictable cyberspace and to find out if there are any gaps to be tackled. In addition, the study looks at how Kenya has implemented UN Cyber Norms to address global security by guaranteeing the security of cyberspace and critical information and communication technology infrastructure. The need for guided cybersecurity capacity development to ensure that Kenya, as a responsible state, can adhere to the UN GGE cyber norms and enhance its cyberspace protection to take care of weighty destructive, disruptive, or otherwise destabilising cyber activity is also explored.

1.2 RESEARCH QUESTIONS

The primary/broad research question of the study is:

- Do Cyber Norms promote international security?

The specific research questions are:

- What is the level of awareness of existing Cyber Norms and emerging threats in cyberspace globally?

- What confidence-building measures for collaboration and cooperation exist between local, regional, and international stakeholders in line with the UN Cyber Norms?
- What are the Kenyan legal and policy framework and its effectiveness in supporting the UN Cyber Norms?

1.3 OBJECTIVES OF THE RESEARCH

The primary/broad objective of the study is:

- To examine the role of UN Cyber Norms in the promotion of international security.

The specific objectives are:

- To assess the level of awareness of existing Cyber Norms and emerging threats in cyberspace globally.
- To analyse the confidence-building measures for collaboration and cooperation between local, regional, and international stakeholders in line with the UN Cyber Norms.
- To critically assess the Kenyan legal and policy framework and its effectiveness in support of the implementation of the UN Cyber Norms.

1.4 RESEARCH HYPOTHESES

The primary/broad hypothesis of the study is:

- That UN Cyber Norms promote international security by giving safeguards against cyber-attacks and fostering cyber security.

The specific hypotheses are that:

- The level of awareness of existing Cyber Norms and emerging threats in cyberspace determine the level of cyber security.
- Confidence-building measures for collaboration and cooperation between local, regional, and international stakeholders in line with the UN Cyber Norms determine the level of cyber security.
- The Kenyan legal and policy framework effectively supports the implementation of the UN Cyber Norms and promotes cyber security.

1.5 JUSTIFICATION OF THE STUDY

This study is helpful to academicians, practitioners, and policymakers alike. For academicians, cyberspace is a grey area that needs proper investigation on why norms and international laws that the nations and organisations can use as they engage in cyberspace have not been universally agreed upon and adopted. In addition, there seems to be a miasma in the theories of international relations as far as cyberspace is concerned, and this needs to be filled.

As for practitioners, the study gives areas of thought in the development, utilisation, and securing of cyberspace that is currently a must for 21st century domestic, business, and governance operations and interactions.

Finally, for policymakers, the interactions in cyberspace need to be guided by certain norms, policies, regulations, and agreements between users, service providers, and other governments.

This study suggests policy direction on cyber norms.

1.6 LITERATURE REVIEW

“All our lauded technological progress – our very civilisation – is like the axe in the hand of the pathological criminal.” – Albert Einstein

The genius Einstein’s negative outlook made in the last century rings true today. ICT is a double-edged sword, proffering opportunities that bring along vulnerabilities. The good and the bad in humanity are manifested in cyberspace. The phenomenal growth in technology has meant that the normative frameworks that should deter malicious actions in cyberspace cannot keep pace – resulting in increased “crime, hacktivism or state-sponsored activities.”¹³ As a prefix, cyber denotes computer and electronic-based technology. At the same time, as an operational field, “cyber-space is outlined by the utilisation of electronics to manipulate information using interconnected systems and their associated setup.”¹⁴

Due to the disturbing sense of cyber insecurity, global actors have attempted to control the risk of escalation and clashes. From the Iranian nuclear plant Stuxnet attack in 2010 to the governments-exposing WikiLeaks by Snowden in 2013, the stakes have changed from hypothetical scenarios of the 1990s to demonstrable state and non-state utilisation of cyberspace. One of the methods used to maintain strategic stability in cyberspace is the employment of norms that stress good behaviour in addition to confidence-building measures that examine the application of international rules of war in cyber conflict. International relations and strategy study concepts come in handy in looking

¹³ Anna-Maria Osula and Henry Rõigas (Eds.), *International Cyber Norms: Legal, Policy & Industry Perspectives*, (Tallinn: NATO CCD COE Publications, 2016).

¹⁴ Joseph S. Nye, Jr., “Cyber Power” (Belfer Center for Science and International Affairs Harvard Kennedy School, 2010), <https://www.belfercenter.org/sites/default/files/legacy/files/cyber-power.pdf>.

at the deployment of cyber instruments for political, military, and economic advantage and the impact on international and national security.¹⁵

1.6.1 NORMS

Norms are described as “a standard of appropriate behaviours for actors with a given identity.”¹⁶ The implication is that the said norms can differ in coverage and legal punch. There are two main types of norms – International ones with legally binding obligations like treaties and points of reference for expected behaviour found in diplomatic engagements, legally non-binding and voluntary. Another way to look at norms is “collective expectation for the proper behaviour of actors with a given identity.”¹⁷ The emergence and evolution of norms depend on collective beliefs that define the actors' proper conduct (usually states in international relations). The norms create mutual expectations framework, and while they lack explicit legal implications, they guide the evolution of international law.

On the other hand, social norms of behaviour apply to non-state actors and regulate behaviour by motivation. The norms may not be adopted with the regulation accompanying documented unanimity, but they could be codified as policy or international law once recognition and widespread support is attained. After consensual adoption by a smaller committee, they are likely to be backed by the general community.

¹⁵ Theresa Hitchens and Nancy W. Gallagher, “Building Confidence in the Cybersphere: A Path to Multilateral Progress,” *Journal of Cyber Policy* 4, no. issue 1 (April 9, 2019): Pp 4-21, <https://doi.org/10.1080/23738871.2019.1599032>.

¹⁶ Finnemore M, Sikkink K., “International Norm Dynamics and Political Change.”

¹⁷ Katzenstein, P. J. ed., *Introduction: Alternatives Perspective on National Security,* in *The Culture of National Security: Norms and Identity in World Politics* (New York: Columbia University Press, 1996).

Norm development undergoes three stages, the “emergence of norms, the cascading adoption of norms, and the internalisation of those norms.”¹⁸ When norms emerge, there are many early promoters who are referred to as “entrepreneurs” since they react to emerging needs, yet they are not part of the authoritative bodies expected to issue the norms. In the early days, there was a proliferation of norms, many of which wither off prematurely. Achieving consensus is a dicey affair, but after publication and reflection by the stakeholders and others concerned, few norms emerge as frontrunners and are either informally or formally adopted by the universal community – this forms the cascade phase. Finally, the norms are comprehended and will be pervasive, requiring enforcement mechanisms. Codification may accompany the enforcement mechanism, though it is not a must for extensive acceptance and implementation.

Norms promotion and adoption have been slowed down by “differing ideological standpoints, mutual mistrust and diverging interests.”¹⁹ States are still grappling with the idea of international and national cyber security best practices and policy integration into their security and political structures. Cyber security will become easier to include in the states’ grand strategy, using the informational, social, diplomatic, military and economic resources to maintain financial and human security.²⁰

¹⁸ Maarten Van Horenbeeck, Ed., “Cybersecurity Culture, Norms and Values: Background Paper to the IGF Best Practices Forum on Cybersecurity.”

¹⁹ Egloff, F. J., Wenger, A, “Public Attribution of Cyber Incidents. In F. Merz (Ed.), *CSS Analyses in Security Policy*,” vol. 244 (Zurich: Center for Security Studies, 2019), 1–4.

²⁰ V. Weber, “Linking Cyber Strategy with Grand Strategy: The Case of the United States,” *Journal of Cyber Policy* Vol. 3 (2018): pp 236-257, <https://doi.org/doi:10.1080/23738871.2018.1511741>.

1.6.2 UN GROUP OF GOVERNMENTAL EXPERTS

Being a global forum that deals with international conflict and security, the United Nations is the central platform for all cybersecurity matters. The United Nation's Group of Governmental Experts (UN GGE) has been the face of the UN efforts in encouraging state positions in ICT developments. The expert engagement commenced in 1998, but progress has been slow because of different approaches and outlooks in scope, mandate and role of the UN, terminologies and even the assessments of the threats faced. In 2013, a "landmark consensus" was achieved as 15 countries acknowledged international law, more so the UN charter as "applicable and essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment."²¹ The 2015 report offered a voluntary cyber norms proposal. This agreement was the precursor to contemporary discussions on cyber norms.

The cross-cutting view is that international law, incorporating laws of armed conflict and the UN Charter, can regulate offensive state conduct in cyberspace. The complication arises from the dearth of agreement and clear insight into applying these legal norms to the complexity of cyberspace.²²

According to the report, further discourse is necessary due to cyberspace's "unique attributes", which may develop new norms. Critics have questioned the ability of existing international laws

²¹ "United Nations, General Assembly, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/68/98 (24 June 2013), http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98.http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98," n.d.

²² Michael N. Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press, 2013), <https://ccdcoe.org/research.html>.

to effectively govern state actions in cyberspace following examples like the attack on Sony Studios and campaigns of cyber espionage. States view the UN GGE process as an agreeable channel towards politically obligatory norms of conduct and “do not believe that attempts to conclude comprehensive multilateral treaties or similar instruments would make a positive contribution to enhanced international cyber security at present.”²³ Outcomes of the UN GGE deliberations have been cited by the US Office of Cyber Coordination in 2015, Leaders’ communique in G20 Antalya summit (2015), ASEAN member states in 2017 and cyber strategies for different nations for example, Australian International Cyber Engagement Strategy (2017).²⁴

Since 2004, a total of six functional groups have been formed (including the current GGE for 2019-2021). There are two significant achievements for the GGEs, setting the international agenda and emphasising the “applicability of international law to cyberspace.”²⁵

²³ “United Nations, General Assembly, Group of Governmental Experts, A/68/98.,” n.d.

²⁴ Maarten Van Horenbeeck, Ed., “Cybersecurity Culture, Norms and Values: Background Paper to the IGF Best Practices Forum on Cybersecurity.”

²⁵ Christian Reuter, *Information Technology for Peace and Security : IT Applications and Infrastructures in Conflicts, Crises, War, and Peace* (Wiesbaden: Springer Vieweg, 2019).

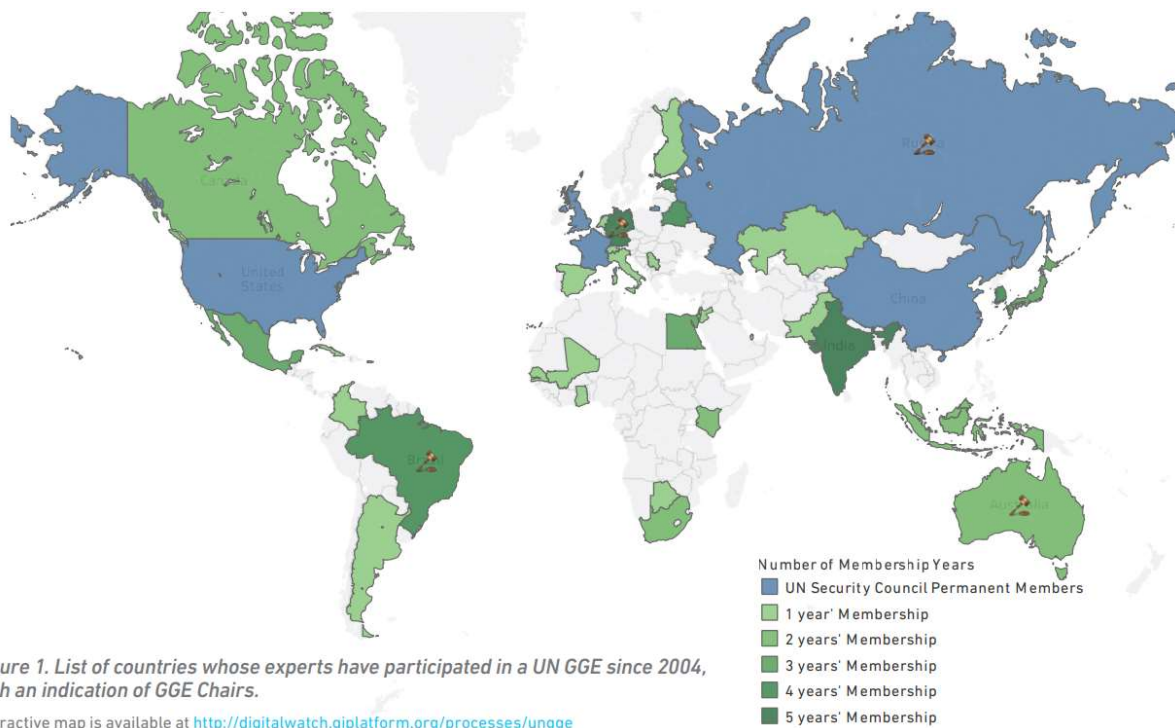


Figure 1. List of countries whose experts have participated in a UN GGE since 2004, with an indication of GGE Chairs.

Interactive map is available at <http://digitalwatch.giplatform.org/processes/ungge>

Figure 1 Experts' Countries (Source, Digital Watch 2021)

1.6.3 UN GGE NORMS

The GGE in 2015 agreed that “voluntary, non-binding norms of responsible State behaviour” could “reduce risks to international peace, security and stability.” The clarification was that the norms were not out to restrain or proscribe activities that are harmonious with international law. The norms are envisaged to signal the international community’s expectations, set accountable State behaviour standards and permit the global community to gauge the actions and aims of States.²⁶

²⁶ UN General Assembly, “Resolution 70/237 - Developments in the Field of Information and Telecommunications in the Context of International Security,” December 30, 2015, <https://undocs.org/a/res/70/237>.

The norms are intended to forestall conflict in cyberspace and ensure its peaceful utilisation globally for social and economic advancement. Initially proposed by the Russian Federation, China, Kazakhstan, Tajikistan, Kyrgyzstan, and Uzbekistan in 2011, the norms were seen as a possible code of conduct to be deployed internationally to deal with information security.²⁷

The Global Commission on the Stability of Cyberspace chairperson, Ms Marina Kaljurand, who was part of 2015 and 2017 GGEs, has noted that international law norms are legally binding, and then there are political norms that are voluntary. Political norms form a precedent when states want to address or understand a particular behaviour. Therefore, the political norms are expressed by way of political declarations and statements or comments and comments. Political norms that are applied and approved by many states may then develop into customary international law.²⁸

Picking recommendations and assessments of the 2010 and 2013 GGE reports, the 2015 GGE came up with eleven voluntary rules and principles, non-binding norms, towards “responsible behaviour of states aimed at promoting an open, secure, stable, accessible and peaceful ICT environment.”²⁹ Eight of the 11 norms could be considered positive duties – recommend states to take a particular action while three are negative, restraining specific behaviour. Protection of critical infrastructure and cooperation are covered by several of the norms indicating emphasis placed by GGE.

²⁷ UN, “A/69/723 -Developments in the Field of Information and Telecommunications in the Context of International Security - Sixty-Ninth Session Agenda Item 91” (UN Office of Disarmament Affairs, 2015), <https://undocs.org/a/69/723>.

²⁸ UN Office for Disarmament Affairs, “Group of Governmental Experts,” accessed November 30, 2020, <https://www.un.org/disarmament/group-of-governmental-experts/>.

²⁹ “Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology: A Commentary” (United Nations, 2017), <http://www.un.org/disarmament>.

Dr Katherine Getao, formerly Kenya’s ICT Secretary in the Ministry of Information, Communications and Technology of Kenya and then CEO of the ICT Authority, was also a member of the 2015 and 2017 GGEs. She opines that the GGE norms are “non-binding agreements that help countries to share a valuable common resource such as cyberspace, and they set the culture and the environment that enables sharing to take place in a coherent and workable way”. She classifies the norm into three – those that address values and use international law as the benchmark (human rights and sovereignty), those that try to set an enabling environment (critical infrastructure protection as the base upon which cyberspace operates and cooperation among non-state and state actors) and finally, norms that are operational (deal with processes that are needed to maintain safe cyberspace).³⁰

The following is an abridged form of the eleven norms:

Norm (a): “Consistent with the purposes of the United Nations, including to maintain international peace and security, States should cooperate in developing and applying measures to increase stability and security in the use of ICTs and to prevent ICT practices that are acknowledged to be harmful, or that may pose threats to international peace and security.”³¹

³⁰ UN Office for Disarmament Affairs, “Group of Governmental Experts.”

³¹ UN, “Efforts to Implement Norms of Responsible State Behaviour in Cyberspace, as Agreed in UN Group of Government Expert Reports of 2010, 2013 and 2015” (UN Disarmament, 2019), <https://www.un.org/disarmament/wp-content/uploads/2019/12/efforts-implement-norms-uk-stakeholders-12419.pdf>.

Norm (b): States that “In the case of ICT incidents, States should consider all relevant information, including the larger context of the event, the challenges of attribution in the ICT environment and the nature and extent of the consequences.”³²

Norm (c): “This norm draws from the 2013 GGE report, which asserts that “States must meet their international obligations regarding internationally wrongful acts attributable to them. Also, States must not use proxies to commit internationally illegal actions. States should seek to ensure that non-state actors do not use their territories for unlawful use of ICTs.”³³

Norm (d): “States should consider how best to cooperate in exchanging information, assisting each other, prosecuting terrorist and criminal use of ICTs and implementing other cooperative measures to address such threats. States may need to consider whether new standards need to be developed in this respect.”³⁴

Norm (e): “States, in ensuring the safe use of ICTs, should respect Human Rights Council resolutions 20/8 and 26/13 on the promotion, protection and enjoyment of human rights on the Internet, as well as General Assembly resolutions 68/167 and 69/166 on the right to privacy in the digital age, to guarantee full respect for human rights, including the right to freedom of expression.”³⁵

³² “Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology: A Commentary.”

³³ UN, “UN GGE Reports.”

³⁴ “Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology: A Commentary.”

³⁵ Ibid, UN, “UN GGE Reports.”

Norm (f): “A State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public.”³⁶

Norm (g): “States should take appropriate measures to protect their critical infrastructure from ICT threats, considering General Assembly resolution 58/199 on the "creation of a global culture of cybersecurity and the protection of critical information infrastructures" and other relevant declarations.”³⁷

Norm (h): “States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts. States should also respond to proper requests to mitigate malicious ICT activity aimed at the critical infrastructure of another State emanating from their territory, taking into account due regard for sovereignty.”³⁸

Norm (i): “States should take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products. States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions.”³⁹

³⁶ “Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology: A Commentary.”

³⁷ “Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology: A Commentary.”

³⁸ “Resolution Adopted by the General Assembly on 5 December 2018 - Seventy-Third Session Agenda Item 96” (United Nations, 2018), <https://undocs.org/pdf?symbol=en/A/RES/73/27>.

³⁹ “73/27. Developments in the Field of Information and Telecommunications in the Context of International Security.”

Norm (j): “States should encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies to such vulnerabilities to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure.”⁴⁰

Norm (k): “States should not conduct or knowingly support activity to harm the information systems of the authorised emergency response teams (sometimes known as computer emergency response teams or cybersecurity incident response teams) of another State. A State should not use authorised emergency response teams to engage in malicious international activity.”⁴¹

1.6.4 NATO

The Cooperative Cyber Defense Center of Excellence (CCDCOE) was founded by the North Atlantic Treaty Organization (NATO) in Tallinn, Estonia. CCDCOE came up with the original Tallinn Manual on the International Law Applicable to Cyber Warfare (Tallinn Manual 1.0). The second manual, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, was released in 2017. NATO has joined other global players in declaring the applicability of international law in cyberspace and the associated cyber norms of behaviour.⁴² The intention of

⁴⁰ Noëlle van der Waag-Cowling, Brett van Niekerk, and Dr Trishana Ramluckan, “Submission to the Call for Inputs: Report on the Provision of Military and Security Cyber Products and Services by ‘Cyber Mercenaries’ and Its Human Rights Impact” (Office of the United Nations High Commissioner for Human Rights, n.d.), <https://www.ohchr.org/Documents/Issues/Mercenaries/WG/CyberMercenaries/Academia-van-der-Waag-Cowling.docx>.

⁴¹ “Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology: A Commentary.”

⁴² Michael N. Schmitt, ed., *Tallinn Manual 2.0 on The International Law Applicable to Cyber Operations* (New York: Cambridge University Press, 2017).

the undertaking was not to come up with new rules or create a manual with the force of law but as an “objective restatement of the *Lex Lata*”⁴³.

The four parts of the manual deal with specialised regimes of international law and cyberspace, international peace and security and cyber activities, general international law and cyberspace, and the last part are basically Tallinn 1.0, which looks at the law of cyber armed conflict. Several parallels can be drawn between the UN GGE norms and the rules in Tallinn Manual 2.0. Rule 4 says that “[a] State must not conduct cyber operations that violate the sovereignty of another State.”⁴⁴ The manual’s rule 6 goes on to state that “a State must exercise due diligence in not allowing its territory, or territory or cyberinfrastructure under its governmental control, to be used for cyber operations that affect the rights of, and generate serious adverse consequences for, other States” which mirrors the sentiments of the UN GGE 2015 recommendations.

1.6.5 INTERNATIONAL TELECOMMUNICATIONS UNION (ITU)

The ITU is the UN’s specialised agency for ICT issues. The 190-member states agreed on the first set of International Telecommunications Regulations (ITRs) in 1988 that mainly addressed telephony matters. A 2012 meeting was convened to update the ITRs “to establish general principles which relate to the establishment and operation of international telecommunication

⁴³ Michael N. Schmitt, ed.

⁴⁴ Eric Talbot Jensen, “The Tallinn Manual 2.0: Highlights and Insights,” 48 *Georgetown Journal of International Law*, BYU Law Research Paper, 735, no. No. 17-10 (2017): 44.

services offered to the public as well as to the underlying international telecommunication transport means used to provide such services.”⁴⁵

The global political divide as far as state behaviour in cyberspace is concerned resulted in limited role and visibility for the ITU on these issues since the controversial meeting in 2012. Out of 144 participating states, only 89 signed the treaty. The rest claimed they were not keen to endorse a new layer of international Internet regulations against open and free internet space. The divide was between nations that would have liked to see more government control instead of the “multi-stakeholder internet governance system”, which was seen as advantageous to the United States government and gave allowance for malicious state activities in cyberspace.

1.6.6 MULTILATERAL AND BILATERAL ARRANGEMENTS

OSCE & Confidence-Building Measures - From the cold war times, the confidence-building measures (CBMs) aimed at preventing conflicts with the risk of nuclear war – by sharing information and cooperation between states. Organisation for Security and Co-operation in Europe (OSCE) came up with eleven CBMs in December 2013 related to States conduct in cyberspace, including voluntary cooperation and information sharing.⁴⁶ The states agreed to have ICT contact points, consultations and national ICT policies discussions. An unofficial working group of delegates from the 57 states was tasked with implementing the CBMs and developing the second

⁴⁵ “International Telecommunication Union, Final Acts of the World Administrative Telegraph and Telephone Conference Melbourne, 1988 (WATTC-88): International Telecommunications Regulations” (International Telecommunication Union, Geneva, 1989), <https://ccdcoe.org/sites/default/files/documents/ITU-881209-ITRFinalActs.pdf>.

⁴⁶ Jason Healey et al, “Confidence-Building Measures in Cyberspace: A Multistakeholder Approach for Stability and Security,” *Atlantic Council*, 2014, www.atlanticcouncil.org/images/publications/Confidence-Building_Measures_in_Cyberspace.pdf.

generation of CBMs by 2015 – this has not been achieved due to political tensions and differing interests and ideologies (US and Russia are members of this group).

