COUNTERING CYBERCRIME IN KENYA: OUR SHARED RESPONSIBILITY

UNIVERSITY OF NAIROBI

BECKY HIMLIN ANYANGO ARUNGA

G62/40844/2021

Research project submitted in partial fulfillment of the requirement for the award of the degree of Masters of Laws (LLM)

September 2023

DECLARATION

I BECKY HIMLIN ANYANGO ARUNGA, declare that this is my original work and that it has not been submitted for award of a degree or any other academic credit to any other university.

BECKY HIMLIN ANYANGO ARUNGA

Signed  Date18th September 2023

This research has been submitted for examination with my approval as a university supervisor

Signed  ……Date 27 September 2023

DR. KEN OBURA

DEDICATION

To Jeff Collins my husband and our son Lela. You have cultivated an atmosphere of excellence, love, happiness and true courtesy in our home. This research project was made possible through your invaluable commitment and support. I dedicate this research project to you.

ACKNOWLEDGEMENT

Praise to the Lord Almighty from whom all blessings flow. He has granted me wisdom, zeal and fortitude to complete that which I began. Immense gratitude to my parents Mr. & Mrs. Tom Arunga who have given me wings to fly to heights of excellence and prosperity. I am indebted to my parents in law Mr. & Mrs. Jacob Otieno Rajwayi for their unwavering emotional, spiritual, psychosocial and financial support throughout this academic journey. You have given your absolute best to see this work come to fruition. May the blessing of the LORD continually flow upon you and your posterity.

Sincere gratitude to my supervisor, Dr. Ken Obura, who patiently bore with me and stood by me to the end of writing this Research project. Your invaluable lessons and instructions shone along my path as light through the darkness.

LIST OF STATUTES

Domestic Laws

Kenya

The Constitution of Kenya, 2010

The Computer Misuse and Cybercrimes Act, No. 5 of 2018

The Data Protection Act, No. 24 of 2019

The Kenya Information and Communication Act, No. 2 of 1998

The National Payment Systems Act, No. 39 of 2011

The Constitution of Kenya, 2010

Singapore

The Singapore Cybersecurity Act, 2018

The Singapore Computer Misuse Act, 1993

The Singapore Personal Data Protection Act, 2012

Ghana

The Cybersecurity Act, 2020

The Electronic Transactions Act, 2008

Domestic Policies

Kenya

The National Cybersecurity Strategy 2022-2027

The Kenya National Digital Master Plan 2022-2032

The Kenya Digital Economy Blue Print

Singapore National Cybersecurity Strategy

Ghana National Cybersecurity Policy and Strategy, 2015

Regional Laws

The African Union Convention on Cybersecurity and Personal Data Protection

LIST OF INTERNATIONAL INSTRUMENTS

The United Nations Convention against Transnational Organized Crime

The Council of Europe Convention on Cybercrime

The Draft United Nations Convention on Countering the Use of Information and Communication Technologies for Criminal Purposes

LIST OF ABBREVIATIONS

AG: Attorney General

ASEAN: Association of South East Asian Nations

AU: African Union

AFRIPOL: African Mechanism for Police Cooperation

CERT: Computer Emergency Response Team

CERT-GH: Computer Emergency Response Team Ghana

CMCCA: Computer Misuse and Cybercrimes Act

CSIRT: Computer Security Incidence Response Team

CSA: Cyber Security Agency/ Authority

CCS: Centre for Cybersecurity Studies

DCI: Directorate of Criminal Investigation

DPA: Data Protection Act

ECOWAS: Economic Community for West African States

ICSE: International Child Sexual Exploitation

ICT: Information and Communication Technologies

INTERPOL: International Criminal Police Organization

IP: Internet Protocol

ISP: Internet Service Provider

ISPA: Interpol Support Program for the African Union

ITU: International Telecommunications Union

KICA: Kenya Information and Communication Act

KE-CIRT/CC: Kenya Computer Incident Response Team/ Coordination Centre

KE-CIRT: Kenya Computer Incident Response Team/

NCBs: National Central Bureaus

NPS: National Police Service

NCERT: National Computer Emergency Response Team

NCSIRT: National Computer Security Incidence Response Team

OECD: Organization for Economic Cooperation and Development

SPF: Singapore Police Force

UN: United Nations

UNCTAD: United Nations Convention on Trade and Development

UNODC: United Nations Office on Drugs and Crime

UNGA: United Nations General Assembly

WSIS: World Summit on Information Society

Contents

CHAPTER ONE: GENERAL INTRODUCTION

1.1.Introduction

This thesis evaluates the efficacy of multistakeholderism in combating cybercrime in Kenya. Using a best practice approach, it explores the adequacy of the regulatory framework for multistakeholderism in countering cybercrime in Kenya. The study argues that the anonymity and borderless nature of cyberspace, coupled with the fact that the private sector controls majority of the infrastructure in cyberspace; demands for a concerted effort to engage all the stakeholders in countering cybercrime. This project calls for the need to put in place mechanisms that facilitate effective stakeholder engagement in combating cybercrime.