Global Commission on the Stability of Cyberspace (GCSC) was inaugurated by two nonpartisan think tanks, the East-West Institute (EWI) and The Hague Centre for Strategic Studies (HCSS). The GCSC comprises twenty-six renowned Commissioners from various stakeholder groups, with regional representation and expertise in different facets of cyberspace. It aims to help foster mutual understanding and recognition among the varied cyberspace stakeholders working on issues linked to international cybersecurity. As a group, it has propositioned several “norms for responsible behaviour in cyberspace.”⁴⁷

The Shanghai Cooperation Organization – led by China and Russia, is an active producer and promoter of cyber norms. The block of states embraced the 2009 Yekaterinburg Agreement that formed the core mechanisms and principles for collaboration in terms of security – resulting in the “International Code of Conduct for Information Security”, passed on to the UN in 2015. The code is intended to apply to all UN member states whose thrust is state sovereignty over its information space, multilateral internet management and principal responsibility for the UN in devising international cyber norms.⁴⁸ Western states are not keen on this code as it restricts the uninhibited flow of information. The current multi-stakeholder internet organisation supports Western countries focusing on existing international laws and politically binding norms instead of new

⁴⁷ Global Commission on the Stability of Cyberspace, “Advancing Cyberstability Final Report” (The Hague Centre for Strategic Studies and EastWest Institute, November 2019), <https://cyberstability.org/report/>.

⁴⁸ “Shanghai Cooperation Organization, Agreement between the Governments of the Member States of the Shanghai Cooperation Organisation on Cooperation in the Field of International Information Security” (Shanghai Cooperation Organization Secretariat., June 16, 2009), <http://eng.sectsco.org/documents/20090616/207486.html>.

overarching treaties. However, a keen look at the proposed Code of Conduct comes up with “legally non-binding norms that are of a voluntary or aspirational nature.”⁴⁹

1.6.7 PRIVATE SECTOR

Microsoft Corporation, as a representative of the private sector, has also weighed in on the matter. The corporation believes that norms should ensure increased security in cyberspace and uphold globally connected society benefits. The tech giant conceptualises two kinds of norms – “Norms for improving defences, which can decrease risk by stipulating a foundation for national cybersecurity capability and for international, regional, and domestic organisational arrangements and approaches that improve understanding between states and norms for restraining conflict or offensive operations, which will serve to reduce conflict, avert escalations, and curb the potential for catastrophic impacts in, through, or even to cyberspace.”⁵⁰ While defining acceptable and unacceptable state behaviour to lessen the risks, cultivate greater predictability and check on negative impacts (including those arising from the activity below the war ceiling).⁵¹

While they acknowledge that the move to legally binding norms from the current political oriented norms will be an uphill task, they are optimistic that the norms can evolve into customary international law in the fullness of time if additional development, general practice and dialogue are encouraged. It is generally accepted at the international level that the policy outlook has been

⁴⁹ China, the Russian Federation, Tajikistan and Uzbekistan, “International Code Of Conduct For Information Security” (UN Office of Disarmament Affairs, 2011), <https://www.un.org/disarmament/publications/library/66-ga-ga-sc/>.

⁵⁰ “International Cybersecurity Norms - Microsoft Policy Papers” (Microsoft Corporation, 2020), <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVmcd>.

⁵¹ Mackay, A. Neutze, J., “International Cybersecurity Norms : Reducing Conflict in an Internet-Dependent World” (Microsoft Corporation, 2015), https://cybersummit.info/sites/cybersummit.info/files/International_Cybersecurity_%20Norms.pdf.

leaning towards cybersecurity norms to lower risk arising from the complex regional and international cyber occurrences and the advancement of CBMs.

Even though cyber activity has not yet resulted in armed conflict in the true sense, the boundaries between conflict and crime are blurred. However, cyber events are challenging to defend against and could have a widespread communal impact. Figure 2 shows how cyber norms can be utilised.

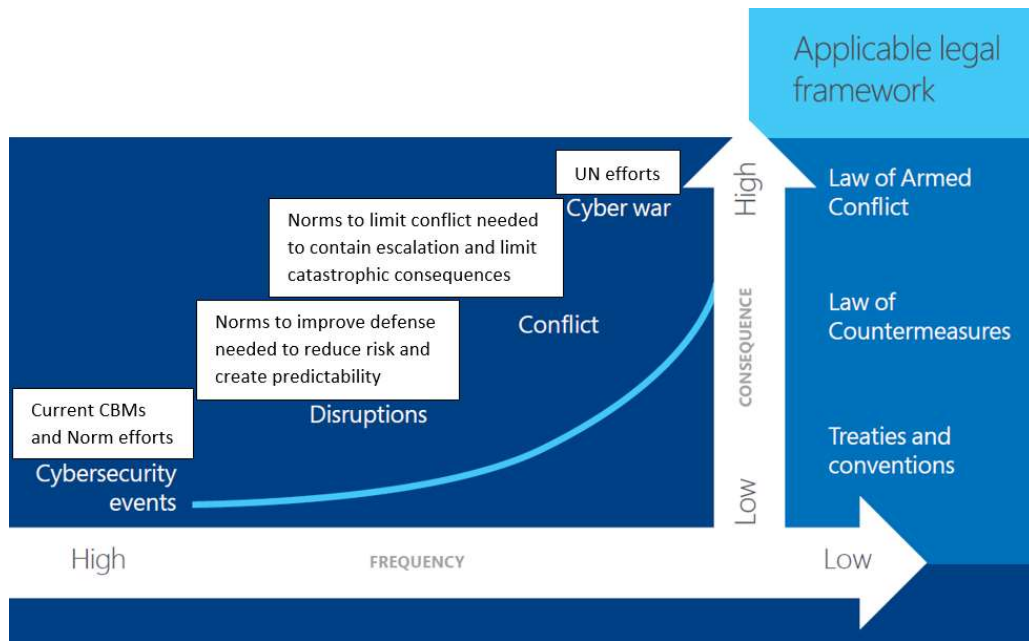


Figure 2 Escalation of cyber events and applicable legal frameworks and opportunity space for cybersecurity norms (Source Microsoft Corporation, 2015)

Microsoft states that there are four criteria for practical norms - practicability of the norms, ability to reduce complex cyber disruptions and risks that could end up in a dispute, result in noticeable behavioural change that transforms cyberspace security of civil society, enterprises, states and individual users. Lastly, the norms should “leverage existing risk management concepts to help

mitigate against escalation, and, if escalation is unavoidable, they should provide useful insight into the potential actions of involved parties.”⁵² ⁵³

Microsoft has fronted six norms to limit conflict, to reduce the prospect that ICT products are exploited, abused or used by non-state and state actors as part of the arsenal of offensive actions. The first norm warns states against states forcing companies to compromise ICT systems in such a way as to undermine public trust in ICT services and products. The second norm asks states to enact clear principle-based policies to deal with system vulnerabilities and not exploit them. The subsequent norm asks the states to exercise restraint in acquiring cyber weapons tying in with the fourth, urging states to commit to nonproliferation of cyber weapons. The last two exhort states to restrain their engagement in aggressive cyber campaigns not to affect the masses and support private-sector efforts to uncover, contain, respond to, and recover from events in cyberspace.

1.7 THEORETICAL FRAMEWORK

Efforts to advance International Relations (IR) theories that are appropriate for the communication and information age have remained relatively insufficient, “primarily due to the inner-looking focus of the discipline.”⁵⁴

Structural liberalists lack clear indications of reciprocity, consensus building and cooperation when addressing cyberspace dilemmas. This issue is particularly challenging at the global level,

⁵² Mackay, A. Neutze, J.

⁵³ Anna-Maria Osula and Henry Rõigas (Eds.), *International Cyber Norms: Legal, Policy & Industry Perspectives*, .

⁵⁴ Eriksson, J. and Giacomello, G. (eds), *International Relations and Security in the Digital Age*, Advances in International Relations and Global Politics (New York: Routledge, 2007).

given that anarchy has often been regarded as generating disincentives to effective collaborative action and assistance.⁵⁵

International regime theories (IRT) reveal that collaboration is achievable in a milieu with no higher power to force the nations to cooperate. “International regimes can be defined as explicit or implicit norms, rules, principles and decision-making processes related to specific issue areas/subjects.”⁵⁶ IRT assumes that members of any regime are like-minded with a common purpose and desire. The UN Charter, which promotes international peace and security, is one such regime that can address the issues in cyberspace.

1.8 METHODOLOGY OF STUDY

This section focuses on the scientific methodology of the research. The research design is a mix of exploratory research to establish the range and extent of implementing UN GGE Cyber Norms and evaluative research to determine the merit and efficacy of the programmes in place. The researcher also considered case studies of other jurisdictions that have implemented the norms.

1.8.1 RESEARCH DESIGN

The study adopted a mixed-methods approach which allows for mixing and triangulation of qualitative and quantitative research methods to collect and analyse data on a single subject of study. A descriptive survey design was adopted as the primary research design. This type of design

⁵⁵ Deudney, D., Ikenberry, J.G., “The Nature and Sources of Liberal International Order, , , ,” *Review of International Studies* Volume 25, no. Issue 2 (April 1999): 179–96.

⁵⁶ Kello, L., ‘Cyber Security: Gridlock and Innovation’, in: Hale T. and Held, D. (Eds.), *Beyond Gridlock*. (UK: Polity Press, 2017).

permits the researcher to collect data to answer the questions of the current status of the subject under study. This study used quantitative and qualitative research designs to collect in-depth interviews with key players in the cyber security realm. Using purposive and quota sampling methods, several respondents were selected based on their presumed knowledge in cyber security enforcement.

1.8.2 RESEARCH SITES

This study focused on the Ministry of ICT, Youth and Innovation, the ICT Authority, The Communications Authority, The Telecommunications Service Providers (TESPOK) and the National Cyber Command Centre (NC3). These have been chosen because the institutions have a wealth of information regarding the problem under study.

1.8.3 TARGET POPULATION

“A target population is the set of individuals, cases or objects with some common observable characteristics with which a researcher generalises the results of a study.”⁵⁷ The study, therefore, targeted senior policymakers and enforcers of cyber security. Key informants were drawn from relevant offices within the institutions identified in the Research sites.

⁵⁷ Mugenda, O. and Mugenda, A., *Research Methods: Quantitative And Qualitative Approaches* (Nairobi: ACTS Press, 1999).

1.8.4 SAMPLE SIZE

“A sample is a group of units selected from a larger group.”⁵⁸ It is the process of selecting several individuals for a study to represent the large group from which they are selected.⁵⁹ A sample is necessary for a study if the population is too large to study in its entirety. The researcher got respondents from all the key institutions and regulators in Kenyan cyberspace.

1.8.5 SAMPLING TECHNIQUES

Key informants included policymakers directly charged with ensuring safety and security in cyberspace from a regulatory, user and service provider perspective. The primary data collection instrument was the interview schedule/guide for key informants and FGDs. Thematic analysis of the response was vital in this study. Examination of the situation on the ground was used to measure the current critical information infrastructure protection status. Secondary data was also retrieved through books, official government documents, newspapers, journals, periodicals, and online publications. Confidentiality of the participants and institutions was guaranteed (where privacy was required or demanded), and information sources were appropriately accredited.

1.8.6 DATA COLLECTION

Data collection consisted of designing and administering questionnaires while leveraging subjective methods such as interviews and observations to supplement the collection of substantive

⁵⁸ Cooper, D., & Schindler, P., *Business Research Methods*, 10th ed. (New York: McGraw-Hill/Irwin, 2008).

⁵⁹ Ogula, P. A., *Research Methods* (Nairobi: CUEA Publications, 2005).

and relevant data. The researcher contacted the selected policymakers and implementers of the cyber security norms.

Initially, the questionnaire was administered to a broad range of participants. Subsequently, a (targeted) defined sample was identified using key informant interviews in the second round of data collection.

1.8.7 QUESTIONNAIRE

The data were collected using structured questionnaires that were distributed to the identified respondents. The questionnaires had both open-ended and closed questions - the instruments comprised structured and semi-structured questions to derive quantitative and qualitative data. The questions were organised in different sub-headings to examine the different variables of the study. Responses were assessed using the Likert scale.

1.8.8 IN-DEPTH INTERVIEWS

“An in-depth interview is a discovery-oriented method that allows deep interaction with the respondent’s feelings and perspectives on the subject.”⁶⁰ Key informant interviews were conducted with senior policymakers and cyber security norms implementers to respond to the same objectives of the study. The areas of the measure during the interview included the extent of implementation of the cyber norms, the impact of the cyber norms on the effectiveness of cyber security and the available opportunities for enhancing the cyber norms.

⁶⁰ Polit, F. D., Polit-O’Hara, D., P. Hungler, B.P., *Essentials of Nursing Research: Methods, Appraisal, and Utilization*, 4th Ed (University of Michigan: Lippincott-Raven, 1997).

1.8.9 DATA ANALYSIS

After collecting the qualitative data from said interviews, careful analysis was done (both manually and utilising relevant software) like a commercial spreadsheet package like Microsoft Excel.

1.8.10 INSTRUMENT VALIDITY

“Validity is the accuracy and meaningfulness of inferences, which are based on the research data collected.”⁶¹ It is the degree to which results obtained from the data analysis represent the study's variables. Validity signifies the degree to which a tool measures what is supposed to be measured. The researcher used research validity to ensure that the studied sample represents the population and used criterion-related legitimacy to reflect the success of measures used for empirical estimation purposes. The data collected through the preliminary survey was used to adjust or modify the questionnaire to boost clarity levels.

To test the study's validity, different experts were given questionnaires, and then their varied responses were examined since different respondents would commonly understand the questions in a different way. Thus, more significant variance in how the interviewees approached the queries generally implied the construct needed some modification.

⁶¹ Mugenda, O. and Mugenda, A., *Research Methods: Quantitative And Qualitative Approaches*.

1.8.11 INSTRUMENT RELIABILITY

“Reliability measures the degree to which a research instrument would yield consistent data results when conducted in another given similar situation. This is done to ensure that there is consistency across all given variables.”⁶²

A measuring device is reliable if it provides consistent results, thus improving the study's reliability by standardising the conditions under which the measurements occur. Reliability in the context of this study was measured by the extent to which questions included in the research instrument yielded similar results across all the categories of the samples.

1.8.12 LEGAL AND ETHICAL CONSIDERATIONS

“Research is an activity designed to test a hypothesis, permit a conclusion to be drawn and thereby contribute to generalised knowledge expressed in theories, principles and statements of relationships.”⁶³ All other people’s ideas, processes and results should be given due credit. The researcher obtained a research permit from the National Council for Science and Technology and Innovation (NACOSTI) before going out to the field. The authorisation letter was presented to the offices where the study was conducted.

Further consent to participate in the research was sought from the respondents who were assured of anonymity and confidentiality to get more honest and accurate responses. The respondents were informed that the information collected was purely for academic purposes and were also notified

⁶² Mugenda, O. and Mugenda, A.

⁶³ Matthews, B. and Ross, L., *Research Methods* (London: Pearson Longman, 2010).

of the aims, methods, anticipated benefits of the research and their right to withdraw from participation in the research at any time. The researcher was also be obliged to reveal the findings of the research.

1.9 LIMITATION AND ASSUMPTIONS

The study was limited to the jurisdiction of Kenya, even though cyberspace and its security is a transnational and global affair. It is probable that due to the confidential nature of cyber security enforcement activities, not all information is availed for purposes of this research – including access to officers involved in the enforcement activities. Due to time constraints and security concerns, it may not be possible to travel to all areas that host critical ICT infrastructure to get first-hand information on the implementation of the cyber norms. Another limiting factor is the prevailing COVID-19 pandemic, limiting activity and interaction in most public places and offices.

1.10 CHAPTERS OUTLINE

This study is organised into six chapters.

Chapter One covers the General Introduction, Background to the Study and presents the Statement of the Problem, Research Objectives, Literature Review, Justification and Significance of the Study, Theoretical Framework and Research Methodology.

Chapter Two deals with discourses on the level of awareness of UN GGE Cyber Norms in Kenya. It covers cyber-crime development, including emerging threats, critical infrastructure issues, ICT vulnerabilities, and the challenge of attribution. It also discusses the contribution of Cyber Norms to cyber security globally.

The third chapter analyses the collaboration and cooperation initiatives between local, regional and international stakeholders to ensure cyber security in line with the cyber norms. Confidence Building Measures (CBMs), supply chain integrity, capacity building, and authorised emergency response teams are covered in this chapter.

Chapter Four has the legal and policy frameworks in place in line with the cyber norms. The chapter looks at international law, respect for human rights and internationally wrongful acts attributable to states before zeroing in on the local legal environment.

Chapter Five analyses, presents and interprets the research findings.

Chapter Six consists of a summary of findings, discussions, conclusions, and recommendations of the study. Also included are suggestions for further research and contribution to the body of knowledge.

CHAPTER TWO - LEVEL OF AWARENESS OF EXISTING AND EMERGING THREATS IN CYBERSPACE GLOBALLY

2.0 INTRODUCTION

Chapter Two presents discourses on the emergence and development of cyber-crime and the global awareness of cyber threats and norms. It also discusses the contribution of Cyber Norms to cyber (in)security globally.

2.1 DEVELOPMENT OF CYBERCRIME

Criminal conduct and information and communication technology systems have been in discussion at regional and national levels since the introduction of ICTs, with the challenge arising from the continuous technical development and the innovation of cybercriminals. In the 1960s, computer technology prevalence increased exponentially with the invention of the transistor, which enabled the transition from the costlier vacuum-tube based machines. The focus was on the physical protection of data holding devices and computer systems during the early days. The USA was looking at centrally storing data for all ministries, with discussions mainly bordering on privacy risks and criminal abuse of the database.⁶⁴

In the 1970s, it was estimated that over 100,000 mainframe computers were serving public and business enterprises in the United States as the prices of the computers dropped.⁶⁵ New forms of

⁶⁴ R. T. Slivka; J. W. Darrow, "Methods and Problems in Computer Security," *Rutgers Journal of Computers and the Law* 5, no. 2 (1976): 217–70.

⁶⁵ Stevens, M. L., "Identifying and Charging Computer Crimes in the Military," *Military Law Review* Vol. 110 (1985): pg. 59.

computer crimes emerged, including proscribed use of computer systems and falsification of electronic data. Electronic fraud also rose with the shift to computer transactions from manual operations.⁶⁶ The movement to personal computers gained momentum in the 1980s, and the increase in computers systems resulted in an exponential rise in the number of potential targets and critical infrastructure. The spread of systems came with the emergence of software piracy and patent-related crimes. Computer networks allow criminals to access computers remotely and spread malicious software, better known as computer viruses. Draft bills specifically to address cybercrime and Interpol involvement looking at possible legal responses emerged. Countries and international organisations like the Council of Europe and the OECD analysed the phenomena to develop legal responses.⁶⁷

The 1990s were characterised by adopting the graphical user interface and growth in internet users - information was globalised. Online services facilitated transnational crime with instant information exchange between criminals challenging law enforcers. The transnational nature of internet crime brought cybersecurity to the international stage, with UN General Assembly passing Resolution 45/121 in 1990⁶⁸ followed by the manual for preventing and controlling crimes related to the computer in 1994.

⁶⁶ Bequia, A., "Computer Crime: A Growing and Serious Problem," *Police Law Quarterly* Vol. 6 (1977): pg. 22.

⁶⁷ Schjolberg, S., Tingrett, M., "A Presentation at the Octopus Interface 2004" (Conference on the Challenge of Cybercrime, Strasbourg, France.: Council of Europe, 2004), <https://www.cybercrimelaw.net/documents/Strasbourg.pdf>.

⁶⁸ "Eight UN Congress on the Prevention of Crime and Treatment of Offenders - UN General Assembly Resolution A/RES/45/121" (UN, December 14, 1990), <https://undocs.org/pdf?symbol=en/A/RES/45/121>.

New trends in cyber and computer crime have emerged in the 21st century with more sophisticated methods, for instance, “phishing” and “botnet attacks”⁶⁹ and the use of cloud computing and voice-over-IP (VoIP) communication.⁷⁰ These have made it more difficult for law enforcers to handle and investigate, not to mention the automation of attacks, which has exponentially increased the number of offences. States, regional and international bodies are now forced to prioritise cyber crime management initiatives.

2.2 EMERGING THREATS

While ICTs provide almost unlimited prospects for economic and social development, in addition to phenomenal growth and importance for the global community, there are ominous developments in cyberspace. These include an exponential rise in confrontations involving the malicious usage of ICTs by State and non-State actors. All States are thus at risk, and the misuse of ICTs will negatively impact international peace and security. “In the last decade, cyber incidents have become more expensive, more disruptive, and in many cases more political.”⁷¹

The threat in cyberspace led the military strategists in the major powers (USA, Russia and China) to look at the value of networked computers for war purposes leading to cyberspace being treated as a “domain of warfare” in the 1990s. In 2011, the US Pentagon declared cyberspace the fifth domain of warfare after sea, land, air and space. Cyberspace is regarded as a double-edged sword

⁶⁹ Wilson, C., “Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress” (Congressional Research Service, January 29, 2008), <https://fas.org/sgp/crs/terror/RL32114.pdf>.

⁷⁰ Simon, M., Slay, J., “Voice Over IP: Forensic Computing Implications.” (4th Australian Digital Forensics Conference, Edith Cowan University, Perth Western Australia, 2006), <https://doi.org/10.4225/75/57b13904c7058>.

⁷¹ Myriam Dunn Cavelty, Andreas Wenger, “Cyber Security Meets Security Politics: Complex Technology, Fragmented Politics, and Networked Science, Contemporary Security Policy” vol 41, no. 1 (2020): 5-32, <https://doi.org/DOI:10.1080/13523260.2019.1678855>.

– information dominance that can be used to win wars, but simultaneously, a source of insecurity due to vulnerabilities because of reliance on the same cyberspace.⁷²

The term *cybercrime* covers a wide variety of criminal activities. “Developing a typology or classification system for cybercrime is tricky due to the broad range of offences.”⁷³ The Council of Europe Convention on Cybercrime (CETS) distinguishes between four different types of offences: Content-related transgressions; Computer-related infractions; Offences against the availability, integrity and confidentiality of computer systems and data, and copyright-related violations.⁷⁴

There is increasing reliance on digital tools for the provision of services globally with attendant security disruptions. In the first decade of the twenty-first century, *NotPetya WannaCry*, and *Stuxnet* incidents and the interference of the American election have cemented the fact that “cyber-attacks are becoming more targeted, more expensive, more disruptive, and in many cases more political and strategic.” Consequently, cyber conflicts, taken as “disruptions of the routine operations of digital technologies,”⁷⁵ have taken a leading position in international and national security policy discourse, with state actors scrambling to get answers to respond to the new threats. The 2015 GGE report notes that several states are in the process of developing ICT competencies

⁷² Rattray, G, *Strategic Warfare in Cyberspace* (Cambridge, MA: The MIT Press., 2001).

⁷³ Sarah Gordon and Richard Ford, “On the Definition and Classification of Cybercrime,” *Journal in Computer Virology* 2, no. 1 (August 1, 2006): 13–20, <https://doi.org/10.1007/s11416-006-0015-z>.

⁷⁴ “Convention on Cybercrime” (European Treaty Series - No. 185, 2001), https://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf.

⁷⁵ Myriam Dunn Cavelty, Andreas Wenger, “Cyber Security Meets Security Politics: Complex Technology, Fragmented Politics, and Networked Science, Contemporary Security Policy.”

for military purposes.” This indicates that the application of ICTs in clashes between nations is becoming a reality.

Also encompassed in the 2015 GGE report is the fear of the utilisation of ICTs for terrorist intents. In addition to “recruitment, financing, training and incitement, including for terrorist attacks against ICTs or ICT-dependent infrastructure, is an increasing possibility that, if left unaddressed, may threaten international peace and security.”⁷⁶

2.3 CRITICAL INFRASTRUCTURE THREATS

Norm (f) states that a “State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public.”⁷⁷ ⁷⁸The 2015 GGE reports notes that “the most harmful attacks using ICTs include those targeted against the critical infrastructure and associated information systems of a State.” ⁷⁹

Coined in the early 2000s, critical information infrastructure is used to mean “material and digital assets, networks, services, and installations that, if disrupted or destroyed, would have a serious

⁷⁶ Eneken Tikk and Mika Kerttunen, *Routledge Handbook of International Cybersecurity - The Role of the UN Security Council in Cyber Security* (London: Routledge, 2020), https://tandfbis.s3-us-west-2.amazonaws.com/rt-files/docs/Open+Access+Chapters/9781351038904_oachapter30.pdf.

⁷⁷ UN General Assembly, “Resolution 70/237 - Developments in the Field of Information and Telecommunications in the Context of International Security.”

⁷⁸ Melissa Hathaway, “Getting beyond Norms: When Violating the Agreement Becomes Customary Practice” (Centre for International Governance Innovation, April 2017), <https://www.cigionline.org/sites/default/files/documents/Paper%20no.127.pdf>.

⁷⁹ UN, “UN GGE Reports.”

impact on the health, security, or economic well-being of citizens and the efficient functioning of a country's government.”⁸⁰

The continued global growth and development has meant complexity and interconnection of critical services leading to challenges in security. Assimilation of ICT has led to new vulnerabilities, increased risks and targets via cyberspace. Country specific cybersecurity policies and strategies are necessary.⁸¹

On Sunday 9th May 2021, the government of the USA announced a regional emergency following a ransomware attack that occasioned the shutdown of the over 5,000-mile Colonial Pipeline, the country's most extensive pipeline fuel arrangement, necessitating road transport of the fuel on the East Coast. The attack is alleged to have been engineered by a cybercriminal gang going by *DarkSide*, thought to be operating from Eastern Europe and Russia. The road transport of the fuel is unsafe and unable to match the 2.5 million barrels shipped through the oil pipeline, with fear of oil price hikes in the near future.⁸²

Kenya has implemented fibre optic connection countrywide through the National Optic Fibre Backbone (NOFBI) project and the last mile County Connectivity Project (CCP). The target is the linkage of all county and sub-county headquarters. Critical government activities benefit from the high-speed broadband across the counties since secure, fast and reliable connectivity is a

⁸⁰ Andreas Wenger, Jan Metzger, and Myriam Dunn Cavelti, “An Inventory of Protection Policies in Eight Countries. Critical Information Infrastructure Protection,” *Center for Security Studies (CSS), ETH Zürich, International CIIP Handbook*, 2002, <https://doi.org/10.3929/ethz-b-000325400>.

⁸¹ Keen Welchman, “Safeguarding Critical Information Infrastructure: Risk and Opportunities” (World Economic Forum, 2020), <https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/Documents/Events/2020/RDF2020/Post%20Forum%20Day%203/CII-Whitepaper-WK.pdf>.

⁸² David Millward, “Biden Declares Emergency after Hackers Shut down Major US Pipeline,” May 9, 2021, <https://news.yahoo.com/biden-administration-step-cybersecurity-hackers-151107172.html>.

prerequisite for robust government-to-citizen platforms. The installation of this critical infrastructure has improved government service delivery, including essential documents like birth and death certificates, passports, and national identity cards. Integrated into the system are a telecommunications network and internet provision that powers many government automated systems, including the Government Human Resource Information System (GHRIS), the Integrated Financial Management System (IFMIS), and the government payroll system (IPPD). Hospital connectivity to NOFBI will contribute immensely to the Universal Health Care initiative with cutting edge technologies like telemedicine and e-health systems bringing the rural and poor populations closer to expert health provision. The NOFBI network is thus an essential aspect in linking the digital divide with the country currently enjoying over 90% broadband access. The NOFBI critical infrastructure extends to South Sudan through the Lesseru-Nadapal-Nakodok Road in the North Rift, enhancing bilateral relations with the South Sudan state as a component of the eastern Africa Regional Trade and Transport development acceleration project.⁸³ Linkage to Ethiopia is also on the cards through the Horn of Africa Initiative.

As part of the ICT critical infrastructure, Kenya has telecommunications masts and other communication hardware, apart from fibre optic cables. The interference with the critical infrastructure is widespread in Kenya, with Al-Shabaab destroying communications masts along the Kenya Somalia border, expansive and porous, leaving the region without telephone and internet connectivity. The plan is to disable the communication system before launching attacks, making it harder for citizens to report to the authorities and slowing down security agencies response and

⁸³ ICTA, “National Optic Fibre Backbone (NOFBI) – ICT Authority,” 2020, <http://icta.go.ke/national-optic-fibre-backbone-nofbi/>.

coordination. Competition, uncoordinated road construction and malicious acts have also been blamed for damage to ICT critical infrastructure.⁸⁴

Conversely, the United Nations issued a report accusing Kenya of carrying out attacks on telecommunications masts belonging to the leading Somalia telecom provider, possibly curtailing troop movement intelligence by the terrorists and even triggering explosives using cellphone signals. Hormuud Telecom has stated it has suffered ten attacks over two years (2017-2018) with estimated infrastructure losses valued at US\$ 5 million, in contravention to international law. The state of affairs is compounded further by the fact that the residents of Somalia rely on remittances from the Somali diaspora, having long suffered climate shocks and drought, not to mention the extremist attacks.⁸⁵

2.4 ICT VULNERABILITIES

Norm (j) encourages responsible state behaviour in reporting ICT vulnerabilities in addition to disclosing related information on existing solutions to such weaknesses to control and possibly exterminate potential threats to ICT-dependent infrastructure and ICTs.⁸⁶ The 2015 GGE report

⁸⁴ Jacob Mugendi, “Al-Shabaab’s Impact on Communications in Kenya,” iAfrikan.com, February 8, 2021, <https://iafrikan.com/2021/02/08/terrorism-a-threat-to-communication-in-northern-kenya/>.

⁸⁵ Tom Odula, “UN Links Kenyan Military to Attacks on Somalia’s Top Telecom,” AP NEWS, November 15, 2019, <https://apnews.com/article/266181bb47cb42bf9af392562c7c8c1f>.

⁸⁶ Richard Hill, “Promoting Stakeholder Action Against Botnets and Other Automated Threats” (Association for Proper Internet Governance, January 2018), https://www.ntia.doc.gov/files/ntia/publications/association_for_proper_internet_governance.pdf.

also observes that the different levels of competence for ICT security among States can fuel vulnerability in an interconnected global setting.⁸⁷

The Communications Authority of Kenya (CA) is responsible for approving ICT equipment, in the process confirming that there are no inherent vulnerabilities while ensuring conformity and compatibility with international and national standards. It relies on the documentation from the device manufacturer (including conformance certificates from the regulator in the country of origin) and a sample of the device to decide “type approval”.⁸⁸ In its consumer protection role, the CA approved 991 models of telecommunications equipment, representing an over 100 per cent growth compared to the previous year, partly enforced by TradeNet, the single window import system by all ICT equipment importers. The challenge is that many electronic devices are considered ‘grey’ imported illegally and come from third party manufacturers whose production systems are not certified and lack requisite information to trace back to the source of origin.⁸⁹

2.5 CHALLENGE OF ATTRIBUTION

Norm (b) addresses the risks of misperception and misattribution. It declares that “In case of ICT incidents, States should consider all relevant evidence, including the larger circumstance of the event, the challenges of attribution in the ICT ecosystem and the nature and extent of the consequences.”⁹⁰ The 2015 GGE report observes that the malicious non-State actors are diverse

⁸⁷ “Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security - A/70/174” (UN, July 22, 2015), https://www.un.org/ga/search/view_doc.asp?symbol=A/70/174.

⁸⁸ Communications Authority of Kenya, “Type Approval Procedure,” *Communications Authority of Kenya* (blog), accessed May 17, 2021, <https://ca.go.ke/industry/type-approval/type-approval-procedure/>.

⁸⁹ “CA Annual Report FY 2019-2020,” accessed May 17, 2021, <https://ca.go.ke/wp-content/uploads/2021/05/Annual-Report-for-Financial-Year-2019-2020.pdf>.

⁹⁰ Hill, “Promoting Stakeholder Action Against Botnets and Other Automated Threats.”

and include criminal groups and terrorists with differentiated motivations. The swiftness with which wayward ICT actions can be executed and the strain of accrediting the source of an ICT attack all amplify the risks. There is concern among the states regarding the “danger of destabilising misunderstandings, the potential for conflict and the possibility of impairment to their citizens, property and economy.”⁹¹

According to Kenya's 2015 Serianu cyber security report, the top sources of malicious attacks perpetrated on Kenya were attributed to the USA (20%), followed by China at 19% and Russia taking the third position with 11%. It is conceivable to anonymise attacks by hiding behind virtual private networks and proxy services to make attacks from a different region appear to be coming from another region.⁹²

Kaspersky, the cybersecurity firm, indicated that Kenya had the highest cyber-attack incidents in the first half of 2020 compared to the other leading targets – South Africa and Nigeria. Kenya faced 14 million malware attacks out of the total 28 million attacks targeting Africa, thus accounting for 50% of the continental attacks. This is in addition to 41 million potentially unwanted programmes (PUA), e.g. adware, pornware against a total of 102 million in Africa.⁹³

Even when a hacker group is identified, they still feel safe since it is difficult to locate them physically. Seventeen government ministries and state corporations' websites were breached and

⁹¹ UN General Assembly, “Resolution 70/237 - Developments in the Field of Information and Telecommunications in the Context of International Security.”

⁹² “Kenya Cyber Security Report 2015,” accessed May 17, 2021, <https://www.serianu.com/downloads/KenyaCyberSecurityReport2015.pdf>.

⁹³ Doreen Wainainah, “Kenya Reports Highest Cyber Attacks in Africa,” Business Daily, September 24, 2020, <https://www.businessdailyafrica.com/bd/corporate/technology/kenya-reports-highest-cyber-attacks-in-africa-2370444>.

defaced in Kenya in June 2019 by a hacker group named “Kurd Electronic Team.” They uploaded their logo on the websites, and it took several days to restore the websites.⁹⁴

2.6 SUMMARY

From this chapter, it is clear that awareness of existing and emerging threats in cyberspace determines the level of cyber security implementation since cyber security experts can only react to what they know. The incessant technical development and innovation by both states and cybercriminals in the ICT sphere since the 1960s call for awareness of emergent threats and full preparedness to counter any attacks. The internet has facilitated transnational crime, meaning no country is safe and thus forcing states to prioritise cybercrime management stratagems.

Developments in ICT have seen an exponential rise in the malicious use of ICT by both non-state and state actors, putting all states at risk with a bearing on international security and peace. It is apparent that cyber incidents have become more expensive, disruptive, and some had political undertones in the recent past.

The National Optic Fibre Backbone (NOFBI) project and the last mile County Connectivity Project (CCP) has implemented countrywide fibre optic connection with the target being the linkage of all county and sub-county headquarters to improve service delivery in government, in addition to enhancing bilateral relations through connectivity to South Sudan, Uganda and Ethiopia as part of

⁹⁴ Obar Mark Asuelaa, “We Have Taken Control of Kenyan Government’s Websites, Declares Hackers,” The Standard, June 3, 2019, <https://www.standardmedia.co.ke/counties/article/2001328320/ifmis-and-other-government-websites-under-cyberattack>.

the eastern Africa regional transport, trade and development facilitation project and the Horn of African Initiative.

All in all, Kenya's critical ICT infrastructure is exposed since we have a lot of unmanned spaces and many conflicting and uncoordinated developments (including road, power and water carriage systems), competition and malicious acts that inadvertently or otherwise interfere with the ICT infrastructure. While there are efforts to ensure type approval of ICT equipment, many more grey pieces of equipment get through unchecked. The bigger worry is the internal software that independent regulators do not verify. The challenge of attribution is universal and will need more effort to maintain safe cyberspace. Identifying the cyber offenders may not yield much since locating them physically is a tall order. Kenya has suffered website defacement and hacking incidents that have not been conclusively attributed. The interference with the critical infrastructure is widespread in Kenya, with Al-Shabaab destroying communications masts along the Kenya Somalia border, expansive and porous, leaving the region without telephone and internet connectivity. The UN has accused Kenya of interfering with Somalia's critical ICT infrastructure as it contends with the Al-Shabaab terror threat.

Krasner's assertion that international regimes allow for state and non-state actors convergence of expectations is apt in cyber (in)security and stability since there is no central control or authority in place.⁹⁵ However, arriving at multilateral agreements among the actors in this emerging domain

⁹⁵ S. Krasner, "Structural Causes and Regime Consequences: Regimes as Intervening Variables.," *International Organization* 2, no. Issue 36 (Spring 1982): 185-205.

is easier said than done. It has been difficult to achieve cooperation and the requisite coordination in an area involving both state and non-state actors.

The emerging cyber threats must thus be examined keenly, with measures put in place to minimise or counter the adverse effects of the aftermath of any intrusion and attack.

CHAPTER THREE - CONFIDENCE-BUILDING MEASURES FOR COLLABORATION AND COOPERATION

3.0 INTRODUCTION

Chapter Three presents an analysis of the confidence-building measures (CBMs) for collaboration and cooperation between local, regional and international stakeholders to ensure cyber security in line with the UN cyber norms.

3.1 CONFIDENCE-BUILDING MEASURES

According to the 2015 GGE report, confidence-building measures (CBMs) bolster international security and peace. Interstate collaboration, predictability, stability and transparency are enhanced if CBMs are in place. States are encouraged to follow the “Guidelines for Confidence-Building Measures”⁹⁶ adopted by the Disarmament Commission (A/S-15/3) in 1988 that was ratified by the General Assembly consensus by in resolution 43/78 (H) in a bid to build confidence to ensure a peaceful ICT environment. “CBMs are a verified instrument of international politics, which aims to prevent the outbreak of war or an (international) armed conflict by miscalculation or misperception of the risk, and the consequent inappropriate escalation of a crisis.”⁹⁷ Preventive crisis management amongst states is the essential tool in confidence building, which is difficult due to the internet’s unique features. Currently, cyberspace CBMs take the character of political pledges. In International relations, these are considered powerful tools.

⁹⁶ UN Office for Disarmament Affairs, “Group of Governmental Experts.”

⁹⁷ Dr Katharina Ziolkowski, “Confidence Building Measures for Cyberspace – Legal Implications” (NATO Cooperative Cyber Defence Centre of Excellence, 2013), www.ccdcoe.org.

To enhance trust and collaboration and decrease the risk of conflict, the 2015 GGE recommended that States contemplate voluntary confidence-building measures, including the following: Mechanisms for bilateral, regional and multilateral consultations, information sharing on critical infrastructures, investigations and capacity-building support.

The ICT4Peace Foundation and the Kenyan Government organised Africa's premier regional instruction workshop on “International Security and Diplomacy in Cyberspace.” In attendance were more than 30 participants drawn from the security, legal, diplomatic, and technical (ICT/Cyber Security) spheres. Civil society, the African union and 12 African states were represented. The capacity building program followed up on the 2013 recommendations of the “UN Group of Governmental Experts on developments in the field of information and telecommunications in the context of international security” and the October 2013 London Process’ Seoul Conference on Cyberspace.⁹⁸

3.2 COOPERATION AMONGST STATES AND PRIVATE SECTOR

States need to move from looking at cyber security as an entirely technical concern to a security undertaking. There is a need to standardise and integrate the policies in different sectors to form a coherent grand strategy. “The heterogeneity of actors that need to cooperate – at the horizontal

⁹⁸ ICT4Peace Foundation, “The Government of Kenya and ICT4Peace Foundation Co-Organize the First Regional Training Workshop in Africa on International Security and Diplomacy in Cyberspace,” *ICT4Peace Foundation* (blog), March 4, 2015, <https://ict4peace.org/activities/the-government-of-kenya-and-ict4peace-foundation-co-organize-the-first-regional-training-workshop-in-africa-on-international-security-and-diplomacy-in-cyberspace/>.

level (civilian and military; public and private) to the vertical level (national, regional, local) – to uphold cyber security creates additional coordination and cooperation problems.”⁹⁹ ¹⁰⁰

The 2015 GGE norm a) urges states to maintain international security and peace and cooperate to increase security and stability in ICTs utilisation. This is to avoid routines deemed to be injurious, or that may be risky to international security and peace. In addition, norm d) urges states to look at ways of cooperation to carry out information exchange and assist each other in prosecuting criminal and terrorist utilisation of ICT systems. The development of new measures in this respect is left at the discretion of the states. Threat intelligence reports indicate that cyber capabilities build-up by states is a segment of the cyber arms race and is seen mainly in intelligence and espionage circles. “The ambiguity about the intentions of other states and the practical inability to know whether such capabilities are used for offence or defence drive a traditional security-dilemma, increasing the motivations of military cyber commands and to intelligence agencies build-up (offensive) capabilities.” ¹⁰¹

Nations must be aware of the intelligence services in cyberspace since “they set practical norms of tolerable (cyber) espionage with far-reaching effects on state behaviour in cyberspace.”¹⁰² Intelligence agencies play a dual role in the cyber conflict – providing safety and the most significant danger. Cyber conflict could be regarded as an intelligence contest since cyber

⁹⁹ Deibert, R., *Black Code. Surveillance, Privacy, and the Dark Side of the Internet* (Toronto: McClelland & Stewart., 2013).

¹⁰⁰ Myriam Dunn Cavelty, Andreas Wenger, “Cyber Security Meets Security Politics: Complex Technology, Fragmented Politics, and Networked Science, Contemporary Security Policy.”

¹⁰¹ Buchanan, B., *The Cybersecurity Dilemma: Hacking, Trust, and Fear between Nations*. (Oxford: Oxford University Press., 2016).

¹⁰² Georgieva, I., “The Unexpected Norm-Setters: Intelligence Agencies in Cyberspace.,” *Contemporary Security Policy* 41 (2020): pp 33-54, <https://doi.org/doi:10.1080/13523260.2019.1677389>.

exploitation is costlier than neutralising released exploitation. The agencies need to be altered to reflect society's digitisation.

The 2015 GGE report further urges states to nominate appropriate contacts for policy and technical functions to deal with severe incidents in the ICT space. This is expected to morph into support systems to include multilateral, sub-regional, regional and bilateral discussions to “develop inter-state confidence-building and reduce the risk of misperception, escalation and conflict that may stem from ICT incidents.”¹⁰³ It is expected that this will promote transparency at all levels fostering confidence and encouraging the sharing of information with respect to transnational and national threats, vulnerabilities and hidden threats in ICT systems and hardware, and best practices for cyber security enhancement. This cooperation is also expected to include disclosing national critical infrastructure and endeavours to protect them, including policies and laws. Collaboration is required more for critical infrastructure weaknesses that go beyond national boundaries. Clearly spelt out technical, legal and diplomatic mechanisms to tackle ICT-related appeals and the enactment of voluntary state activities to classify ICT incidents in terms of the scale and gravity of the incident, to facilitate the exchange of information on incidents should be in place if meaningful cooperation is to take place.¹⁰⁴

The undertaking of actors in the state (e.g. state agencies) and other players like cybersecurity organisations look at the “strategic restraint and stability”¹⁰⁵ at the top end of the clash and

¹⁰³ “Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology: A Commentary.”

¹⁰⁴ Hitchens and Gallagher, “Building Confidence in the Cybersphere: A Path to Multilateral Progress.”

¹⁰⁵ Thomas Frear, Lukasz Kulesa, and Denitsa Raynova, “Russia and NATO: How to Overcome Deterrence Instability?” (European Leadership Network, 2018), <http://www.jstor.org/stable/resrep22119>.

permanent subversion and unpredictability at the lower side of the clash. The opacity of cyber operations and the inscrutability and ambiguity of actors involved is a big issue in grasping state behaviour in cyberspace. The linkage between socio-technical facets of cybersecurity and the socio-political undercurrents in cyber security politics is not very clear. Three overlapping approaches can be discerned – norms, governance and markets – meaning the development of cyber technologies is only partly manipulated by political deliberations. Political subtleties of cyber conflict can connect to cyber market undercurrents by applying perceptions from the international political economy and organisational and economic studies. Cyber security private organisations also have an impact on international and national practice by influencing state policies. These organisations are also crucial in attributing cyber infringements to particular perpetrators (including states, in some instances).¹⁰⁶

The 2014 Kenyan National Cyber Security Strategy avers that “cybersecurity is a complex, multidisciplinary challenge that requires coordination across a wide array of stakeholders.”¹⁰⁷ It was, therefore, envisioned that contributions by all concerned parties are included in a comprehensive governance model.

The Kenya ICT Action Network (KICTANet) is a multi-stakeholder non-profit platform for institutions and individuals interested in ICT regulation and policy. The NGO pushed for establishing and implementing a successful institutional, legal and policy framework to anticipate, detect, respond, and combat cyber threats to build resilience in the country’s cyber environment.

¹⁰⁶ Rid, T., Buchanan, B., “Attributing Cyber Attacks,” *Journal of Strategic Studies* 38 (2015): 4–37, <https://doi.org/doi:10.1080/01402390.2014.977382>.

¹⁰⁷ Ministry of Information Communications and and Technology, “National CyberSecurity Strategy” (GoK, 2014), <https://icta.go.ke/pdf/NATIONAL%20CYBERSECURITY%20STRATEGY.pdf>.

Towards the end of 2019, KICTANet launched a policy brief on Kenya’s cybersecurity framework examining forward-looking strategic actions and areas of concern. Fashioned as “6Ps, the brief calls upon all the stakeholders to Prioritize cybersecurity, put in appropriate Policies, invest in Preparation, put the People at the centre of cybersecurity initiatives, promote Partnership among multi-stakeholders, and ensure there is Political Will to achieve targets.”¹⁰⁸

Another organisation that works with the state in cyberspace matters is Global Partners Digital (GPD), which promotes a digital environment focusing on democratic values and human rights. GPD pushes for open policy processes that are inclusive, transparent, strategic and informed, with the coordinated engagement of public interest actors. GDP is funded by the UK government and is a crucial cog in “Promoting an inclusive and value-based approach to cyber policymaking in the Commonwealth.”¹⁰⁹

3.3 PROTECTION OF CRITICAL INFORMATION INFRASTRUCTURES

Two vital strategic concerns in cyber security are the low entry expenses for disruptive cyber munitions and the attendant defencelessness of critical infrastructures. This has lifted cyber security from “low politics to high politics and turned a mostly technical issue into an issue of international and national security politics.”¹¹⁰ The appreciation of increased vulnerabilities because of the tighter interlocking emerged from the expansion of the military network to the entire

¹⁰⁸ Kenya ICT Action Network, “Cybersecurity in Kenya: Strategizing for the Future” (kictanet, March 12, 2020), <https://www.kictanet.or.ke/wp-content/uploads/2020/03/Cybersecurity-in-Kenya-Strategizing-for-the-Future-Concept-Note-and-Programme.pdf>.

¹⁰⁹ Global Digital Partners, “Global Digital Partners Work,” May 2021, <https://www.gp-digital.org/our-work/>.