This chapter has outlined the background of the study while appreciating the problem statement under research. It enunciates the objectives alongside the research question and the hypothesis that the study is premised on. The justification for the study is made clearer in the literature review and the theoretical framework underpinning the study. The chapter further articulates the research methodology, with the chapter breakdown being addressed last.

1.2.Background of the study

An exponential increase in cybercrimes has been witnessed in the world in the recent past. As a borderless global village, the cyber space provides a platform that facilitates virtual connection between people regardless of their geographical location. The use of Information Communication Technologies (ICTs) for criminal purposes has resulted in both cyber dependent crimes and cyber enabled crimes. Cyber dependent are crimes that can only be committed with the use of ICTs.[1] While cyber enabled crimes refer to traditional crimes that are exacerbated by the use of ICTs.[2] Cybercrime is predominantly transnational, hence investigation using traditional criminal justice frameworks is quite complex. This is largely due to variation in legal framework in various jurisdictional.[3]As a result, corporations and industry have increasingly been involved in mitigating various forms of cybercrime.[4] Especially since these corporations control the technological infrastructure that is often handy in ensuring effective investigation of cybercrime. Consequently,

[1] Available at https://www.thamesvalley.police.uk/police-forces/thames-valley-police/areas/c/2018/protect-your-world/protect-your-world-the-risks-of-cyber-crime/ last accessed on 01.12.2023 at 1111hrs
[2] Ibid
[3]T. Holt. *Regulating Cybercrime through Law Enforcement and Industry Mechanisms*. The Annals of the American Academy of Political and Social Science, September 2018, Vol. 679, (September 2018), p. 140
[4]Ibid

effective investigation and prosecution of cybercriminals is heavily dependent on effective collaboration between law enforcement and industry.[5]

In spite of this heavy control of the cyberspace by technology companies, governments still reserve their state sovereignty and power to protect the legitimate interests of individual states. Accordingly calling on law enforcement to adapt their crime response strategies to the changing criminal environment in the cyberspace, including through strategic partnerships with stakeholders.[6]Such partnerships are not without criticism, as States are reluctant to confidently engage the private sector in countering cybercrime. This is largely attributed to the treatment of cybercrime as a security issue deserving a security-based intervention. Hence the need to create a platform upon which States and key stakeholders can engage in Cybercrime discussions without fear.[7]

The reality is that computer systems by nature possess qualities that require consideration and attention by law enforcement agencies. The fact that technology is constantly advancing may appear to curtail any efforts made to counter cybercrime. However, it is by understanding the tenor of computer systems that civilization has attempted to develop legislation that addresses cybercrime.

To begin with, attribution or identification of individuals controlling computer systems is difficult.[8] Similarly, expeditiously locating information from voluminous data sets is often an arduous task.[9] Especially where criminal groups employ data anonymization software to avoid detection by law enforcement agencies.[10] This is further exacerbated by software that facilitate destruction of evidence. As a result, time is often of essence in effective cybercrime investigation. Also, remote storage of data poses significant challenges in accessing data, especially through

[5] Ibid

[6]J.Yun, *The criminal Justice Response and Development Strategy in the age of the Fourth Industrial Revolution* (II): The Internet of Things and Blockchain, Korea Institute of Criminology and Justice, No. 013 April 2021 at pg. 1.Available at https://www.kicj.re.kr/board.es?mid=a20203000000&bid=0031 Last accessed on 30.06.2023 at 1243hrs

[7]Hutchings, Alice, and Thomas J. Holt. 2015. *A crime script analysis of the online stolen data market*. British Journal of Criminology 55:596–614

[8] The High Court of Kenya in Bloggers Association of Kenya versus DPP and others Pet 206 of 2019 took judicial notice of the nature of computer systems in determining the constitutionality of procedures by investigation officers under the Computer Misuse and Cybercrimes Act, 2019 Available at http://kenyalaw.org last accessed on 21.11.2023 at 0950hrs

[9] Ibid.

[10] Ibid

search and seizure. Unfortunately, whereas there is widespread manifestation of cybercrime, a very low proportion of cybercrime is brought to the attention of law enforcement. Essentially, the complexities attending cybercrime investigation require involvement of forensic experts using forensic techniques to detect and counter cybercrime.[11] As a result, it is necessary to develop an effective stakeholder framework to effectively counter cybercrime.