¹¹⁰ Dunn Cavelty, M., *The Normalization of Cyber-International Relations*. In O. Thränert, & M. Zapfe (Eds.), *Strategic Trends 2015: Key Developments in Global Affairs* (Zurich: Center for Security Studies., 2015).

society in the late 1990s, with ‘critical infrastructures’ being viewed as the pillar of modern civilisations.¹¹¹ Information infrastructures provision and facilitate the economies’ functioning, including military, government, commerce and the general society. Thus, the strategic threat discussed for years has been labelled “Electronic Pearl Harbour – a sudden destructive cyber-attack that would bring ICT reliant states to their knees in seconds.”¹¹²

The GGE norm (g) advises states to take suitable actions to defend their critical infrastructure ICT threats, considering General Assembly resolution 58/199 on establishing a global culture of cybersecurity and fortifying critical information infrastructures and other relevant resolutions. Norm (h) goes further to urge states to be responsive when proper requests for support are received from other states whose crucial infrastructure is exposed to malicious ICT acts. This includes mitigation of malicious cyber activity targeting another country but emanating from its territory, taking into cognisance the sovereignty obligations. The need for critical infrastructure protection was further emphasised by the UN General Assembly resolution 64/211 on the “Creation of a global culture of Cybersecurity and taking stock of national efforts to protect critical information infrastructures.”¹¹³

Protection of Critical Information Infrastructure is further reinforced in the Sustainable Development Goals (SDGs) number 9 that talks of building “resilient infrastructure” and the

¹¹¹ Myriam Dunn Cavelty, Andreas Wenger, “Cyber Security Meets Security Politics: Complex Technology, Fragmented Politics, and Networked Science, Contemporary Security Policy.”

¹¹² Schwartau, W., *Chaos on the Electronic Superhighway: Information Warfare*, Second Edition (New York, NY: Thunder’s Mouth Press, 1996).

¹¹³ United Nations, “Creation of a Global Culture of Cybersecurity and Taking Stock of National Efforts to Protect Critical Information Infrastructures” (United Nations, December 21, 2009), <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N09/474/49/PDF/N0947449.pdf?OpenElement>.

“promotion of inclusive and sustainable industrialization” in addition to “fostering innovation.”¹¹⁴

Digital technologies are more at the forefront, with the Covid-19 pandemic pushing many to socialise, work, learn, shop, pay bills and seek healthcare remotely.

Every state's responsibility is to safeguard vital infrastructure from human activities, including riots, war, arson, terrorism, and even malicious attacks like cyber-attacks. In addition, there are natural hazards to think of, including earthquakes, floods and even the effects of climate change and natural wear and tear. Kenya has a Critical Infrastructure Protection Unit (CIPU), a division of the Administration Police service,¹¹⁵ signalling Kenya’s classification of critical infrastructure as a national security concern. A firmer Critical Infrastructure Protection framework is needed since the country suffers huge losses annually due to either degradation or damage to the critical infrastructure and the resultant disruption to private and government service delivery and business.¹¹⁶

It is instructive to note that a Critical Infrastructure Protection (CIP) bill has not been passed into law since 2016. The bill defines “Critical Infrastructure Assets to mean designated assets or facilities, whether owned by private or public entities which are designated as such under this Act as essential to the delivery of essential services to Kenyans for their economic and social wellbeing, and which if destroyed, degraded or rendered unavailable, would impact on the social or economic

¹¹⁴ Jensen, L (ed), “The Sustainable Development Goals Report 2020” (UN Department of Economic and Social Affairs, 2020), <https://unstats.un.org/sdgs/report/2020/The-Sustainable-Development-Goals-Report-2020.pdf>.

¹¹⁵ NPS, “Inspector General Visits Administration Police Service Units,” July 19, 2019, <https://www.nationalpolice.go.ke/2015-09-08-17-56-33/news/294-inspector-general-visits-to-aps-units.html>.

¹¹⁶ Kingori Choto, “Secure Critical Infrastructure For Sustainable Development,” *Capital FM News* (blog), July 28, 2020, <https://www.capitalfm.co.ke/news/2020/07/secure-critical-infrastructure-for-sustainable-development/>.

wellbeing of the nation or affect Kenya’s ability to conduct national defence and security;”¹¹⁷ The bill proposes a committee to research on global trends and assess and evaluate the security needs of the critical infrastructure, receive intelligence and consequently in collaboration with the office of the Inspector-General of Police, ensure that critical infrastructure assets are offered continued security protection and surveillance. ¹¹⁸

An attack of the same enormity as the 2007 Estonian one would result in widespread harm affecting privately owned critical infrastructure in telecommunications, power and finance – which are generally inadequately protected and already suffer constant intrusion. Relying on private investment for protection and prevention while using public funds for prosecution results in a defensive strategy that “is simply the sum of dispersed decisions of individual users and businesses - a bifurcated approach to network security.”¹¹⁹

3.4 SUPPLY CHAIN INTEGRITY

UN GGE norm (i) deals with supply chain integrity and counsels states to “ensure the integrity of the supply chain so that end users can have assurance in the security of ICT products.”¹²⁰ The integrity check ensures the limitation of the spread of malicious implements and techniques and checks on unsafe concealed functions. For this to be efficacious, there needs to be intentional cooperation with the private sector. The private sector has a profit motive, and to capture the

¹¹⁷ Stanley K. Manduku, “Securing Kenya: Overview and Implications of the Critical Infrastructure Protection Bill” (ISACA Kenya Annual Conference, Mombasa, Kenya, 2016), <http://isaca.or.ke/downloads/Overview-and-Implications-of-the-Critical-Infrastructure-Protection-Bill-Stanley-manduku.pdf>.

¹¹⁸ GoK, “The Critical Infrastructure Protection Bill, 2019” (GoK, 2019).

¹¹⁹ Christopher J. Coyne and Peter T. Leeson, “National Security Threats in Cyberspace,” *American Bar Association*, 2009, pp 475-76.

¹²⁰ “73/27. Developments in the Field of Information and Telecommunications in the Context of International Security.”

market, they have to present cutting-edge systems and demonstrate analytical capabilities whilst maintaining trade secrets and confidentiality agreements.¹²¹

The suppliers of ICT systems and the associated hardware have as their customers, governments, corporations and individuals – whose requirements may be at cross purposes with one another. Their in-depth analysis and reports show that cyber security firms like Symantec are instrumental in understanding attacks like the Stuxnet. It should be noted that the frontier between security professionals and hackers is blurred. Cyberspace has been portrayed as a landscape of “persistent threat, systemic vulnerability, and intelligence opacity, a classic “noir” chronicle that results from systemic economic insufficiencies (distorted incentives for protection) and systemic political deficiencies (black markets for new exploits).”¹²²

Techno Nationalism comes into play in supply chain integrity with states conducting as merchants would by linking their technological capabilities and foreign business interactions to matters of economic prosperity, social stability and eventually to national security interests. This has led to restrictions and controls as far as exports are concerned.¹²³ In this type of nationalism, it is possible for supply chain integrity to be compromised either by supplying inferior products or planting bugs and spy software in ICT equipment and systems to collect information illegally or otherwise

¹²¹ Egloff, F. J., Wenger, A, “Public Attribution of Cyber Incidents. In F. Merz (Ed.), *CSS Analyses in Security Policy*.”

¹²² Shires, J., “Cyber-Noir: Cybersecurity and Popular Culture.” *Contemporary Security Policy* 41 (2020): pp 82-107, <https://doi.org/doi:10.1080/13523260.2019.1670006>.

¹²³ Alex Capri, “US-China Techno-Nationalism and the Decoupling of Innovation,” *The Diplomat*, September 10, 2020, <https://thediplomat.com/2020/09/us-china-techno-nationalism-and-the-decoupling-of-innovation/>.

undermine the efficacy of the ICT equipment. The turf wars between communications giants Cisco from USA and Huawei from China is the poster example of this fight.

3.5 AUTHORIZED EMERGENCY RESPONSE TEAMS

Norm (K) states that “States should not conduct or intentionally support activity to harm the information systems of the authorized emergency response teams (sometimes known as computer emergency response teams or cybersecurity incident response teams) of another State.”¹²⁴ This norm speaks to the state use of authorised emergency response teams to engage in unpleasant international activity as being proscribed.

Authorised emergency response teams are supplementary confidence-building instruments and cooperation on a multilateral and bilateral basis. The emergency response teams will allow diplomatic, legal and technical methods to deal with ICT infrastructure connected requests, including personnel exchanges to support law enforcement, incident response and even academic and research collaboration. National Computer Emergency Response Teams or Cyber Security Incident Response Teams include focal points for investigative assistance and malicious ICT use information exchange. Countries are encouraged to enlarge and assist emergency response teams in developing their information exchange capacities on attack patterns, vulnerabilities, best practices, exercises, incident handling and the necessary sector-based and regional cooperation. In all these, the cooperation should be consistent with international and national law and support

¹²⁴ Kello, L., *The Virtual Weapon and International Order*. (New Haven, CT: Yale University Press, 2017).

states in probing ICT-related transgressions, including using ICTs for terrorist purposes and mitigation of ICT activity deemed malicious emanating from foreign territory.

The National Kenya Computer Incidence Response Team – Coordination Centre (National KE-CIRT/CC) is the country’s point of contact for cybersecurity issues. It is a multi-agency collaboration setup that coordinates cybersecurity nationally. The team notes that the rapid digital adoption has increased the “attack surface” with cybercriminals optimizing their attack methods to improve their successful hit frequencies – including the use of botnet attacks, trojans, ransomware, phishing globally and other industrialised social engineering and malware deployments. The CIRT has local and international collaborations geared towards observation and monitoring, analysis and response to cyber threats through the National KE-CIRT/CC Cybersecurity Committee (NKCC) that boasts of membership from the telecommunications, internet service providers (ISP), financial and academic sectors, in addition to law enforcement agencies. The CIRT offers technical advisories and cyber appreciation campaigns geared towards hygiene and readiness in cyberspace. In the first quarter of 2021, the CIRT discovered 28,247,819 cyber threat events, reducing from 56,206,097 in the previous quarter. It also issued 25,506 advisories, over an 18% increase compared to the previous quarter.¹²⁵

3.6 CAPACITY BUILDING

While states bear the prime responsibility for the safety of citizens and national security that increasingly includes the ICT environment, many states lack the adequate capability to offer

¹²⁵ Communications Authority of Kenya, “National Ke-CIRT/CC Cybersecurity Report For The Period January To March 2021” (Nairobi, 2021), https://ke-cirt.go.ke/wp-content/uploads/2021/04/Quarter-3-FY-2020_21-National-KE-CIRT_CC-Report_compressed-3.pdf.

protection in the ICT sphere making critical infrastructure and citizens vulnerable and creating a refuge for malicious actors. International cooperation in ICT capacity building assistance with a particular focus on ICT security is necessary for international security as it improves the capability of states for collective engagement. The UN GGE concurred that capacity-building actions should seek to foster the use of ICTs for peaceful functions. The 2010 report asked states to seek opportunities to aid capacity building in developing states. 2013 reiterated the need for the international community “to bridge the divide in the security of ICTs and their use.”¹²⁶ Capacity building is much more than skills transfer to developing countries from the developed ones, as all states can learn from threats faced and thoughtful responses. Critical infrastructure security, technical skills development and applicable legislation and regulatory framework are crucial for capacity building.

Regional arrangements for capacity building are beneficial as they consider particular political, geographic, cultural, economic, social and cultural nuances, allowing a tailor-made approach. The bilateral or multilateral initiatives assist in efficacious mutual assistance amongst states in reaction to ICT incidents with the further input of the civil society, private sector, academia and even the United Nations and its agencies. Many of the Kenya institutions of higher learning are now teaching ICT courses, with a few of them concentrating on cyber security. The accessibility of employable talent is one of the essential foundations for developing both IT services and IT-Enabled Services (ITES). McKinsey Global Institute reports that approximately only 13% of the

¹²⁶ UN, “UN GGE Report 2013 (A/68/98*)” (GIP Digital Watch, 2013), <https://dig.watch/un-gge-report-2013-a6898>.

generalist graduates had basic employment qualifications, with trainability and willingness to work in the sector as additional vital considerations.¹²⁷

In 2017, the ICT Cabinet Secretary in Kenya indicated collaboration with the US Government targeting digital economy and cyber security to enhance training in the protection and security of information assets and increase public confidence in internet use.¹²⁸

3.7 SUMMARY

From this chapter, it is clear that CBMs for collaboration and cooperation between local, regional and international stakeholders in line with the UN Cyber Norms determine the level of cyber security. CBMs, as a verified instrument in international politics, aim to avert the outbreak of armed clashes by misperception or miscalculation of risk. It is all about preventive crisis management.

The African Union, Kenyan Government and NGOs like ICT4Peace have organised regional conferences on international diplomacy and security in cyberspace with participants from the security, legal, diplomatic and technical disciplines. This is a result of the 2013 UN GGE recommendations and the London Process.

In terms of cooperation amongst states and the private sector, there is a need to move from regarding cyber security as a purely technical concern to looking at it as a security undertaking.

¹²⁷ Alexander Klimburg and Hugo Zylberberg, “Cyber Security Capacity Building: Developing Access” (Norwegian Institute of International Affairs, 2015).

¹²⁸ Cheruiyot Korir, “Kenya to Collaborate with US in Cyber Security,” *Ministry of ICT, Innovation and Youth Affairs* (blog), June 22, 2017, <https://ict.go.ke/kenya-to-collaborate-with-us-in-cyber-security/>.

There is a need to coordinate and amalgamate the policies in different sectors to form a coherent grand strategy. To uphold cyber security, the vertical bias (local, regional and national) and the horizontal bias (public and private; civilian and military) cooperation generates additional coordination and cooperation problems.

The first norm urges States to maintain global peace and security and cooperate to boost stability and security in using ICTs to avoid harmful practices or pose threats to international security and peace. The fourth norm is somewhat related and exhorts states to look at ways of cooperation to carry out information exchange and assist each other in prosecuting criminal and terrorist utilisation of ICTs. While ordinary firms in the competitive space may take good protective care of their cyberspace, those in uncompetitive disciplines such as the utility providers may be unlikely to defend their systems against foreign state-backed adversaries. The development of new measures in this respect is left at the discretion of the states.

The 2014 Kenyan National Cyber Security Strategy sees cybersecurity as a composite, multidisciplinary question that requires synchronization across a wide assortment of stakeholders. Contribution by all concerned parties is included in a comprehensive governance model. The Kenya ICT Action Network (KICTANet) has pushed for the establishment and implementation of a successful institutional, legal and policy framework, fashioned as 6Ps - Prioritize cybersecurity, put in appropriate Policies, invest in Preparation, put the People at the centre of cybersecurity initiatives, promote Partnership among multi-stakeholders, and ensure there is Political Will to achieve targets. UK funded Global Partners Digital (GPD) promotes an inclusive and value-based approach to cyber policymaking in the commonwealth countries with a bias towards open policy

processes that are inclusive, transparent, strategic and informed, with the coordinated engagement of public interest actors.

The point of contact in Kenya is in the CIRT that is in place at the Communications Authority. Much more needs to be done in capacity building and the protection of critical infrastructure. Key is the enactment of the Critical Infrastructure Protection bill and the equipping of the national CIRT.

Authorised emergency response teams are a welcome addition to confidence-building instruments and cooperation on a multilateral and bilateral basis. The emergency response teams will allow diplomatic, legal and technical methods to deal with ICT infrastructure connected requests, including personnel exchanges to support law enforcement, incident response and even academic and research collaboration. The CIRT has local and international collaborations geared towards observation and monitoring, analysis and reaction to cyber threats through the National KE-CIRT/CC Cybersecurity Committee (NKCC) that boasts of membership from the telecommunications, Internet service providers (ISP), financial, academic sectors, in addition to law enforcement agencies. The CIRT offers technical advisories and cyber appreciation campaigns geared towards hygiene and readiness in cyberspace. In the first quarter of 2021, the CIRT discovered 28,247,819 cyber threat events, reducing from 56,206,097 events reported in the previous quarter. It also issued 25,506 advisories, over an 18% increase compared to the previous quarter.

The seventh norm advises states to take suitable measures in the fortification of their critical infrastructure ICT threats. This includes mitigation of malicious cyber activity targeting another country but emanating from its territory, taking into cognisance the sovereignty obligations. At the

same time, the eighth urges states to be responsive when proper requests for assistance are received from other territories whose critical infrastructure is exposed to malicious ICT acts to safe guard vital infrastructure from human activities, including riots, war, arson, terrorism. The Sustainable Development Goals (SDGs) number 9 weighs in and talks of building robust infrastructure and the promotion of all-encompassing and balanced industrialization in addition to fostering innovation. Digital technologies are more at the forefront, with the Covid-19 pandemic pushing many to socialise, work, learn, shop, pay bills and seek healthcare remotely.

In addition, there are natural hazards to think of, including earthquakes, floods and even the effects of climate change and natural wear and tear. Kenya has a Critical Infrastructure Protection Unit (CIPU), a division of the Administration Police service, signalling Kenya's classification of critical infrastructure as a national security concern. A firmer Critical Infrastructure Protection framework is needed since the country suffers huge losses annually due to either degradation or damage to the critical infrastructure and the resultant disruption to private and government service delivery and business. It is instructive to note that a Critical Infrastructure Protection (CIP) bill has not been passed into law since 2019.

In terms of supply chain integrity, it should be noted that suppliers of ICT systems and the associated hardware have as their customers, governments, corporations and individuals – whose requirements may be at cross purposes with one another. The ninth norm asks states to ensure the integrity of the supply of technological systems and devices so that end users can have an assurance of ICT products' safety. The integrity check ensures the limitation of the propagation of malicious implements and techniques and checks on unsafe concealed functions. Techno-nationalism plays a significant role in this area.

As far as capacity building is concerned, while states assume the primary concern for the safety of citizens and national security that increasingly includes the ICT environment, many states lack the adequate capability to offer protection in the ICT sphere making critical infrastructure and citizens vulnerable and creating a refuge for malicious actors. International cooperation in ICT capacity building assistance with a particular focus on ICT security is indispensable for worldwide security as it improves the capacity of states for collective action. Capacity building is much more than skills transfer to developing countries from the developed ones, as all states can learn from one another regarding threats faced and effective responses. Security of critical infrastructure, technical skills development and applicable regulatory and legislative framework are fundamental areas for capacity building.

Regional arrangements for capacity building are beneficial as they consider particular political, geographic, cultural, economic, social and cultural nuances, allowing a tailor-made approach. The bilateral or multilateral initiatives assist in efficacious mutual assistance amongst states in response to ICT incidents with further input from academia, the private sector, civil society and even the United Nations and its agencies. Many of the Kenya institutions of higher learning are now teaching ICT courses, with a few of them concentrating on cyber security. The accessibility of employable talent is one of the most critical foundations for developing IT services and IT-Enabled Services (ITES). McKinsey Global Institute reports that approximately only 13% of the generalist graduates had basic employment qualifications, with trainability and willingness to work in the sector as additional vital considerations.

CHAPTER FOUR - KENYAN LEGAL AND POLICY FRAMEWORK AND ITS EFFECTIVENESS

4.0 INTRODUCTION

Chapter Four assesses the Kenyan legal and policy framework and its effectiveness in supporting the implementation of the UN Cyber Norms.

4.1 INTERNATIONAL LAW

According to the 2013 GGE report, states adherence and obligations to international law and, more so, the United Nations Charter is relevant and essential to upholding “an open, secure, stable, accessible and peaceful ICT environment.”¹²⁹ The principles of international law and the UN charter apply to cyberspace are sovereign equality, just, secure and peaceful settlement of international disputes and international relations that do not threaten or use force against other states' political independence and territorial integrity. Regard for human rights and fundamental freedoms also come into play is also a state’s obligation under international law. The conduct of states’ sovereignty and international principles and norms apply to ICT-related activities and authority over territorial ICT infrastructure.

Resolution 68/243 made by the UN General Assembly gave views on applying international law to states’ ICT utilisation, including control over ICT infrastructure within their territorial control. The use of proxies to commit internationally wrongful acts is against international law, allowing

¹²⁹ “Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology: A Commentary.”

non-state actors to use state territory to carry out such acts. The resolution further reiterates that ICTs should be used peacefully for humanity's common good, “adhering to the principles of humanity, necessity proportionality, and distinction.”¹³⁰ Scholars acknowledge that “technical and structural characteristics of cyberspace fundamentally challenge some of IR’s core concepts—power, sovereignty, territoriality—so that they lose traction for explaining state behaviour.”¹³¹ There is little explanation for why the power to subvert seems to override the power to coerce and attract in cyberspace. The difference between reciprocally acceptable espionage in pursuit of strategic muscle and unacceptable political intrusion in the internal affairs of another state is blurred.

4.2 INTERNATIONALLY WRONGFUL ACTS ATTRIBUTABLE TO STATES

Norm (C) draws from the 2013 GGE report, which asserts that “States must meet their international obligations regarding internationally wrongful acts attributable to them. The reference to internationally wrongful acts stems from the 2002 General Assembly resolution 56/83 on the responsibility of States for internationally wrongful acts. It stipulates that “there is an internationally wrongful act of a State when conduct consisting of an action or omission: (a) is attributable to the State under international law; and (b) constitutes a breach of an international obligation of the State.”¹³² Commitments as far as internationally wrongful acts attributable to

¹³⁰ Michael N. Schmitt, ed., *Tallinn Manual 2.0 on The International Law Applicable to Cyber Operations*.

¹³¹ Fischerkeller, M., *Offense-Defense Theory, Cyberspace, and the Irrelevance of Advantage*. (Alexandria, VA: Institute for Defense Analysis, 2018).

¹³² Hill, “Promoting Stakeholder Action Against Botnets and Other Automated Threats.”

states under international law must be met by states.”¹³³ It should be noted that ICT activity launched or originating a state’s territorial ICT infrastructure could be inadequate in attributing the undesirable activity to the state and should be substantiated. Also, States must not use proxies to commit internationally wrongful acts. States should seek to guarantee that non-state actors do not utilise their territories for illegitimate application and use of ICTs.

Experts are awakening to the reality of cyber operations that are persistent across the conflict continuum. While strategic Cyberwar or cyber terrorism (individual out of the blue cyber-attacks targeting critical ICT infrastructure) has been limited, low-level conflict with political and strategic implications has become more significant in international relations. Mounting testimony suggests that both non-state and state actors attempt to influence information and also cause disruptions “before and during political disputes or conflicts.”¹³⁴ ICT network attacks have also come to the forefront from the 2009 *GhostNet* and the 2010 *Stuxnet* - the covert and unremitting cyber operations directed at the functionality and information of particular entities. This points to the conclusion that there is an interconnection between the professional cyber-crime market and covert state action, which acquired an international outlook in the *Snowden* leaks.¹³⁵

Open attribution of cyber occurrences by threat intelligence organisations and states has risen in the recent past despite the economic and political motives not to disclose the evidence comprehensively. The fragmentation of accountability and authority exacerbates the attribution

¹³³ Akhand Pratap Rai and Aman Mani Tripathi, “U.S. Sanction against Iran: Breach of International Obligation,” *Modern Diplomacy*, June 2020, <https://moderndiplomacy.eu/2020/06/23/u-s-sanction-against-iran-breach-of-international-obligation/>.

¹³⁴ Baezner, M., *Hotspot Analysis: Synthesis 2017: Cyber-Conflicts in Perspective* (Zurich: Center for Security Studies (CSS), ETH Zurich., 2018).

¹³⁵ Maurer, T., *Cyber Mercenaries: The State, Hackers and Power*. (Cambridge: Cambridge University Press, 2017).

challenge and forms broader repercussions of cyber conflicts dynamics for governance and government. Networked governance implies that cyberspace is made up of network infrastructure and technical devices in addition to socio-political institutions. There is a lack of dependable knowledge and unrestricted transparency. Consequently, attribution claims endure as contested in the public domain, emasculating the legality of state reaction – from insurance settlements and criminal procedures to global cooperation mechanisms and escalation restraint.¹³⁶

“An important precondition for upholding the credibility of both cyber norms and cyber deterrence is the (sometimes public) attribution of cyber incidents to a politically responsible actor.”¹³⁷

In the ongoing war against terror, there have been allegations of Somali telecommunications companies working in cahoots with the Al-Shabaab terror group to destabilise critical infrastructure in Kenya. Attacks on communications masts on the Kenyan side have been on the increase, according to confidential reports. The Somali telco firm is keen to dominate the border and up to 50 kilometres into Kenya to the disadvantage of the Kenyan communications organisations. The Al-Shabaab group has been paid US\$3 million to finance its operations. They destroy vital communication infrastructure resulting in communication blackout for the security enforcers and the local communities. “The Somali company also uses its money remittance

¹³⁶ Hofmann, J., “Multi-Stakeholderism in Internet Governance: Putting a Fiction into Practice.,” *Journal of Cyber Policy* 1 (2016): 29-49., <https://doi.org/doi:10.1080/23738871.2016.1158303>.

¹³⁷ Egloff, F. J., Wenger, A, “Public Attribution of Cyber Incidents. In F. Merz (Ed.), *CSS Analyses in Security Policy*.”

platform in Somalia to run al-Shabaab’s day-to-day operations including the collection of taxes, commonly known as Zakat.”¹³⁸

According to the former ITU Secretary-General, Hamadoun Toure, cyber-victimisation has increased since cybercriminals view Africa as a safe sanctuary where their impunity and illegal acts would not be punished. Africa recorded 24 million malware incidents in 2016 and was regarded as the region with the most incredible growth in cyber-crime.¹³⁹

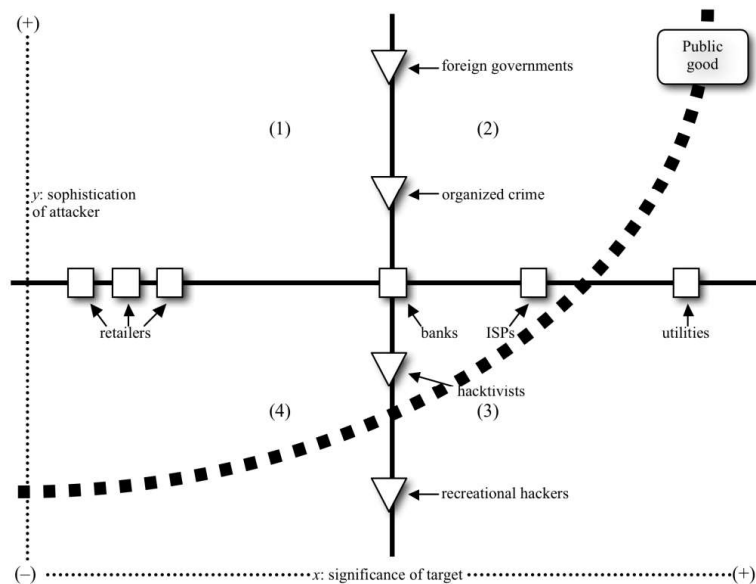


Figure 3 Significance of target vs. sophistication of attacker (Source Sales, 2013)

The range of possibilities of attackers can swing from recreational hackers to foreign state-sanctioned operatives, as indicated in figure 3 above, with firms targeted ranging from insignificant

¹³⁸ Walter Menya, “Somalia Based Telecom Company Financing Terror Group to Destroy Communication Masts in Kenya to Increase Its Market Share,” *Daily Nation (Kenya)*, September 9, 2019, <https://www.business-humanrights.org/en/latest-news/somalia-based-telecom-company-allegedly-financing-terror-group-to-destroy-communication-masts-in-kenya-to-increase-its-market-share/>.

¹³⁹ Nir Kshetri, “Cybercrime and Cybersecurity in Africa,” *Journal of Global Information Technology Management*, vol 22, no. issue 2 (2019): pp 77-81, <https://doi.org/DOI: 10.1080/1097198X.2019.1603527>.

firms in competitive markets where there are many choices (e.g. retailers) to utility providers which are strategically significant with very few options. In between are the telecommunications providers and financial institutions, as depicted in the X-axis.¹⁴⁰

Cyber-crime perpetrators are the Y-axis, starting with recreational hackers at the bottom of the scale looking for a digital joy ride. Next are hacktivists – skilled hackers who have a political motive for attacking particular systems, e.g. the group Anonymous that launched denial of service attacks on financial establishments that stopped their clients from donating to *WikiLeaks*, the publisher of classified documents. Organised criminals (mainly found in Eastern Europe and Russia) come next in hierarchy and include terrorist groups. These criminals have a financial motive behind their intrusions. Computers seized from Al-Qaeda indicated that they were in the process of setting up a cyber-terrorism academy targeting SCADA systems in the USA. Foreign states intelligence and military groups come at the top and boast of sophisticated methodologies that enable them to penetrate secure systems. It is alleged that Chinese spies infiltrated internet giant Google’s servers in a bid to intercept communication by the Dalai Lama.¹⁴¹

4.3 RESPECT FOR HUMAN RIGHTS

Norm (E) states that “in ensuring the secure use of ICTs, should respect Human Rights Council resolutions 20/8 and 26/13 on the promotion, protection and enjoyment of human rights on the Internet, as well as General Assembly resolutions 68/167 and 69/166 on the right to privacy in the

¹⁴⁰ Randal C. Picker, “, ‘Cyber Security: Of Heterogeneity and Autarky’ (John M. Olin Program in Law and Economics Working Paper No. 223, 2004),” n.d.

¹⁴¹ Nathan Alexander Sales, “Regulating Cyber Security,” *Northwestern University Law Review* Vol. 107, no. No. 4 (2013): pp 1503-1568.

digital age, to guarantee full respect for human rights, including the right to freedom of expression.”¹⁴² The widespread invasive cyber capabilities give states superfluous means for citizens control – within their domestic territory and abroad as well – as demonstrated by increased development of spyware and surveillance tools in addition to offensive dictates.¹⁴³ On the other hand, as reported earlier, Kenya has also been blamed for interfering with critical ICT infrastructure in Somalia. They try to contain Al-Shabaab and maintain law and order. This interference disrupts emergency and commercial communication and makes the receipt of diaspora remittances more difficult.¹⁴⁴

In neighbouring Uganda, there was a five-day internet blackout during the Presidential elections in January 2021. According to human rights activists, internet blackout should be based on the international human rights codes of “proportionality, necessity and legality” and not emotional retribution mechanisms.¹⁴⁵

4.4 LEGAL ENVIRONMENT

At the end of 2016, the African Union Commission (AUC), in conjunction with Symantec, the cyber security firm, gave a report indicating that 11 countries in Africa, excluding Kenya, had specific provisions and laws to deal with cyberspace issues. A dozen countries had partial laws,

¹⁴² Hill, “Promoting Stakeholder Action Against Botnets and Other Automated Threats.”

¹⁴³ Deibert, R., *Black Code. Surveillance, Privacy, and the Dark Side of the Internet.*

¹⁴⁴ Odula, “UN Links Kenyan Military to Attacks on Somalia’s Top Telecom.”

¹⁴⁵ APC, “Uganda 2021 General Elections: The Internet Shutdown and Its Ripple Effects,” *Association for Progressive Communications*, 2020, <https://www.apc.org/en/news/uganda-2021-general-elections-internet-shutdown-and-its-ripple-effects>.

while thirty states had no significant cyber-crime legal framework. Kenya has since joined the bandwagon.¹⁴⁶

The 2014 Convention of Cyber Security and Personal Data Protection (Malabo Convention) is the continent's central policy guideline in cyber issues. It mirrors the Convention on Cybercrime (ETS No. 185) formulated by the Council of Europe. In East Africa, only Rwanda has signed the convention. The main highlights of the AU Convention stress data protection against exploitation by third parties and cybercriminals, the inauguration of state computer emergency teams, stronger government and private sector cooperation. The convention also has provisions for dual criminality, allowing suspect's prosecution in the country of incidence or their home country – ensuring cooperation and avoiding conflict of laws. The Convention statutes also envisioned mutual legal assistance in intelligence sharing and collaboration in investigations between different states.¹⁴⁷

Rwanda, Uganda and Kenya are taking baby steps in harmonising cybersecurity practices, data protection and collaboration in prosecution and investigation of incidences.¹⁴⁸

Through its Ministry of ICT, Innovation and Youth Affairs, the Government of Kenya came up with a National Cybersecurity Strategy in 2014 to support the National ICT Master Plan and in the

¹⁴⁶ Kshetri, "Cybercrime and Cybersecurity in Africa."

¹⁴⁷ Africa Union Commission, "Africa Union Convention on Cyber Security and Personal Data Protection," 2014, https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf.

¹⁴⁸ Mercy Muendo, "What's Been Done to Fight Cybercrime in East Africa," *The Conversation*, December 2, 2019, <https://theconversation.com/whats-been-done-to-fight-cybercrime-in-east-africa-127240>.

Vision 2030. While promoting ICT adoption for economic growth, the strategy defines the country's cybersecurity vision, goals and objectives.¹⁴⁹

The country's cyber security is governed by the 2010 constitution (article 31), the Data Protection Act no. 24 of 2019, the Computer Misuse and Cyber Crimes Act no. 5 of 2018, and the initial 1998 Kenya Information and Communication Act no. 2, which came into being after the Kenya Post and Telecommunications Corporation was divided into three separate bodies - and the Communication Commission of Kenya (CCK) as the regulatory and licensing authority of the government, Postal Corporation of Kenya (to provide postal and courier services) and Telkom Kenya (for telecommunication services).¹⁵⁰

The Computer Misuse and Cyber Crimes Act enumerate offences relating to computer systems, touch on international cooperation, and establish the National Computer and Cybercrimes Coordination Committee. The law was challenged in court over freedom of expression and the right to privacy, among other provisions. The challenge was set aside after a two-year court battle. Thus, the country has provisions for some emerging issues, including interference and interception of data. Fake news, cyber harassment, child pornography, cybersquatting, identity theft and electronic fraud are among the highlights in cyber-crime law. Organisations now are responsible for ensuring unauthorised persons have no access to personal data and restricted computer systems

¹⁴⁹ Ministry of Information Communications and and Technology, "National CyberSecurity Strategy."

¹⁵⁰ Melanie Munyori and Judy Mumbi, "The Rise in Cyber Crimes in Kenya: How Effective Are Our Laws?," *Wamae and Allen Legal Update* (blog), January 15, 2020, <https://wamaeallen.com/the-rise-in-cyber-crimes-in-kenya-how-effective-are-our-laws/>.

under their purview. Negligent organisations will be liable to pay fines, with employees facing jail times as well upon conviction.¹⁵¹

The Data Protection Act of 2019 (DPA) was put in place to ensure the protection of personal data. The Act follows international data protection standards and principles, especially the European General Data Protection Regulations (GDPR).¹⁵² It controls the gathering, processing, storage and handling of personal data, by non-resident and resident data processors and controllers, for cases where data subjects are in Kenya. It also outlines data subjects' rights.¹⁵³

4.5 SUMMARY

It is clear that the legal and policy frameworks in place in line with the UN Cyber Norms determine the level of cyber security. While most legal provisions are in place, more needs to be done regarding end-user awareness and cooperation with external jurisdictions to ensure a safe cyberspace. The challenge of attribution calls for more expertise and alertness by government agencies in protecting cyberspace. The cyber legal space is still hazy and does not cover all eventualities since this is a growing area with a plethora of actors whose interests are most of the time at cross purposes.

¹⁵¹ Mahesh Acharya and Neema Oriko, "Kenya's Computer Misuse and Cybercrimes Act, 2018: Suspended Provisions Now Effective," February 21, 2020, <https://www.lexology.com/library/detail.aspx?g=ed5937e1-b7e3-42bb-baa9-2cef53cced5a>.

¹⁵² EU, "Regulation (EU) 2016/679 of The European Parliament and of the Council" (Official Journal of the European Union, April 27, 2016), <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679>.

¹⁵³ Ariana Issaias, "Data Protection Update: Recruitment of a Data Commissioner Begins," April 1, 2020, <https://www.bowmanslaw.com/insights/intellectual-property/data-protection-update-recruitment-of-a-data-commissioner-begins/>.

Other jurisdictions have declared cyber as the fifth theatre of war after the sea, land, air and space. This calls for establishing a detailed convention to guide the dealings of states and their subjects in this new realm. The International Regimes Theories may be inadequate in addressing this sphere since cyberspace has an increasingly military angle.

The legal provisions need to impress upon all the field actors with increased capacity building and awareness sessions. Even in developed countries, the poor state of cyber defence is because the analytical framework is deficient. At the same time, the policy and legal instruments are undertheorized, leaning towards the law of armed conflict or criminal law¹⁵⁴.

¹⁵⁴ Matthew C. Waxman, "Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)," *Yale Journal of International Law* Vol 36, no. No. 2 (2011), <https://digitalcommons.law.yale.edu/yjil/vol36/iss2/5>.

CHAPTER FIVE – RESEARCH FINDINGS AND ANALYSIS

5.0 INTRODUCTION

This chapter presents, analyzes and interprets the research findings.

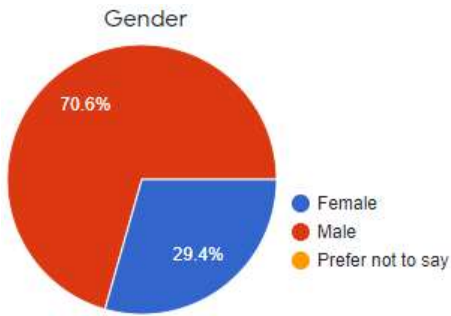
5.1 FINDINGS

5.11 DEMOGRAPHICS

The study targeted 100 respondents from a cross-section of organisations dealing with cyber security either as policymakers, policy implementers or policy users. The respondents were drawn from several organisations, including the Ministry of Information and Communications Technology, Innovation and Youth Affairs, Ministry of Interior, Ministry of Defence/ Kenya Defence Forces, the National Treasury, the Directorate of Criminal Investigations, the Directorate of Public Prosecutions, the Judiciary, ICT Authority, Communications Authority of Kenya, National Cyber Control Centre, Telecommunications and Internet Service Providers, Bankers Association of Kenya, The East African Science and Technology Commission (EASTECO), Universities – Nairobi, Strathmore, Jomo Kenyatta, Oxford, Commonwealth Telecommunications Organisation, Global Forum for Cyber Expertise, Various Government Parastatals, Telecommunications Service Providers Association, Central Bank of Kenya and Kenya Bankers Association.

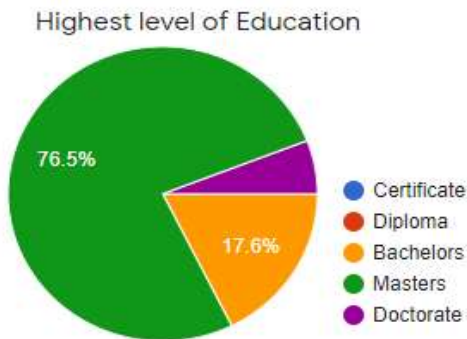
These organisations are vital to the management and use of cyberspace in the Kenyan context. Due to the confidential nature of cyber security matters, there was hesitation in some quarters to give

information or answer all the questions, both in the questionnaire and in the key informant interviews.



A total of 68 responses were received, from 48 males and 20 from females, as illustrated in figure 3. This ratio is representative of the gender distribution in the ICT industry.

Figure 4 Respondents' Gender Distribution (Source Author, 2021)



It is instructive to note that four-fifths of the respondents have master's degree qualifications and above, as displayed in figure 4. Cyber security is a speciality of Computer Science and Information Technology disciplines, and thus advanced studies are needed for policy formulators and implementers.

Figure 5 Respondents' Level of Education (Source Author, 2021)

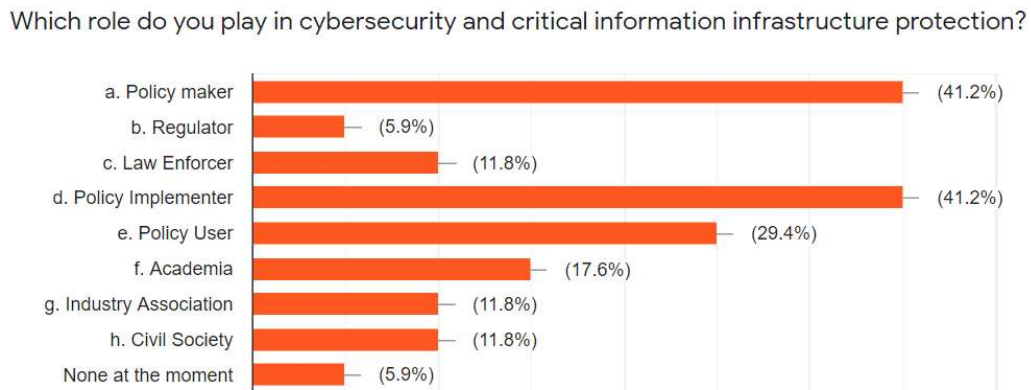


Figure 6 Respondent's Role in Cyber Security (Source Author, 2021)

Over 40% of the respondents were both in policymaking and policy implementation roles, with a minority of 6% claiming no role in cyber security and critical infrastructure protection.

5.12 AWARENESS AND GLOBAL CULTURE OF CYBER SECURITY

Importance of Cyber Security

	Extremely Important	Very Important	Moderately Important	Slightly Important	Not Important at all
National Economy	82%	18%	-	-	-
National Security	88%	12%	-	-	-
Criticalinfrastructures*	71%	29%	-	-	-
Civil Society	59%	29%	12%	-	-
* critical infrastructures such as transportation, water and food supplies, public health, energy, finance, emergency services					

Table 1 Importance of Cyber Security in various sectors (Source, Author 2021)

The respondents rated the national security and the economy highest, with over 80% indicating that cyber security was extremely important, as seen in table 1 above. The critical infrastructures and civil society also got high ratings, with only 12% of the respondents of the opinion that cyber security in civil society was moderately important.

They further indicated that the critical information communications infrastructure and cybersecurity risks to the economy and security must be managed, including financial systems like MPESA and other systems, including the critical infrastructure that runs, controls, and conveys these systems. Hackers and people who wrongfully access personal and official information, or on the other hand, perpetrate Denial of Service (DoS) strikes are also a threat. This protection should be done through the development, deployment and sensitization of harmonized policies and laws with transnational reach.

The respondents observed that Denial-of-service (DoS) attacks, distributed denial-of-service (DDoS) attacks, ransomware, and other malware attacks could potentially cause loss of life, destruction of property and disruption of services and various other threats to national security, potentially leading to heavy financial losses. Cyberbullying and cyber terrorism were also mentioned as causing concern.

The respondents observed that it is vital to protect the stability and proper operation of infrastructures like the national power plant, rail network and aviation safety from security infringement, sabotage and malicious infiltration that can cause malfunction, denial of service and eventual compromise to national security. This was also a cause for concern since the country has adopted automated systems for service delivery, including the e-Citizen portal, National Transport and Safety Authority's Transport Information Management System (TIMS), Land Information Management System, Integrated Financial Management System (IFMIS) to mention but a few. Industrial SCADA controlled systems include power distribution, oil pipeline management, air traffic control. These are ICT controlled systems, and thus it is easy to compromise them remotely and severely impact the security and economy of the state.

In summary, the respondents indicated that the protection of sensitive financial data and the systems must be ensured for the National Economic growth and preservation. For National Security, protection of strategic country resources should be guaranteed against cyber terrorists. For the Civil Society, protection must be provided to guarantee civil liberties of activists and citizens, privacy and human rights.

Vulnerabilities of the networks in use and the relative levels of threat

The respondents indicated that the fibre optic network is vulnerable to physical and technical attacks and damage that could spread malware and hacking of critical information. The use of outdated and unpatched systems also provide loopholes for illegal entry into cyberspace.

Low skill levels and ignorance were cited as causes of network vulnerability to social engineering and political interference – inadequate protection, phishing, malware or ransomware attack, cyberbullying, identity theft, credit card cloning, cyber financial related frauds. ‘Grey devices’ (stolen, refurbished, counterfeit devices with pirated software) whose origin and integrity cannot be vouched for and increase the network vulnerabilities to international attacks and espionage.

Current Management Plan

The respondents indicated the presence of an outdated National Cybersecurity Strategy (2014). There is a cyber command to man systems, mitigate and disrupt threats, and comply with most ICT Industry requirements by training its ICT staff on new technologies to protect systems, hardware, and organization processes from threats. The Cyber security multi-agency unit based at the Communications Authority monitors cyber security incidences and responds appropriately. At the same time, the Ministry of ICT provides policy and legislation direction on cyber security.

Other plans are Asset Management, Security Control, Configuration Management, Incidence Response and Monitoring. A respondent indicated the need to improve the technology in use, continuous learning, in addition to reinforcement of infrastructures and systems.

The respondents indicated a need for extensive sensitisation on cyber threats as most cyber users err unknowingly. The implementation of Information Security Management Systems is paramount. The use of genuine hardware and software systems is encouraged and should be reinforced. Several respondents indicated that their entities manage their cyber security risks without collaboration domestically or internationally.

Goals of the National Cybersecurity and Critical Information Infrastructure Protection Strategy.

The respondents concurred that the goal was to protect cyberspace and enhance cyber access capacity, cyber security and protection, collaboration and information sharing while providing national leadership.

The strategy aims to ensure the availability of infrastructure that will facilitate secure electronic services provisioning, workforce and employee data security, capability to pragmatically deter, expose, scrutinize and counteract the danger from the cyber events directed against private and government systems. In addition, the development of cybersecurity skills and increased investor and public assurance in government providing safe digital services while protecting critical information and the associated infrastructure. This is to safeguard and protect the national interests against cyber hacks.

The strategy creates awareness of cyber threats and operationalises the current cyber defence strategies by first ensuring that all stakeholders assume responsibility for and take steps to reduce risk to harness information technology for national security and economic development.

The strategy should improve national infrastructures and services security and resilience, ensuring business continuity with minimal disruptions. In addition, the aim is to prevent loss of life and property and momentous shock on national defence and security and the working of the nation-state. The strategy does not appropriately coordinate the designing, approving, planning, deploying, and sustaining crucial infrastructure with powers to issue penalties to defaulters and offenders. In addition, the strategy is also supposed to create and maintain a critical infrastructure register with a database of all infrastructures that stakeholders can use as a reference point.

Level of Strategy Implementation

What is the current level of implementation of the strategy?

While 70% of the respondents agreed that the Cyber Security strategy was related to other national policies, a sizeable 30% were of a contrary opinion.

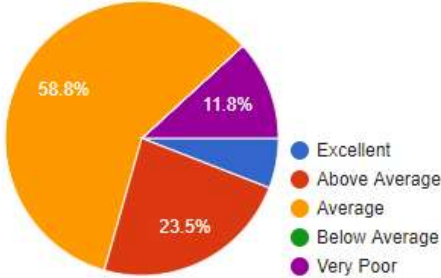
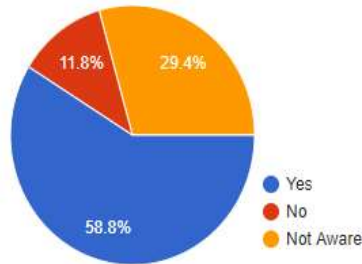


Figure 7 National Cyber Strategy Implementation (Source Author, 2021)

From figure 7 above, under 30% of the respondents thought that the implementation of the strategy was either “excellent” or “above average.” 60% of the respondents agreed that the strategy aligned with regional and international initiatives.

Are there plans to develop a national culture of cybersecurity?



Almost 60% of the respondents agreed that there are plans to develop a national cyber security culture, with a slightly higher percentage (65%) confirming the presence of national awareness-raising programs.

Figure 8 Alignment of National Cyber Strategy with Regional and International Initiatives (Source Author, 2021)

It is instructive to note that almost a quarter of the respondents were not aware of any awareness-raising programs, with a good 10% emphatically indicating the absence of such programs. A further two-thirds of the respondents were aware of the cyber security plan for government-operated systems, with a sizeable 30% unaware of such plans.