In light of these challenges, States have increasingly recognized the need to develop mechanisms and clear frameworks to combat cybercrime.

1.2.1. Historical developments towards countering cybercrime

New methods of perpetrating crimes have emerged following advancements in computer technology. The cyberspace provides an avenue through which ordinary crimes are committed with increased intensity and magnitude. Suffice to say, traditional laws on criminal conduct were not enacted with the cyberspace in mind; hence the challenge in applicability of such legislations to cybercrime. Remarkably, whereas traditional criminal law has evolved over time since the inception of societies, cybercrime legislation has been necessitated by advancements in Information Communication Technologies. Arguably, it is safe to say that traditional criminal laws are unable to keep pace with cybercrime.

It is trite that a crime must be sufficiently defined to enable law enforcement agencies adequately address it. Hence the need to develop concise legislation that distinguishes cybercrime from ordinary crime. Also, it was necessary that the transborder aspect of cybercrime be dealt with through harmonization in legislation through Conventions, Treaties and International Instruments among others.

The first international initiative on Cybercrime was held in 1976, when the Council of Europe held a conference on criminological aspects of economic crime. Ultimately resulting into identification and classification of several categories of cybercrime.[12] In 1977, the United States' Federal Computer Systems Protection Act was unsuccessfully debated into law.[13] Nevertheless,

---

[11] Ibid

[12] A Paper for the 12th Conference of Directors of Criminological Research Institutes: Criminological Aspects of Economic Crime, Strasbourg, 15-18 November 1976, page 225-229.

[13] Congressional Record, 95th Congress, Vol. 123, No. 111, June 27, 1977

it raised significant awareness on the impact of unauthorized computer usage and the necessity of flexibility in addressing computer related crimes.

The first international organization to address cybercrime was the International Criminal Police Organization (INTERPOL). In its third International Symposium on International fraud in 1979, it urged the need for substantive law on computer crime.[14] Following the conference, INTERPOL initiated capacity building on computer crimes for its member countries. Consequently, demonstrating the first step towards harmonization of penal laws on computer crime around the world.

In 1982, the Organization for Economic Cooperation and Development (OECD) appointed a committee of experts to discuss computer related crime. The Committee was also mandated to develop a framework that provided for the amendment of the penal laws of various states to address cybercrime.[15] As a result of their recommendations, a definition was crafted for computer crimes. The definition addressed salient legal and ethical issues in automatic processing and transmission of data.[16]

Ultimately, in 2001 the Council of Europe adopted the Convention on Cybercrime (Budapest Convention)[17] to pursue a common policy towards protection of the society against cybercrime. This was to be achieved by adopting appropriate legislation and fostering international cooperation. Impressively, the Convention was open for ratification by States within and outside the Council Europe.[18] Thus, it became the first Convention of an international nature on cybercrime.

In the absence of a United Nations (UN) globally binding instrument on cybercrime, the

[14] The Third Interpol Symposium on International Fraud, Saint-Cloud, Paris, France, December 11-13, 1979.

[15] A group of experts met at the OECD in Paris on May 30, 1983: Mme C.M.Pitrat, France, Mr. M. Masse, France, Mr.A. Norman, United Kingdom, Mr. S. Schjolberg, Norway, Mr. B. de Schutter, Belgium, and Mr. U. Sieber, Germany. These" founders " of the harmonization of European computer crime legislation recommended that the OECD should take an initiative. An expert committee was established, and recommended in September 18, 1986 through the ICCP Committee a common denominator between the different approaches taken by the Member countries.

[16] Computer-related criminality: Analysis of Legal Politics in the OECD Area (1986

[17] The Budapest Convention

[18] Article 37 of the Convention

International Telecommunications Union (ITU) has been instrumental in coordinating responses to cybersecurity and cybercrime. In 2006, ITU was tasked by the United Nations General Assembly (UNGA) to coordinate robust multistakeholder participation in the events of the World Summit on Information Society (WSIS).[19] Ultimately leading to the development of the Global Cybersecurity Agenda (GSA) in 2008. The GSA addresses identified key principles that embody a stakeholder framework for countering cybercrime such as: Legal Measures, Technical and Procedural Measures, Organizational Structures, Capacity Building and International Cooperation. Furthermore, ITU has developed a National Cyber Strategy Toolkit to assist States develop or improve their national cybersecurity strategies.[20] Essentially, ITU calls upon governments to cooperate with stakeholders towards countering cybercrime.