5.13 COLLABORATION AND COOPERATION

Almost half of the respondents acknowledged the existence of Public-Private cooperation, with a further 30% talking of planned initiatives. Slightly over 20% of the respondents were not aware of or denied any such cooperation, as indicated in figure 10.

Do we have collaboration between Government and the private sector as part of Public-Private cooperation?

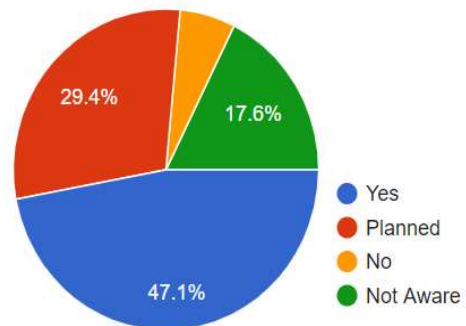


Figure 9 Public-Private Cooperation (Source, Author 2021)

If "yes or planned" above, select all the arrangements in place for collaboration:

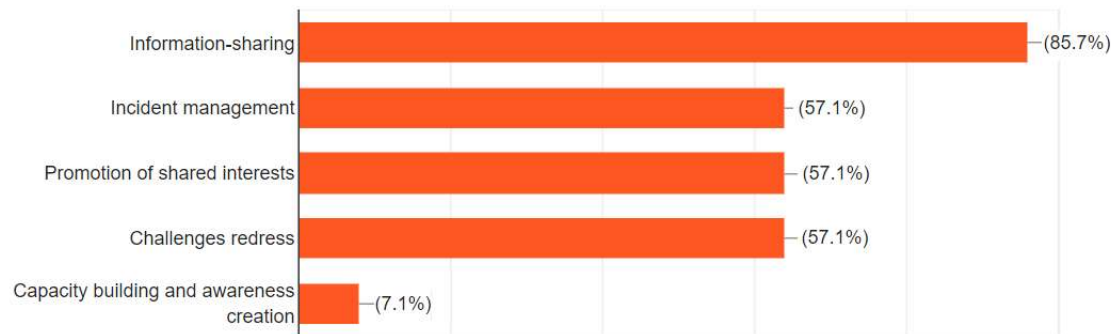


Figure 10 Collaboration Arrangements (Source Author, 2021)

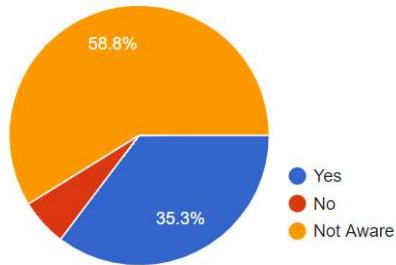
The primary collaboration and cooperative activities were in the sharing of information, according to the respondents. Incident management, promotion of shared interests and redress of challenges followed with equal importance while capacity building and awareness creation was a distant fifth as depicted in figure 11 above.

The respondents gave varying responses to the question regarding the coordinator for incident management. Only 20 respondents (less than 30%) were able to identify this critical role of the Communications Authority correctly. A good 20% of the respondents were ‘not aware.’ Three-quarters of the respondents indicated that the organisation they identified as the “coordinator for cyber incidents management” had the expertise for surveillance, forewarning, rejoinder and recovery roles. The other attributed the coordination to the Ministry of ICT, The ICT Authority, National Cyber Command Centre (NC3), Kenya Education Network (KENET), National Security Advisory Council (NSAC), National Intelligence Service (NIS), and even an unidentified organisation called ‘Information Security’.

International Cooperation

60% of the respondents indicated that there are arrangements for international cooperation and trusted information sharing. A significant third of the respondents are 'not aware' of such arrangements. In the same vein, close to 60% of the respondents were 'not aware' of

Are there networks and processes of International Cooperation that may enhance incident response and contingency planning?



international cooperation networks and processes that may enhance emergency planning and case response, with only 35% responding positively.

Figure 11 Network and Processes of

International Cooperation (Source, Author 2021)

The partners and arrangements for bilateral and multilateral cooperation were listed as International Telecommunications Union (ITU), African Union, EAC-Sub-regional level, East Africa Communications Organisations (EACO), Forum for Incident Response and Security Teams (FIRST), Commonwealth Telecommunication Organisation (CTO) and other National CIRT/CSIRTs, e.g. US-CERT and other private entities that manage cyber concerns.

5.14 LEGAL AND POLICY FRAMEWORKS

Over 70% of the respondents agreed that formal and informal avenues existed for government-industry collaboration in developing cyber security and critical infrastructure protection policy. Only slightly over a third were optimistic that the avenues were adequate in achieving the protection goals.

If yes, are the avenues adequate in achieving relevant cybersecurity and critical information infrastructure protection goals?

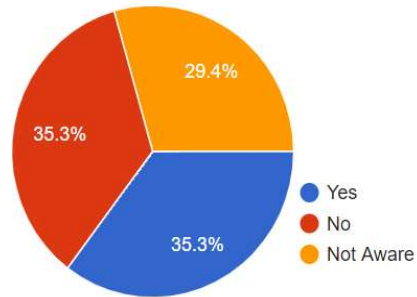


Figure 12 Government - Industry Collaboration for Policy Development (Source, Author 2021)

The respondents identified the other forums and structures helpful in integrating the government and non-government viewpoints and knowledge necessary to achieve national critical information infrastructure and cybersecurity protection goals, including the inclusion into the education syllabus and sensitisation from the very lowest level.

They indicated that cyber security should be understood as a personal responsibility since almost every household in Kenyan uses technology. Open forums for citizen inputs. Industry expert groups/task force for policy interrogation and delivery, partnership with civil society. Equipment manufacturers & ICT certification training institutions in addition to security assurance and research forums.

The respondents also noted a need to undertake extensive stakeholder mapping within the public sector and, after that, undertake activities geared towards acquiring the required buy-in from all the identified stakeholders for ownership purposes. Partnerships with business communities,

especially in the MSME sector, would help to disseminate the information to those who need it but do not know that they do.

On the relevance and currency of the legal framework as a result of the swift uptake of, and dependence on, new communications and information systems to direct the different areas, the respondents rated the data protection highest at 76% and digital signatures and commercial law trailed at 47% as depicted in table 2 below. Over a third of the respondents were not aware of the commercial law legal framework. Close to a third were negative on the existence of a legal framework in Cybercrime, Privacy and Encryption.

	Yes	No	Not Aware
Cybercrime	59%	29%	12%
Privacy	71%	29%	-
Data protection	76%	12%	12%
Commercial law	47%	18%	35%
Digital signatures	47%	24%	29%
Encryption	53%	29%	18%

Table 2 Sector Legal Framework (Source Author, 2021)

Generally, only 53% of the respondents were of the opinion that the country had developed mandatory legislation for the analysis and prosecution of cybercrime. This means almost half of the respondents were not aware or did not think highly of the legal frameworks for investigating and prosecuting cybercrime.

What is the level of understanding among prosecutors, judges and legislators of cybercrime issues?

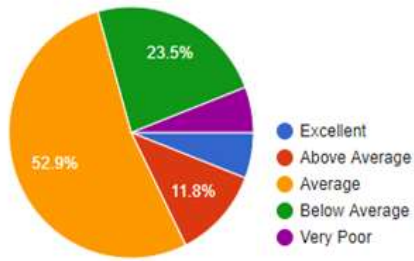


Figure 13 Level of Understanding of Cybercrime Issues (source, Author, 2021)

The majority of respondents rated the understanding among legislators, prosecutors and judges of cybercrime issues as ‘average’ (53%), with 23.5% rating their knowledge ‘below average’, only 11.8% and 5.9% rating ‘above average’ and ‘excellent’ respectively.

For sufficiency of legal codes and authorizations in addressing challenges of cyberspace, a significant portion of the respondents (41.2%) responded as ‘average’ with a further 29.4% responding as ‘below average’ and only 17.6% indicating that the codes above average’ as indicated in figure 14.

What is the adequacy of current legal codes and authorities in addressing the current and future challenges of cybercrime, and of cyberspace more generally?

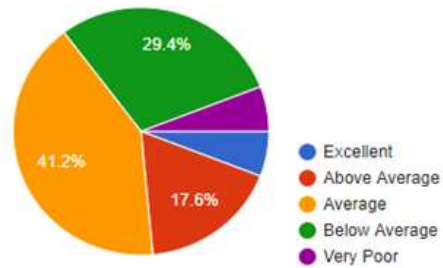


Figure 14 Adequacy of Legal Codes and Authorities in addressing challenges of cyber space (Source, Author 2021)

On international membership in efforts to fight cybercrime, such as around-the-clock cybercrime point of contact network, a good 47% were ‘not aware’ while 12% indicated non-existence of such initiatives. The rest responded in the affirmative. The 41% that was affirmative vaguely indicated that Kenya needed to be ‘Signatory to the International Statutes.’ International participation was mentioned through the Communications Authority as the regional and international point of Contact and as a member of the Forum for Incident Response and Security Teams (FIRST) and the G7 24/7 High Tech Crime Network. The country’s participation in ITU and AU cybersecurity initiatives was also given to represent avenues for international participation in combating cybercrime. On

cooperation with international counterparts by the law enforcement agencies, three-fifths of the respondents affirmed the existence of such arrangements. At the same time, almost one third were 'not aware', with the rest indicating a 'no' response.

For those respondents who were positive, the requirements in those occurrences in which infrastructure is situated, or offenders reside in the state territory, but victims live elsewhere were varied and widespread - monitoring data traffic across international gateways and regional and international collaboration, i.e. through Interpol, Mutual Legal Assistance (MLA) frameworks and other legal frameworks that are applicable in the circumstances.

Some indicated a general lack of international level agreement and consensus on addressing cyber security incidents with the *wiki leaks* saga given as an example.

Other Pertinent Comments

A respondent asked for the involvement of the private sector, civil society and general public in the cyber security policies and their implementation. To get implementation (of cyber security) going, awareness is the first port of call. A massive continuous awareness campaign targeting ordinary end-users is needed urgently since they unknowingly put themselves at risk. It was also noted that it is vital to facilitate the establishment of sector-specific CIRT/SCIRT to enhance the level of trust, data protection and incident response through collaborative frameworks that would enhance, amongst other things, information sharing and technical assistance in responding to cyber threats.

5.2 ANALYSES AND INTERPRETATION

In taking stock of cybersecurity needs and strategies, information and communications technologies are increasingly critical in national security and economy, critical infrastructures (such as water and food supplies, transportation, finance, public health, energy, emergency services) and civil outfits.

The study reveals severe cybersecurity and critical information infrastructure protection hazards to the national security, economy, critical infrastructures and civil society that must be governed, with vulnerabilities and high threat levels each sector faces. Considering the economic setting and national security priorities, the management plans were unclear and not well-coordinated. At the same time, there are attempts at national cybersecurity and critical information infrastructure protection, the current level of execution and measures to appraise its progress compared to other national policy intentions. The strategic fit within international and regional schemes are not very clear and thus need to be streamlined.

In the development of a global culture of cybersecurity, steps have been taken, and blueprints are in place to develop a national culture of cybersecurity, including implementation of cybersecurity schemes for Government managed systems, national awareness nurturing campaigns with outreach sessions and programmes, to among others, children (Child safety online project) and individual users, and national cybersecurity and critical information infrastructure protection training requirements. Regular internet users have no access to simple training to avoid threats online and limited awareness-raising cybersecurity campaigns.

Stakeholder functions and responsibilities are not well defined. The key stakeholders with a share in cybersecurity and critical information infrastructure protection have overlapping roles in the advancement of relevant operations and policies, including National Government ministries or agencies that lack vital points of contact and responsibilities; The Ministry of ICT, the Ministry of Interior, The Ministry of Defence and the agencies including the CA, The NC3, The ICT Authority, the Police, The Judiciary and the Central Bank all have overlapping and non-defined roles in the management of the cyberspace. The role of civil society and academia is also not well defined.

Public-private cooperation activities and plans to advance collaboration between the private sector and the government, including information-sharing and incident management measures, are in place. However, there is suspicion between the two and thus possible that the information sharing is incomplete. There are planned programs to promote shared interests and address common challenges among critical infrastructure owners, users, and private-sector actors reciprocally dependent on the interconnected critical infrastructure. The government operatives appear wary of exposing themselves to the private sector operatives. It is instructive to note that the Government is yet to pass the Critical Infrastructure bill, which was mooted in 2016. While there is a Critical Infrastructure Protection Unit (CIPU) within the National Police Service, its role is limited to guard duties for physical infrastructure, often at strategic points. Kenya has been accused of interfering with the neighbouring country's critical infrastructure in the fight against terror, interfering with the local economy and livelihoods.

The CA that serves as the incident management controller also undertakes surveillance, warning, response and recovery functions; with defined cooperating Government agencies; non-governmental cooperating participants, including industry and other partners. There are provisions

in place for collaboration and reliable information-sharing. The CA indicated that the country has national-level computer incident response capacity, including a response team for computer incidents with national commitments, existing devices and methods for the defence of Government computer systems, and existing tools and procedures for disseminating incident-management information. The details and evidence were not available to the researcher due to security concerns.

The networks and processes of international cooperation that may enhance incident response and contingency planning are not well defined, with partners and arrangements for bilateral and multilateral cooperation appear to be lacking and ill-developed.

CHAPTER SIX - CONCLUSION AND RECOMMENDATIONS

Chapter Six consists of a summary of findings, discussions, conclusions, and recommendations of the study. Also included are be suggestions for further research and contribution to the body of knowledge.

6.1 SUMMARY OF FINDINGS

This study has found out that there is an increasingly critical role of information and communications technologies in the Kenyan national security, economy, critical infrastructures (such as finance, transportation, energy, water and food supplies, public health, emergency services) and civil society, more so in the post -COVID 19 age. It also confirms that the Cyber Norms, if followed, would result in a more stable and safer Cyberspace, thus enhancing international security. There is a need to move from Norms to an actual convention anchored on International Law to address Cyberspace matters. While ICT use has grown exponentially, the attendant cyber security measures have not followed suit. We have gaps in the legal and policy space, inadequate awareness and capacity, overlapping institutions and poor supply chain integrity.

6.2 DISCUSSIONS

Management plans for critical information infrastructure and cybersecurity security risks to the national security, economy, critical infrastructures, and civil society must be governed and well-coordinated, considering the changes in the economic environment and national security priorities.

The government agencies in charge of cyberspace should prioritise the development of a national culture of cybersecurity, including the execution of a cybersecurity blueprint for Government-

operated systems, state awareness-raising programmes, outreach programmes to, among others, children and individual users, and national cybersecurity and training requirements for critical information infrastructure protection.

Public-private cooperation should be backed by clear actions and plans with clearly defined stakeholder roles and responsibilities, with overlapping roles clarified.

As the government agency that serves as the controller for incident management, including the competence in surveillance, warning, response and recovery functions, CA should cooperate and collaborate with other government agencies; non-governmental cooperating participants, including industry, academia and other partners. It was clear that several of the private sector agencies did not know what CA does.

The networks and processes of international cooperation that may enhance incident response and contingency planning should be well defined, with partners and arrangements for bilateral and multilateral cooperation.

6.3 CONCLUSION AND RECOMMENDATIONS

In conclusion, the critical challenge in governance at the local political level is how to surmount division of authority and accountability as far as the use of ICTs is concerned. Governments increasingly share the space and responsibility with other governments and non-state actors, both with positive and negative intent. The norms applied wisely can assist Kenya in regulating the ICT space and positively influencing the country's economic, political, and military power at the international level. The adherence to the international norms while considering a coherent overall policy framework will involve challenging negotiation between security and privacy with the

resultant horizontal and vertical synchronization and cooperation issues across government and at the crossroads between society, economy and state.

There is a need to develop critical cyber infrastructure identification and protection criteria to guide the private and public sectors. Kenya has been cited for interfering with a neighbouring country's critical ICT infrastructure, thus requiring clear policy guidelines. The GoK should urgently conclude enacting the critical infrastructure protection law and its attendant regulations requiring GoK ministries and private sector companies to identify their critical cyberinfrastructures and report their inventory to GoK.

Reporting and follow up of any cyber breaches should be formalized and acted upon promptly to ensure the safety of assets and data in the country. All organisations, especially government agencies, should plug security gaps in their systems to take care of vulnerabilities.

The Communications and Anti-Counterfeit Authorities should enhance the regime around type approval and monitoring of 'grey' equipment to manage the emergence of malware and intentional bugs. At the same time, capacity building, especially for public and private sector officials handling cyber security, has to be prioritised and funded. Most of the ICT and Computer Science studies are generalist in nature.

Formal Regional and International cooperation and mutual legal assistance agreements in cyber security should be put in place as a matter of urgency. Further research needs to be undertaken in international law to deal with cyber security. This is a relatively new area growing exponentially and affects state and non-state actors, including public and private enterprises.

In terms of academic gain – there is a need to develop a theoretical framework to address the Cyberspace phenomenon, specifically cyber relations. Working together with the Private sector and Government Agencies, the Academia should guide on capacity building for cyber professionals, both initial and continuous professional learning. This calls for close Government - industry collaboration.

For Policymakers in the ICT and security docket, identification, classification and protection of critical information infrastructure is paramount. The Critical Infrastructure bill needs to be passed as a matter of urgency. There is also a thin line between self-defence and interference with hostile nations' critical infrastructure, as seen in the Kenya-Somalia tiff.

The government needs to make additional investments in cyber deterrence and the certification of ICT equipment.

In the Legal space, expansion of the legal and policy framework, bilateral and multilateral cooperation as far as cyber relations are concerned (mutual legal assistance) should be prioritised. Kenya should use its tenure at the UN Security Council to push for internationally binding Cyber Laws to ensure safer and stable cyberspace for all.

The policymakers from the Ministry of Education and ICT also need to sustain national awareness campaigns on cyber hygiene, working closely with the non-state actors who own most of the ICT end-user equipment and internet access systems.

BIBLIOGRAPHY/REFERENCE

- Acharya, Mahesh, and Neema Oriko. "Kenya's Computer Misuse and Cybercrimes Act, 2018: Suspended Provisions Now Effective," February 21, 2020. <https://www.lexology.com/library/detail.aspx?g=ed5937e1-b7e3-42bb-baa9-2cef53cced5a>.
- Africa Union Commission. "Africa Union Convention on Cyber Security and Personal Data Protection," 2014. https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf.
- Anna-Maria Osula and Henry Rõigas (Eds.). *International Cyber Norms: Legal, Policy & Industry Perspectives*, Tallinn: NATO CCD COE Publications, 2016.
- APC. "Uganda 2021 General Elections: The Internet Shutdown and Its Ripple Effects." *Association for Progressive Communications*, 2020. <https://www.apc.org/en/news/uganda-2021-general-elections-internet-shutdown-and-its-ripple-effects>.
- Asuelaa, Obar Mark. "We Have Taken Control of Kenyan Government's Websites, Declares Hackers." *The Standard*, June 3, 2019. <https://www.standardmedia.co.ke/counties/article/2001328320/ifmis-and-other-government-websites-under-cyberattack>.
- Baezner, M. *Hotspot Analysis: Synthesis 2017: Cyber-Conflicts in Perspective*. Zurich: Center for Security Studies (CSS), ETH Zurich., 2018.
- Bequia, A. "Computer Crime: A Growing and Serious Problem." *Police Law Quarterly* Vol. 6 (1977): pg. 22.
- Buchanan, B. *The Cybersecurity Dilemma: Hacking, Trust, and Fear between Nations*. Oxford: Oxford University Press., 2016.
- "CA Annual Report FY 2019-2020." Accessed May 17, 2021. <https://ca.go.ke/wp-content/uploads/2021/05/Annual-Report-for-Financial-Year-2019-2020.pdf>.
- Capri, Alex. "US-China Techno-Nationalism and the Decoupling of Innovation." *The Diplomat*, September 10, 2020. <https://thediplomat.com/2020/09/us-china-techno-nationalism-and-the-decoupling-of-innovation/>.
- China, the Russian Federation, Tajikistan and Uzbekistan. "International Code Of Conduct For Information Security." UN Office of Disarmament Affairs, 2011. <https://www.un.org/disarmament/publications/library/66-ga-ga-sc/>.
- Choto, Kingori. "Secure Critical Infrastructure For Sustainable Development." *Capital FM News* (blog), July 28, 2020. <https://www.capitalfm.co.ke/news/2020/07/secure-critical-infrastructure-for-sustainable-development/>.
- Clarke, R. "War from Cyberspace." *National Interest*, December 22, 2009. <https://nationalinterest.org/article/war-from-cyberspace-3278>.
- Communications Authority of Kenya. "National Ke-CIRT/CC Cybersecurity Report For The Period January To March 2021." Nairobi, 2021. https://ke-cirt.go.ke/wp-content/uploads/2021/04/Quarter-3-FY-2020_21-National-KE-CIRT_CC-Report_compressed-3.pdf.
- Communications Authority of Kenya. "Type Approval Procedure." *Communications Authority of Kenya* (blog). Accessed May 17, 2021. <https://ca.go.ke/industry/type-approval/type-approval-procedure/>.
- "Convention on Cybercrime." *European Treaty Series - No. 185*, 2001. https://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf.
- Cooper, D., & Schindler, P. *Business Research Methods*. 10th ed. New York: McGraw-Hill/Irwin, 2008.
- Coyne, Christopher J., and Peter T. Leeson. "National Security Threats in Cyberspace." *American Bar Association*, 2009, pp 475-76.
- Deibert, R. *Black Code. Surveillance, Privacy, and the Dark Side of the Internet*. Toronto: McClelland & Stewart., 2013.

- Deudney, D., Ikenberry, J.G. “The Nature and Sources of Liberal International Order,” *Review of International Studies* Volume 25, no. Issue 2 (April 1999): 179–96.
- Dewar, R. S. (Ed.). *National Cyber Security and Cyber Defence Policy Snapshots*. Zurich: Centre for Cyber Security Studies, 2018.
- Dunn Cavelt, M. *The Normalization of Cyber-International Relations*. In O. Thränert, & M. Zapfe (Eds.), *Strategic Trends 2015: Key Developments in Global Affairs*. Zurich: Center for Security Studies., 2015.
- Egloff, F. J., Wenger, A. “Public Attribution of Cyber Incidents. In F. Merz (Ed.), *CSS Analyses in Security Policy*,” 244:1–4. Zurich: Center for Security Studies, 2019.
- “Eight UN Congress on the Prevention of Crime and Treatment of Offenders - UN General Assembly Resolution A/RES/45/121.” UN, December 14, 1990. <https://undocs.org/pdf?symbol=en/A/RES/45/121>.
- Eric Talbot Jensen. “The Tallinn Manual 2.0: Highlights and Insights.” *48 Georgetown Journal of International Law*, BYU Law Research Paper, 735, no. No. 17-10 (2017): 44.
- Eriksson, J. and Giacomello, G. (eds). *International Relations and Security in the Digital Age*. Advances in International Relations and Global Politics. New York: Routledge, 2007.
- EU. “Regulation (EU) 2016/679 of The European Parliament and the Council.” Official Journal of the European Union, April 27, 2016. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679>.
- Feledy, B. “Challenges of Theoretical Approaches to Cyber Security Theorizing Security in the Eastern European Neighbourhood: Issues and Approaches.” *Academia.Edu*, 2018, 147–63.
- Finnemore M, Sikkink K. “International Norm Dynamics and Political Change.” *International Organization* 52 (1998): 887–917.
- Fischerkeller, M. *Offense-Defense Theory, Cyberspace, and the Irrelevance of Advantage*. Alexandria, VA: Institute for Defense Analysis, 2018.
- Frear, Thomas, Lukasz Kulesa, and Denitsa Raynova. “Russia and NATO: How to Overcome Deterrence Instability?” European Leadership Network, 2018. <http://www.jstor.org/stable/resrep22119>.
- Gable, Kelly A. “Cyber-Apocalypse Now: Securing the Internet against Cyberterrorism and Using Universal Jurisdiction as a Deterrent.” 2010. <https://www.thefreelibrary.com/Cyber-apocalypse+now%3a+securing+the+Internet+against+cyberterrorism...-a0219374102>.
- Georgieva, I. “The Unexpected Norm-Setters: Intelligence Agencies in Cyberspace.” *Contemporary Security Policy* 41 (2020): pp 33-54. <https://doi.org/doi:10.1080/13523260.2019.1677389>.
- Global Commission on the Stability of Cyberspace. “Advancing Cyberstability Final Report.” The Hague Centre for Strategic Studies and EastWest Institute, November 2019. <https://cyberstability.org/report/>.
- Global Digital Partners. “Global Digital Partners Work,” May 2021. <https://www.gp-digital.org/our-work/>.
- GoK. “The Critical Infrastructure Protection Bill, 2019.” GoK, 2019.
- Gordon, Sarah, and Richard Ford. “On the Definition and Classification of Cybercrime.” *Journal in Computer Virology* 2, no. 1 (August 1, 2006): 13–20. <https://doi.org/10.1007/s11416-006-0015-z>.
- Hathaway, Melissa. “Getting beyond Norms: When Violating the Agreement Becomes Customary Practice.” Centre for International Governance Innovation, April 2017. <https://www.cigionline.org/sites/default/files/documents/Paper%20no.127.pdf>.
- Hill, Richard. “Promoting Stakeholder Action Against Botnets and Other Automated Threats.” Association for Proper Internet Governance, January 2018. https://www.ntia.doc.gov/files/ntia/publications/association_for_proper_internet_governance.pdf.
- Hitchens, Theresa, and Nancy W. Gallagher. “Building Confidence in the Cybersphere: A Path to Multilateral Progress.” *Journal of Cyber Policy* 4, no. issue 1 (April 9, 2019): Pp 4-21. <https://doi.org/10.1080/23738871.2019.1599032>.

- Hofmann, J. “Multi-Stakeholderism in Internet Governance: Putting a Fiction into Practice.” *Journal of Cyber Policy* 1 (2016): 29-49. <https://doi.org/doi:10.1080/23738871.2016.1158303>.
- ICT4Peace Foundation. “The Government of Kenya and ICT4Peace Foundation Co-Organize the First Regional Training Workshop in Africa on International Security and Diplomacy in Cyberspace.” *ICT4Peace Foundation* (blog), March 4, 2015. <https://ict4peace.org/activities/the-government-of-kenya-and-ict4peace-foundation-co-organize-the-first-regional-training-workshop-in-africa-on-international-security-and-diplomacy-in-cyberspace/>.
- ICTA. “National Optic Fibre Backbone (NOFBI) – ICT Authority,” 2020. <http://icta.go.ke/national-optic-fibre-backbone-nofbi/>.
- “International Cybersecurity Norms - Microsoft Policy Papers.” Microsoft Corporation, 2020. <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVmcd>.
- “International Telecommunication Union, Final Acts of the World Administrative Telegraph and Telephone Conference Melbourne, 1988 (WATTC-88): International Telecommunications Regulations.” International Telecommunication Union, Geneva, 1989. <https://ccdcoe.org/sites/default/files/documents/ITU-881209-ITRFinalActs.pdf>.
- Issaias, Ariana. “Data Protection Update: Recruitment of a Data Commissioner Begins,” April 1, 2020. <https://www.bowmanslaw.com/insights/intellectual-property/data-protection-update-recruitment-of-a-data-commissioner-begins/>.
- Jason Healey et al. “Confidence-Building Measures in Cyberspace: A Multistakeholder Approach for Stability and Security.” *Atlantic Council*. 2014. www.atlanticcouncil.org/images/publications/Confidence-Building_Measures_in_Cyberspace.pdf.
- Jensen, L (ed). “The Sustainable Development Goals Report 2020.” UN Department of Economic and Social Affairs, 2020. <https://unstats.un.org/sdgs/report/2020/The-Sustainable-Development-Goals-Report-2020.pdf>.
- Katzenstein, P. J. ed. *Introduction: Alternatives Perspective on National Security, in The Culture of National Security: Norms and Identity in World Politics*. New York: Columbia University Press, 1996.
- Kello, L. *Cyber Security: Gridlock and Innovation*, in: Hale T. and Held, D. (Eds.), *Beyond Gridlock*. UK: Polity Press, 2017.
- . *The Virtual Weapon and International Order*. New Haven, CT: Yale University Press, 2017.
- “Kenya Cyber Security Report 2015.” Accessed May 17, 2021. <https://www.serianu.com/downloads/KenyaCyberSecurityReport2015.pdf>.
- Kenya ICT Action Network. “Cybersecurity in Kenya: Strategizing for the Future.” kictanet, March 12, 2020. <https://www.kictanet.or.ke/wp-content/uploads/2020/03/Cybersecurity-in-Kenya-Strategizing-for-the-Future-Concept-Note-and-Programme.pdf>.
- Klimburg, Alexander, and Hugo Zylberberg. “Cyber Security Capacity Building: Developing Access.” Norwegian Institute of International Affairs, 2015.
- Korir, Cheruiyot. “Kenya to Collaborate with US in Cyber Security.” *Ministry of ICT, Innovation and Youth Affairs* (blog), June 22, 2017. <https://ict.go.ke/kenya-to-collaborate-with-us-in-cyber-security/>.
- Kothari, C.R. () *Research Methodology: Methods and Techniques*. New Age International, 2009.
- Krasner, S. “Structural Causes and Regime Consequences: Regimes as Intervening Variables.” *International Organization* 2, no. Issue 36 (Spring 1982): 185-205.
- Kremer, J., and B. (Eds.) Müller. *Cyberspace and International Relations: Theory, Prospects and Challenges* -, 2014. Editors: www.springer.com.
- Kshetri, Nir. “Cybercrime and Cybersecurity in Africa.” *Journal of Global Information Technology Management*, vol 22, no. issue 2 (2019): pp 77-81. <https://doi.org/DOI:10.1080/1097198X.2019.1603527>.

- Maarten Van Horenbeeck, Ed. “Cybersecurity Culture, Norms and Values: Background Paper to the IGF Best Practices Forum on Cybersecurity.” *Internet Governance Forum Best Practices Forum on Cybersecurity* (2018).
- Mackay, A. Neutze, J. “International Cybersecurity Norms : Reducing Conflict in an Internet-Dependent World.” Microsoft Corporation, 2015.
https://cybersummit.info/sites/cybersummit.info/files/International_Cybersecurity_%20Norms.pdf.
- Manduku, Stanley K. “Securing Kenya: Overview and Implications of the Critical Infrastructure Protection Bill.” Mombasa, Kenya, 2016. <http://isaca.or.ke/downloads/Overview-and-Implications-of-the-Critical-Infrastructure-Protection-Bill-Stanley-manduku.pdf>.
- Matthews, B. and Ross, L. *Research Methods*. London: Pearson Longman, 2010.
- Maurer, T. *Cyber Mercenaries: The State, Hackers and Power*. Cambridge: Cambridge University Press, 2017.
- Mazanec, B. M. *Cyber War: International Norms for Emerging-Technology Weapons*. Nebraska: Potomac Books, 2015.
- Menya, Walter. “Somalia Based Telecom Company Financing Terror Group to Destroy Communication Masts in Kenya to Increase Its Market Share.” *Daily Nation (Kenya)*, September 9, 2019.
<https://www.business-humanrights.org/en/latest-news/somalia-based-telecom-company-allegedly-financing-terror-group-to-destroy-communication-masts-in-kenya-to-increase-its-market-share/>.
- Michael N. Schmitt, ed. *Tallinn Manual 2.0 on The International Law Applicable to Cyber Operations*. New York: Cambridge University Press, 2017.
- . *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press, 2013. <https://ccdcoe.org/research.html>.
- Millward, David. “Biden Declares Emergency after Hackers Shut down Major US Pipeline,” May 9, 2021. <https://news.yahoo.com/biden-administration-step-cybersecurity-hackers-151107172.html>.
- Ministry of Information Communications and Technology. “National Cybersecurity Strategy.” GoK, 2014. <https://icta.go.ke/pdf/NATIONAL%20CYBERSECURITY%20STRATEGY.pdf>.
- Muendo, Mercy. “What’s Been Done to Fight Cybercrime in East Africa.” *The Conversation*, December 2, 2019. <https://theconversation.com/whats-been-done-to-fight-cybercrime-in-east-africa-127240>.
- Mugenda, O. and Mugenda, A. *Research Methods: Quantitative And Qualitative Approaches*. Nairobi: ACTS Press, 1999.
- Mugendi, Jacob. “Al-Shabaab’s Impact on Communications in Kenya.” iAfrikan.com, February 8, 2021. <https://iafrikan.com/2021/02/08/terrorism-a-threat-to-communication-in-northern-kenya/>.
- Munyori, Melanie, and Judy Mumbi. “The Rise in Cyber Crimes in Kenya: How Effective Are Our Laws?” *Wamae and Allen Legal Update* (blog), January 15, 2020. <https://wamaeallen.com/the-rise-in-cyber-crimes-in-kenya-how-effective-are-our-laws/>.
- Myriam Dunn Cavelt, Andreas Wenger. “Cyber Security Meets Security Politics: Complex Technology, Fragmented Politics, and Networked Science, Contemporary Security Policy” vol 41, no. 1 (2020): 5-32, <https://doi.org/DOI: 10.1080/13523260.2019.1678855>.
- Ndung’u, Njuguna, and Landry Signé. “The Fourth Industrial Revolution and Digitization Will Transform Africa into a Global Powerhouse.” *Foresight Africa 2020*. Washington DC: The Brookings Institution, January 8, 2020. <https://www.brookings.edu/research/the-fourth-industrial-revolution-and-digitization-will-transform-africa-into-a-global-powerhouse/>.
- NPS. “Inspector General Visits Administration Police Service Units,” July 19, 2019. <https://www.nationalpolice.go.ke/2015-09-08-17-56-33/news/294-inspector-general-visits-to-aps-units.html>.
- Nye, Jr., Joseph S. “Cyber Power.” Belfer Center for Science and International Affairs Harvard Kennedy School, 2010. <https://www.belfercenter.org/sites/default/files/legacy/files/cyber-power.pdf>.

- Odula, Tom. "UN Links Kenyan Military to Attacks on Somalia's Top Telecom." AP NEWS, November 15, 2019. <https://apnews.com/article/266181bb47cb42bf9af392562c7c8c1f>.
- Office of the Press Secretary. "Remarks by The President on Securing Our Nation's Cyber Infrastructure." White House, Washington DC, May 29, 2009. <https://obamawhitehouse.archives.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure>.
- Ogula, P. A. *Research Methods*. Nairobi: CUEA Publications, 2005.
- Picker, Randal C. "Cyber Security: Of Heterogeneity and Autarky" (John M. Olin Program in Law and Economics Working Paper No. 223, 2004), n.d.
- Polit, F. D., Polit-O'Hara, D., P. Hungler, B.P. *Essentials of Nursing Research: Methods, Appraisal, and Utilization*. 4th Ed. University of Michigan: Lippincott-Raven, 1997.
- R. T. Slivka; J. W. Darrow. "Methods and Problems in Computer Security." *Rutgers Journal of Computers and the Law* 5, no. 2 (1976): 217–70.
- Rai, Akhand Pratap, and Aman Mani Tripathi. "U.S. Sanction against Iran: Breach of International Obligation." *Modern Diplomacy*, June 2020. <https://modern diplomacy.eu/2020/06/23/u-s-sanction-against-iran-breach-of-international-obligation/>.
- Rattray, G. *Strategic Warfare in Cyberspace*. Cambridge, MA: The MIT Press., 2001.
- "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security - A/70/174." UN, July 22, 2015. https://www.un.org/ga/search/view_doc.asp?symbol=A/70/174.
- "Resolution Adopted by the General Assembly on 5 December 2018 - Seventy-Third Session Agenda Item 96." United Nations, 2018. <https://undocs.org/pdf?symbol=en/A/RES/73/27>.
- Reuter, Christian. *Information Technology for Peace and Security: IT Applications and Infrastructures in Conflicts, Crises, War, and Peace*. Wiesbaden: Springer Vieweg, 2019.
- Rid, T., Buchanan, B. "Attributing Cyber Attacks." *Journal of Strategic Studies* 38 (2015): 4–37. <https://doi.org/doi:10.1080/01402390.2014.977382>.
- Sales, Nathan Alexander. "Regulating Cyber Security." *Northwestern University Law Review* Vol. 107, no. 4 (2013): pp 1503-1568.
- Schjølberg, S., Tingrett, M. "A Presentation at the Octopus Interface 2004." Strasbourg, France.: Council of Europe, 2004. <https://www.cybercrimelaw.net/documents/Strasbourg.pdf>.
- Schwartz, W. *Chaos on the Electronic Superhighway: Information Warfare*. Second Edition. New York, NY: Thunder's Mouth Press, 1996.
- "Shanghai Cooperation Organization, Agreement between the Governments of the Member States of the Shanghai Cooperation Organisation on Cooperation in the Field of International Information Security." Shanghai Cooperation Organization Secretariat., June 16, 2009. <http://eng.sectsco.org/documents/20090616/207486.html>.
- Shires, J. "Cyber-Noir: Cybersecurity and Popular Culture." *Contemporary Security Policy* 41 (2020): pp 82-107. <https://doi.org/doi:10.1080/13523260.2019.1670006>.
- Simon, M., Slay, J. "Voice Over IP: Forensic Computing Implications." Edith Cowan University, Perth Western Australia, 2006. <https://doi.org/10.4225/75/57b13904c7058>.
- Stevens, M. L. "Identifying and Charging Computer Crimes in the Military," *Military Law Review* Vol. 110 (1985): pg. 59.
- Tikk, Eneken, and Mika Kerttunen. *Routledge Handbook of International Cybersecurity - The Role of the UN Security Council in Cyber Security*. London: Routledge, 2020. https://tandfbis.s3-us-west-2.amazonaws.com/rt-files/docs/Open+Access+Chapters/9781351038904_oachapter30.pdf.
- UN. "A/69/723 -Developments in the Field of Information and Telecommunications in the Context of International Security - Sixty-Ninth Session Agenda Item 91." UN Office of Disarmament Affairs, 2015. <https://undocs.org/a/69/723>.
- . "Efforts to Implement Norms of Responsible State Behaviour in Cyberspace, as Agreed in UN Group of Government Expert Reports of 2010, 2013 and 2015." UN Disarmament, 2019.

- <https://www.un.org/disarmament/wp-content/uploads/2019/12/efforts-implement-norms-uk-stakeholders-12419.pdf>.
- . “UN GGE Report 2013 (A/68/98*).” GIP Digital Watch, 2013. <https://dig.watch/un-gge-report-2013-a6898>.
- . “UN Resolution Adopted by the General Assembly [on the Report of the Third Committee (A/55/593)] 55/63. Combating the Criminal Misuse of Information Technologies.” UN Office of Disarmament Affairs, 2001. https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf.
- UN Economic Commission for Africa. “Tackling the Challenges of Cybersecurity in Africa. Policy Brief. No. 002, 6 p.” UNECA, 2014. <https://repository.uneca.org/handle/10855/22544>.
- UN General Assembly. “Resolution 70/237 - Developments in the Field of Information and Telecommunications in the Context of International Security,” December 30, 2015. <https://undocs.org/a/res/70/237>.
- UN Office for Disarmament Affairs. “Group of Governmental Experts.” Accessed November 30, 2020. <https://www.un.org/disarmament/group-of-governmental-experts/>.
- United Nations. “Creation of a Global Culture of Cybersecurity and Taking Stock of National Efforts to Protect Critical Information Infrastructures.” United Nations, December 21, 2009. <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N09/474/49/PDF/N0947449.pdf?OpenElement>.
- “United Nations, General Assembly, Group of Governmental Experts, A/68/98.,” n.d.
- “United Nations, General Assembly, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/68/98 (24 June 2013), http://www.un.org/Ga/Search/View_doc.asp?Symbol=A/68/98. http://www.un.org/Ga/Search/View_doc.asp?Symbol=A/68/98.,” n.d.
- “USA and 26 Countries Issue Joint Statement on Responsible Behaviour in Cyberspace 23.” Digital Watch-Geneva Internet Platform, September 2019. <https://dig.watch/updates/usa-and-26-countries-issue-joint-statement-responsible-behaviour-cyberspace>.
- “Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology: A Commentary.” United Nations, 2017. <http://www.un.org/disarmament>.
- Waag-Cowling, Noëlle van der, Brett van Niekerk, and Dr Trishana Ramluckan. “Submission to the Call for Inputs: Report on the Provision of Military and Security Cyber Products and Services by ‘Cyber Mercenaries’ and Its Human Rights Impact.” Office of the United Nations High Commissioner for Human Rights, n.d. <https://www.ohchr.org/Documents/Issues/Mercenaries/WG/CyberMercenaries/Academia-van-der-Waag-Cowling.docx>.
- Wainainah, Doreen. “Kenya Reports Highest Cyber Attacks in Africa.” Business Daily, September 24, 2020. <https://www.businessdailyafrica.com/bd/corporate/technology/kenya-reports-highest-cyber-attacks-in-africa-2370444>.
- Waxman, Matthew C. “Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4).” *Yale Journal of International Law* Vol 36, no. No. 2 (2011). <https://digitalcommons.law.yale.edu/yjil/vol36/iss2/5>.
- Weber, V. “Linking Cyber Strategy with Grand Strategy: The Case of the United States.” *Journal of Cyber Policy* Vol. 3 (2018): pp 236-257. <https://doi.org/doi:10.1080/23738871.2018.1511741>.
- Welchman, Keen. “Safeguarding Critical Information Infrastructure: Risk and Opportunities.” World Economic Forum, 2020. <https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/Documents/Events/2020/RDF2020/Post%20Forum%20Day%203/CII-Whitepaper-WK.pdf>.

- Wenger, Andreas, Jan Metzger, and Myriam Dunn Cavelty. "An Inventory of Protection Policies in Eight Countries. Critical Information Infrastructure Protection." *Center for Security Studies (CSS), ETH Zürich*, International CIIP Handbook, 2002. <https://doi.org/10.3929/ethz-b-000325400>.
- Wilson, C. "Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress." Congressional Research Service, January 29, 2008. <https://fas.org/sgp/crs/terror/RL32114.pdf>.
- Ziolkowski, Dr Katharina. "Confidence Building Measures for Cyberspace – Legal Implications." NATO Cooperative Cyber Defence Centre of Excellence, 2013. www.ccdcoe.org.

APPENDICES

APPENDIX 1: QUESTIONNAIRE

IMPLEMENTATION OF UN CYBER NORMS IN THE PROMOTION OF INTERNATIONAL SECURITY: A CASE STUDY OF KENYA.

Dear Respondent

This letter is to request the provision of information to complete my MA study titled **“IMPLEMENTATION OF UN CYBER NORMS IN THE PROMOTION OF INTERNATIONAL SECURITY: A CASE STUDY OF KENYA”**.

The study intends to establish the implementation of the UN Group of Governmental normative framework on the use of ICTs in Kenya to bolster national and international security. It further seeks to examine the level of awareness, collaboration and policy framework in place as far as cyber security is concerned.

I have identified you as a critical player in the Kenyan cyberspace and thus a potential source of relevant information. All responses will be acknowledged, credited and strictly used only for academic purposes. The information obtained will be treated in confidence.

Your cooperation is highly appreciated.

Thank you.

TIMOTHY WERE

MA STUDENT

UNIVERSITY OF NAIROBI /NATIONAL DEFENCE COLLEGE, KENYA

A. GENERAL INFORMATION

Please mark with an (x) or (tick) in the box with the appropriate response. Mark one box only.

- 1. Gender: Male () Female()
- 2. Age bracket: 18 – 24 () 25 – 35 () 36 – 45 () 46 -55 () 56 and above ()
- 3. Highest level of education attained: Diploma () Bachelors () Masters () PhD ()
 Others (specify)
- 4. Occupation/Employment/Sector.....
- 5. Designation.....

B. AWARENESS AND GLOBAL CULTURE OF CYBER SECURITY

Taking stock of cybersecurity needs and strategies

1. What is the role of ICT in the following areas? *(Please mark the appropriate box).*

		Extremely Important	Very Important	Moderately Important	Slightly Important	Not at all Important
a	National Economy					
b	National Security					
c	Critical infrastructures*					
d	Civil Society					

** critical infrastructures such as transportation, water and food supplies, public health, energy, finance, emergency services*

2. What cybersecurity and critical information infrastructure protection risks to the economy, national security, critical infrastructures, and civil society must be managed?

3. Vulnerabilities and the levels of threat

a. What are the vulnerabilities of the networks in use and the relative levels of threat faced by your sector?

b. What is the current management plan?

4. Determine the goals of the national cybersecurity and critical information infrastructure protection strategy;

a. What are the goals of the national cybersecurity and critical information infrastructure protection strategy?

b. What is the current level of implementation of the strategy? (*select one*)

Excellent Above Average Average Below Average Very Poor

c. Is the strategy related to other national policy objectives? Yes () No ()

d. Does the strategy within regional and international initiatives? Yes () No ()

4. Developing a global culture of cybersecurity

a. Are there plans to develop a national culture of cybersecurity? Yes () No ()

b. Is there a cybersecurity plan for Government-operated systems? Yes () No ()

c. Are there national awareness-raising programmes? ** Yes () No ()

d. Are there national cybersecurity and critical information Yes () No ()

infrastructure protection training programmes?

*** outreach programmes to, among others, children and individual users*

C. COLLABORATION AND COOPERATION

Stakeholder roles and responsibilities

5. Which role do you play in cybersecurity and critical information infrastructure protection?
(select all that apply)

- a. Policymaker () b. Regulator () c. Law Enforcer () d. Policy Implementer ()
e. Policy User () f. Academia () g. Industry Association () h. Civil Society ()
h. Other _____

6. Public-private cooperation

a. Do we have collaboration between Government and the private sector?

- Yes () Planned () No () Not Aware ()

b. If yes, select all the arrangements in place for collaboration:

Information-sharing () Incident management () Promotion of shared interests ()

Challenges redress () Others (*specify*) _____

7. Incident management and recovery

a. Which Government agency serves as the coordinator for incident management?

b. Does it have the capability for watch, warning, response and recovery functions?

- Yes () No () Not Aware ()

c. Are there arrangements in place for cooperation and trusted information-sharing?

- Yes () No () Not Aware ()

8. International Cooperation

a. Are there networks and processes of international cooperation that may enhance incident response and contingency planning?

- Yes () No () Not Aware ()

b. If yes, please list the partners and arrangements for bilateral and multilateral cooperation, where appropriate:

D. LEGAL AND POLICY FRAMEWORKS

6. Policy processes and participation

a. Are there formal and informal avenues currently for Government - industry collaboration in developing cybersecurity and critical information infrastructure protection policy?

Yes () No () Not Aware ()

b. Are the avenues adequate in achieving relevant cybersecurity and critical information infrastructure protection goals?

Yes () No () Not Aware ()

c. Could you identify other forums or structures that may be needed to integrate the government and non-government perspectives and knowledge necessary to realize national cybersecurity and critical information infrastructure protection goals?

Legal frameworks

7. Do we have an up-to-date legal framework due to the rapid uptake of and dependence upon new information and communications technologies to address the following areas?

- | | | | |
|-----------------------|---------|--------|---------------|
| a. Cybercrime | Yes () | No () | Not Aware () |
| b. Privacy | Yes () | No () | Not Aware () |
| c. Data protection | Yes () | No () | Not Aware () |
| d. Commercial law | Yes () | No () | Not Aware () |
| e. Digital signatures | Yes () | No () | Not Aware () |
| f. Encryption | Yes () | No () | Not Aware () |

8. Investigation and Prosecution

a. Has the country developed necessary legislation for the investigation and prosecution of cybercrime? Yes () No () Not Aware ()

b. What is the level of understanding among prosecutors, judges and legislators of cybercrime issues?

Excellent Above Average Average Below Average Very Poor

c. What is the adequacy of current legal codes and authorities in addressing the current and future challenges of cybercrime and cyberspace more generally.

Excellent Above Average Average Below Average Very Poor

d. Does the country participate in international efforts to combat cybercrime, such as the round-the-clock Cybercrime Point of Contact Network? *(if yes, please give details)*

Yes () No () Not Aware ()

e. Do national law enforcement agencies cooperate with international counterparts to investigate transnational cybercrime? Yes () No () Not Aware ()

If yes, what are the requirements in those instances where infrastructure is situated, or perpetrators reside in national territory, but victims reside elsewhere?

End

Thank you for your contribution!

APPENDIX 2: KEY INFORMANT INTERVIEW GUIDE

A. GENERAL INFORMATION

Please mark with an (x) or (tick) in the box with the appropriate response. Mark one box only.

1. Gender: Male () Female ()
2. Age bracket: 18 – 24 () 25 – 35 () 36 – 45 () 46 -55 () 56 and above ()
3. Highest level of education attained: Diploma () Bachelors () Masters () PhD ()
Others (specify)
4. Occupation/Employment.....
5. Designation.....

B. AWARENESS AND GLOBAL CULTURE OF CYBER SECURITY

Taking stock of cybersecurity needs and strategies

1. What is your assessment of the role of information and communications technologies in your national economy, national security, critical infrastructures (such as transportation, water and food supplies, public health, energy, finance, emergency services) and civil society?
2. Do we suffer cybersecurity and critical information infrastructure protection risks to the economy, national security, critical infrastructures and civil society that must be managed?
3. What are the vulnerabilities of the networks in use, the relative levels of threat faced by each sector, and the current management plan; note how changes in the economic environment, national security priorities, and civil society needs affect these calculations?
4. What is the national cybersecurity and critical information infrastructure protection strategy; describe its goals, the current level of implementation, measures that exist to gauge its progress, relation to other national policy objectives and how such a strategy fits within regional and international initiatives.

Developing a global culture of cybersecurity

18. What actions have been taken and what plans are in place to develop a national culture of cybersecurity referred to in General Assembly resolutions 57/239 and 58/199, including implementation of a cybersecurity plan for Government-operated systems, national awareness-raising programmes, outreach programmes to, among others, children and individual users, and national cybersecurity and critical information infrastructure protection training requirements?

C. COLLABORATION AND COOPERATION

Stakeholder roles and responsibilities

5. Who are key stakeholders with a role in cybersecurity and critical information infrastructure protection and describe the role of each in the development of relevant policies and operations, including:

- National Government ministries or agencies, noting primary points of contact and responsibilities of each;
- Other government (local and regional) participants;
- Non-governmental actors, including industry, civil society and academia;
- Individual citizens, noting whether average users of the Internet have

access to basic training in avoiding threats online and whether there is a national awareness-raising campaign regarding cybersecurity.

Public-private cooperation

8. What actions and plans are in place to develop collaboration between the government and the private sector, including arrangements for information-sharing and incident management?

9. Please share any current and planned initiatives to promote shared interests and address common challenges among critical infrastructure participants and private-sector actors mutually dependent on the same interconnected critical infrastructure?

Incident management and recovery

10. Do we have a Government agency that serves as the coordinator for incident management, including the capability for surveillance, warning, response and recovery functions; the cooperating Government agencies; non-governmental cooperating participants, including industry and other partners; and any arrangements in place for cooperation and reliable information-sharing?

11. What is the national-level computer incident response capacity, including any computer incident response team with national responsibilities and its roles and responsibilities, including existing tools and procedures for the protection of Government computer networks and existing tools and procedures for the dissemination of incident -management information?

12. Elaborate on the networks and processes of international cooperation that may enhance incident response and contingency planning, identifying partners and arrangements for bilateral and multilateral cooperation, where appropriate.

D. LEGAL AND POLICY FRAMEWORKS

Policy processes and participation

13. Identify formal and informal venues that currently exist for Government - industry collaboration in the development of cybersecurity and critical information infrastructure protection policy and operations; determine participants, role(s) and objectives, methods for obtaining and addressing input, and adequacy in achieving relevant cybersecurity and critical information infrastructure protection goals.

14. Identify other forums or structures that may be needed to integrate the government and non-government perspectives and knowledge necessary to realize national cybersecurity and critical information infrastructure protection goals.

Legal frameworks

15. Does the country possess up to date legal authorities (including those related to cybercrime, privacy, data protection, commercial law, digital signatures and encryption) that may be obsolete as a result of the rapid uptake of and dependence upon new information and communications technologies, and use regional and international conventions, arrangements and precedents in these reviews? *Ascertain whether the country has developed necessary legislation for the investigation and prosecution of cybercrime, noting existing frameworks, for example, General Assembly resolutions 55/63 and 56/121 on combating the criminal misuse of information technologies, and regional initiatives, including the Council of Europe Convention on Cybercrime.*

16. What is the current status of national cybercrime authorities and procedures, including legal authorities and national cybercrime units, and the level of understanding among prosecutors, judges and legislators of cybercrime issues?

17. Do we have adequate legal codes and authorities to address the current and future challenges of cybercrime and cyberspace more generally?






18. What is the status of national participation in international efforts to combat cybercrime? *E.g. round-the-clock Cybercrime Point of Contact Network.*

19. What are the requirements for national law enforcement agencies to cooperate with international counterparts to investigate transnational cybercrime in those instances where infrastructure is situated or perpetrators reside in national territory, but victims reside elsewhere?

End

Thank you for your contribution

APPENDIX 3: NACOSTI LICENSE

 REPUBLIC OF KENYA	 NATIONAL COMMISSION FOR SCIENCE, TECHNOLOGY & INNOVATION
RefNo: 176204	Date of Issue: 02/February/2021
RESEARCH LICENSE	
	
<p>This is to Certify that Mr. TIMOTHY OTHIENO WERE of University of Nairobi, has been licensed to conduct research in Kisumu, Mombasa, Nairobi, Nakuru on the topic: IMPLEMENTATION OF UN GGE CYBER NORMS IN THE PROMOTION OF INTERNATIONAL SECURITY: A CASE STUDY OF KENYA, for the period ending : 02/February/2022.</p>	
License No: NACOSTI/P/21/8766	
176204 Applicant Identification Number	 Director General NATIONAL COMMISSION FOR SCIENCE, TECHNOLOGY & INNOVATION
	Verification QR Code 
<p>NOTE: This is a computer generated License. To verify the authenticity of this document, Scan the QR Code using QR scanner application.</p>	

THE SCIENCE, TECHNOLOGY AND INNOVATION ACT, 2013

The Grant of Research Licenses is Guided by the Science, Technology and Innovation (Research Licensing) Regulations, 2014

CONDITIONS

1. The License is valid for the proposed research, location and specified period
2. The License any rights thereunder are non-transferable
3. The Licensee shall inform the relevant County Director of Education, County Commissioner and County Governor before commencement of the research
4. Excavation, filming and collection of specimens are subject to further necessary clearance from relevant Government Agencies
5. The License does not give authority to transfer research materials
6. NACOSTI may monitor and evaluate the licensed research project
7. The Licensee shall submit one hard copy and upload a soft copy of their final report (thesis) within one year of completion of the research
8. NACOSTI reserves the right to modify the conditions of the License including cancellation without prior notice

National Commission for Science, Technology and Innovation
off Waiyaki Way, Upper Kabete,
P. O. Box 30623, 00100 Nairobi, KENYA
Land line: 020 4007000, 020 2241349, 020 3310571, 020 8001077
Mobile: 0713 788 787 / 0735 404 245
E-mail: dg@nacosti.go.ke / registry@nacosti.go.ke
Website: www.nacosti.go.ke

APPENDIX 4: TARGET INSTITUTIONS

The study targeted the following institutions to provide information and insights.

1. Ministry of Information and Communications Technology and Youth Affairs
2. Ministry of Interior
3. Ministry of Defence/ Kenya Defence Forces
4. The National Treasury
5. Directorate of Criminal Investigations
6. Directorate of Public Prosecutions
7. Judiciary
8. ICT Authority
9. Communications Authority of Kenya
10. National Cyber Control Centre
11. Telecommunications and Internet Service Providers
12. Bankers Association of Kenya
13. The East African Science and Technology Commission (EASTECO)
14. Universities – Nairobi, Strathmore, Jomo Kenyatta, Oxford
15. Commonwealth Telecommunications Organisation
16. Global Forum for Cyber Expertise
17. Various Government Parastatals
18. Telecommunications Service Providers Association
19. Kenya Bankers Association
20. Central Bank of Kenya

APPENDIX 5: INTERNATIONAL CODE OF CONDUCT FOR INFORMATION SECURITY

Annex to the letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General (A/66/359)¹⁵⁵

Code of Conduct for Information Security

The General Assembly,

Recalling its resolutions on the role of science and technology in the context of international security, in which, inter alia, it recognized that scientific and technological developments could have both civilian and military applications and that progress in science and technology for civilian applications needed to be maintained and encouraged,

Noting that considerable progress has been achieved in developing and applying the latest information technologies and means of telecommunication,

Recognizing the need to prevent the potential use of information and communication technologies for purposes that are inconsistent with the objectives of maintaining international stability and security and may adversely affect the integrity of the infrastructure within States, to the detriment of their security,

Underlining the need for enhanced coordination and cooperation among States in combating the criminal misuse of information technologies and, in that context, stressing the role that can be played by the United Nations and other international and regional organizations,

Highlighting the importance of the security, continuity and stability of the Internet and the need to protect the Internet and other information and communications technology networks from threats and vulnerabilities, and reaffirming the need for a common understanding of the issues of Internet security and for further cooperation at the national and international levels,

Reaffirming that policy authority for Internet-related public issues is the sovereign right of States, which have rights and responsibilities for international Internet-related public policy issues,

Recognizing that confidence and security in the use of information and communications technologies are among the main pillars of the information society and that a robust global culture of cybersecurity needs to be encouraged, promoted, developed and vigorously implemented, pursuant to General Assembly resolution 64/211 of 21 December 2009, entitled —Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures,

¹⁵⁵ China, the Russian Federation, Tajikistan and Uzbekistan, “International Code Of Conduct For Information Security.”

Stressing the need for enhanced efforts to close the digital divide by facilitating the transfer of information technology and capacity-building to developing countries in the areas of cybersecurity best practices and training, pursuant to resolution 64/211,

Adopts the international code of conduct for information security as follows:

Purpose and scope The purpose of the present code is to identify the rights and responsibilities of States in information space, promote their constructive and responsible behaviours and enhance their cooperation in addressing the common threats and challenges in information space, so as to ensure that information and communications technologies, including networks, are to be solely used to benefit social and economic development and people's well - being, with the objective of maintaining international stability and security. Adherence to the code is voluntary and open to all States.

Code of conduct Each State voluntarily subscribing to the code pledges:

- (a) To comply with the Charter of the United Nations and universally recognized norms governing international relations that enshrine, inter alia, respect for the sovereignty, territorial integrity and political independence of all States, respect for human rights and fundamental freedoms and respect for the diversity of history, culture and social systems of all countries;
- (b) Not to use information and communications technologies, including networks, to carry out hostile activities or acts of aggression, pose threats to international peace and security or proliferate information weapons or related technologies;
- (c) To cooperate in combating criminal and terrorist activities that use information and communications technologies, including networks, and in curbing the dissemination of information that incites terrorism, secessionism or extremism or that undermines other countries' political, economic and social stability, as well as their spiritual and cultural environment;
- (d) To endeavour to ensure the supply chain security of information and communications technology products and services, in order to prevent other States from using their resources, critical infrastructures, core technologies and other advantages to undermine the right of the countries that have accepted the code of conduct, to gain independent control of information and communications technologies or to threaten the political, economic and social security of other countries;
- (e) To reaffirm all the rights and responsibilities of States to protect, in accordance with relevant laws and regulations, their information space and critical information infrastructure from threats, disturbance, attack and sabotage;
- (f) To fully respect rights and freedom in information space, including rights and freedom to search for, acquire and disseminate information on the premise of complying with relevant national laws and regulations;

(g) To promote the establishment of a multilateral, transparent and democratic international Internet management system to ensure an equitable distribution of resources, facilitate access for all and ensure a stable and secure functioning of the Internet;

(h) To lead all elements of society, including its information and communication partnerships with the private sector, to understand their roles and responsibilities with regard to information security, in order to facilitate the creation of a culture of information security and the protection of critical information infrastructures;

(i) To assist developing countries in their efforts to enhance capacity building on information security and to close the digital divide;

(j) To bolster bilateral, regional and international cooperation, promote the important role of the United Nations in formulating international norms, peaceful settlements of international disputes and improvements in international cooperation in the field of information security, and enhance coordination among relevant international organizations;

(k) To settle any dispute resulting from the application of the code through peaceful means and to refrain from the threat or use of force.

APPENDIX 6: RESOLUTION 70/237

Resolution adopted by the General Assembly on 23 December 2015 [on the report of the First Committee (A/70/455)] 70/237.

Developments in the field of information and telecommunications in the context of international security¹⁵⁶

The General Assembly,

Recalling its resolutions 53/70 of 4 December 1998, 54/49 of 1 December 1999, 55/28 of 20 November 2000, 56/19 of 29 November 2001, 57/53 of 22 November 2002, 58/32 of 8 December 2003, 59/61 of 3 December 2004, 60/45 of 8 December 2005, 61/54 of 6 December 2006, 62/17 of 5 December 2007, 63/37 of 2 December 2008, 64/25 of 2 December 2009, 65/41 of 8 December 2010, 66/24 of 2 December 2011, 67/27 of 3 December 2012, 68/243 of 27 December 2013 and 69/28 of 2 December 2014,

Recalling also its resolutions on the role of science and technology in the context of international security, in which, inter alia, it recognized that scientific and technological developments could have both civilian and military applications and that progress in science and technology for civilian applications needed to be maintained and encouraged,

Bearing in mind the results of the World Summit on the Information Society at its first phase, held in Geneva from 10 to 12 December 2003, and at its second phase, held in Tunis from 16 to 18 November 2005,¹

Noting that considerable progress has been achieved in developing and applying the latest information technologies and means of telecommunication,

Affirming that it sees in this process the broadest positive opportunities for the further development of civilization, the expansion of opportunities for cooperation for the common good of all States, the enhancement of the creative potential of humankind and additional improvements in the circulation of information in the global community,

Noting that the dissemination and use of information technologies and means affect the interests of the entire international community and that optimum effectiveness is enhanced by broad international cooperation,

Expressing concern that these technologies and means can potentially be used for purposes that are inconsistent with the objectives of maintaining international stability and security and may adversely affect the integrity of the infrastructure of States to the detriment of their security in both civil and military fields,

¹⁵⁶ UN General Assembly, “Resolution 70/237 - Developments in the Field of Information and Telecommunications in the Context of International Security.”

Considering that it is necessary to prevent the use of information resources or technologies for criminal or terrorist purposes,

Noting the importance of respect for human rights and fundamental freedoms in the use of information and communications technologies,

Noting also the contribution of those Member States that have submitted their assessments on issues of information security to the Secretary-General pursuant to paragraphs 1 to 3 of resolutions 53/70, 54/49, 55/28, 56/19, 57/53, 58/32, 59/61, 60/45, 61/54, 62/17, 63/37, 64/25, 65/41, 66/24, 67/27, 68/243 and 69/28,

Taking note of the reports of the Secretary-General containing those assessments,

Considering that the assessments of Member States contained in the reports of the Secretary-General have contributed to a better understanding of the substance of issues of international information security and related notions,

Bearing in mind that the Secretary-General, in fulfilment of resolution 68/243, established in 2014, on the basis of equitable geographical distribution, a group of governmental experts, which, in accordance with its mandate, considered existing and potential threats in the sphere of information security and possible cooperative measures to address them, including norms, rules or principles of responsible behaviour of States and confidence-building measures, the issues of the use of information and communications technologies in conflicts and how international law applies to the use of information and communications technologies by States, and conducted a study on relevant international concepts aimed at strengthening the security of global information and telecommunications systems,

Welcoming the effective work of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security and the relevant outcome report transmitted by the Secretary General,

Stressing the importance of the assessments and recommendations contained in the report of the Group of Governmental Experts,

Welcoming the conclusion of the Group of Governmental Experts in its 2013 report that international law, and in particular the Charter of the United Nations, is applicable and essential to maintaining peace and stability and promoting an open, secure, stable, accessible and peaceful information and communications technology environment, that voluntary and non-binding norms, rules and principles of responsible behaviour of States in the use of information and communications technologies can reduce risks to international peace, security and stability, and that, given the unique attributes of such technologies, additional norms can be developed over time,

1. *Welcomes* the 2015 report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security;
2. *Calls upon* Member States:
 - (a) To be guided in their use of information and communications technologies by the 2015 report of the Group of Governmental Experts;
 - (b) To promote further, at multilateral levels, the consideration of existing and potential threats in the field of information security, as well as possible strategies to address the threats emerging in this field, consistent with the need to preserve the free flow of information;
3. *Considers* that the purpose of such measures could be served through further examination of relevant international concepts aimed at strengthening the security of global information and telecommunications systems;
4. *Invites* all Member States, taking into account the assessments and recommendations contained in the report of the Group of Governmental Experts, to continue to inform the Secretary-General of their views and assessments on the following questions:
 - (a) General appreciation of the issues of information security;
 - (b) Efforts taken at the national level to strengthen information security and promote international cooperation in this field;
 - (c) The content of the concepts mentioned in paragraph 3 above;
 - (d) Possible measures that could be taken by the international community to strengthen information security at the global level;
5. *Requests* the Secretary-General, with the assistance of a group of governmental experts, to be established in 2016 on the basis of equitable geographical distribution, taking into account the assessments and recommendations contained in the above-mentioned report, to continue to study, with a view to promoting common understandings, existing and potential threats in the sphere of information security and possible cooperative measures to address them and how international law applies to the use of information and communications technologies by States, as well as norms, rules and principles of responsible behaviour of States, confidence-building measures and capacity-building and the concepts referred to in paragraph 3 above, and to submit a report on the results of the study to the General Assembly at its seventy-second session;
6. *Decides* to include in the provisional agenda of its seventy-first session the item entitled "Developments in the field of information and telecommunications in the context of international security". |

82nd plenary meeting

23 December 2015

APPENDIX 7: RESOLUTION 55/63

Adopted by the General Assembly - Combating the Criminal Misuse of Information Technologies¹⁵⁷

The General Assembly,

Recalling the United Nations Millennium Declaration, in which Member States resolved to ensure that the benefits of new technologies, especially information and communication technologies, in conformity with recommendations contained in the Ministerial Declaration of the high-level segment of the substantive session of 2000 of the Economic and Social Council, are available to all,

Recalling also its resolution 45/121 of 14 December 1990, in which it endorsed the recommendations of the Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders,³ and noting in particular the resolution on computer-related crimes, in which the Eighth Congress called upon States to intensify their efforts to combat computer-related abuses more effectively,

Emphasizing the contributions that the United Nations, in particular the Commission on Crime Prevention and Criminal Justice, can make in the promotion of more efficient and effective law enforcement and administration of justice and of the highest standards of fairness and human dignity,

Recognizing that the free flow of information can promote economic and social development, education and democratic governance,

Noting significant advancements in the development and application of information technologies and means of telecommunication,

Expressing concern that technological advancements have created new possibilities for criminal activity, in particular the criminal misuse of information technologies,

Noting that reliance on information technologies, while it may vary from State to State, has resulted in a substantial increase in global cooperation and coordination, with the result that the criminal misuse of information technologies may have a grave impact on all States,

Recognizing that gaps in the access to and use of information technologies by States can diminish the effectiveness of international cooperation in combating the criminal misuse of information

¹⁵⁷ UN, "UN Resolution Adopted by the General Assembly [on the Report of the Third Committee (A/55/593)] 55/63. Combating the Criminal Misuse of Information Technologies" (UN Office of Disarmament Affairs, 2001), https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf.

technologies, and noting the need to facilitate the transfer of information technologies, in particular to developing countries,

Noting the necessity of preventing the criminal misuse of information technologies, Recognizing the need for cooperation between States and private industry in combating the criminal misuse of information technologies,

Underlining the need for enhanced coordination and cooperation among States in combating the criminal misuse of information technologies, and, in this context, stressing the role that can be played by both the United Nations and regional organizations,

Welcoming the work of the Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders,

Noting the work of the Committee of Experts on Crime in Cyberspace of the Council of Europe on a draft convention on cybercrime, the principles agreed to by the Ministers of Justice and the Interior of the Group of Eight in Washington, D.C., on 10 December 1997, which were endorsed by the heads of State of the Group of Eight in Birmingham, United Kingdom of Great Britain and Northern Ireland, on 17 May 1998, the work of the Conference of the Group of Eight on a dialogue between government and industry on safety and confidence in cyberspace, held in Paris from 15 to 17 May 2000, and the recommendations approved on 3 March 2000 by the Third Meeting of Ministers of Justice or of Ministers or Attorneys General of the Americas, convened in San José, Costa Rica, from 1 to 3 March 2000 within the framework of the Organization of American States,

1. *Notes with appreciation* the efforts of the above-mentioned bodies to prevent the criminal misuse of information technologies, and also notes the value of, inter alia, the following measures to combat such misuse:

(a) States should ensure that their laws and practice eliminate safe havens for those who criminally misuse information technologies;

(b) Law enforcement cooperation in the investigation and prosecution of international cases of criminal misuse of information technologies should be coordinated among all concerned States;

(c) Information should be exchanged between States regarding the problems that they face in combating the criminal misuse of information technologies;

(d) Law enforcement personnel should be trained and equipped to address the criminal misuse of information technologies;

(e) Legal systems should protect the confidentiality, integrity and availability of data and computer systems from unauthorized impairment and ensure that criminal abuse is penalized;

(f) Legal systems should permit the preservation of and quick access to electronic data pertaining to particular criminal investigations;

(g) Mutual assistance regimes should ensure the timely investigation of the criminal misuse of information technologies and the timely gathering and exchange of evidence in such cases;

(h) The general public should be made aware of the need to prevent and combat the criminal misuse of information technologies;

(i) To the extent practicable, information technologies should be designed to help to prevent and detect criminal misuse, trace criminals and collect evidence;

(j) The fight against the criminal misuse of information technologies requires the development of solutions taking into account both the protection of individual freedoms and privacy and the preservation of the capacity of Governments to fight such criminal misuse;

2. *Invites* States to take into account the above-mentioned measures in their efforts to combat the criminal misuse of information technologies;

3. *Decides* to maintain the question of the criminal misuse of information technologies on the agenda of its fifty-sixth session, as part of the item entitled "Crime prevention and criminal justice".

81st Plenary Meeting

4 December 2000

thesis

ORIGINALITY REPORT

15%	15%	9%	6%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	cyber-peace.org Internet Source	2%
2	mgimo.ru Internet Source	1%
3	www.un.org Internet Source	1%
4	www.tandfonline.com Internet Source	1%
5	www.kictanet.or.ke Internet Source	<1%
6	erepository.uonbi.ac.ke:8080 Internet Source	<1%
7	Ruwantissa Abeyratne. "Aviation in the Digital Age", Springer Science and Business Media LLC, 2020 Publication	<1%
8	www.icta.go.ke Internet Source	<1%

ccdcoe.org