Though there is no binding UN Convention on cybercrime, the UN General Assembly has consistently passed resolutions geared towards recognizing and addressing cybercrime.[21] Notably, it is in the process of developing the Convention on the use of Information and Communication Technologies for criminal purpose. Should this convention come into force, it will be the first global Convention under the auspices of the United Nations to address Cybercrime.

Regionally, the African Union developed the African Convention on Cybersecurity and Personal Data Protection (the Malabo Convention) in 2014. Operationalization of the Convention was conditional on ratification by at least fifteen member states.[22] Unfortunately, almost a decade lapsed before the Convention entered into force since the threshold for ratification had not been made. However, in May 2023 the Convention finally came to force following ratification by Mauritania (the 15th member state to ratify the Convention).[23] The Convention calls on member states to develop effective national cybersecurity policies and strategies.[24] It also requires member states to develop institutions and procedures to identify and report cybersecurity; as well as to

[19] Available at https://cybercrimelaw.net/documents/cybercrime_history.pdf last accessed on 24.11.2023 at 1012hrs
[20] National Strategy Toolkit introduction.pdf, Available at https://www.itu.int/en/Pages/default.aspx last accessed on 24.11.2023
[21] Un Resolutions 55/63 of 2000 and 56/121 of 2001 on combating criminal misuse of Information and Communication Technologies.
[22] Article 36 of the Convention
[23] Available at https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection last accessed on 30.11.2023 at 0133hrs
[24] Article 26 of the Convention

ensure international cooperation on cybersecurity and cybercrime.[25]

In 2018, Kenya enacted the Computer Misuse and Cybercrimes Act as the substantive penal statute on cybercrime. The Act also provides for mechanisms and procedures towards countering computer and cybercrime; including promotion of international cooperation.[26] Though both the Budapest and the Malabo Conventions have been open for ratification, Kenya is yet to sign either of the Conventions. Nevertheless, Kenya is a member of the International Telecommunication Union and has greatly benefited from the cybersecurity initiatives by the ITU. In fact, prior to the enactment of the Computer Misuse and Cybercrimes Act, certain cybercrimes were established and largely governed by the Kenya Information and Communication Act, No. 2 of 1998. The Act establishes[27] the Communication Authority which houses the Kenya Computer Incident Response Team (KE-CIRT). The Kenya Cyber Strategy 2022 seeks to convert the KE-CIRT into the National Multistakeholder Computer Incident Response Team towards strengthening coordination, collaboration and cooperation in combating cybercrime.

Arguably, from the historical developments in countering cybercrime, it appears an effective framework for countering cybercrime exists in enhanced cooperation among all those who have a stake in governance of cyberspace. A multistakeholder approach would provide a platform upon which all stakeholders work together towards combating cybercrime. Hence then need for shared responsibility among all stakeholders to wit: States, non-state actors, and private companies among other stakeholders, towards countering cybercrime. This paper therefore seeks to critically analyze the efficacy of multistakeholderism in combating cybercrime in Kenya.

1.3.Statement of the Problem

The evolution of cybercrime has been exponential and rapid. Actors in the criminal justice system in Kenya have experienced multiple challenges in their attempt to hold accountable cybercriminals. Difference in legal systems between countries coupled with variations in national cybercrime laws pose a major challenge to law enforcement officers. Variation in legal frameworks of various States has significantly impacted State capacity to address transnational

[25] Article 28

[26] Long title of the Computer Misuse and Cybercrimes Act, No. 5 of 2018 available at https://kenyalaw.org last accessed on 24.11.2023 at 1036 hrs

[27] Section 3 of the Kenya Information and Communication Act, No. 2 of 2018 Available at http://kenyalaw.org:8181/exist/kenyalex/actview.xql?actid=No.%202%20of%201998#part_II last accessed on 24.11.2023 at 1045 hrs

cybercrime. In fact, differences in the rules of acquiring evidence further stymies the capabilities of law enforcement to access digital evidence needed for successful cross border investigation and prosecution of cybercrime.

Notably, variation in scope and applicability of cybercrime Treaties coupled with legal challenges of data protection and human rights affect the efficiency of cybercrime investigation and prosecution. Technical challenges such as attribution negatively affects the quality of investigations as cybercriminals utilize technology to evade recognition by law enforcement officers.[28]As a result, establishing the critical elements needed to prove a criminal offence against the cybercriminals become a challenge. Moreover, software vulnerabilities easily grant cybercriminals opportunities to access computer systems without permission as the computer systems become vulnerable to unauthorized access by cybercriminals.

Evidently, the borderless and decentralized nature of cyberspace poses significant challenges to law enforcement to effectively counter cybercrime in spite of the existing legislative framework. In instances where virtualized information technology infrastructure is employed, it is imperative that the service provider be involved to assist law enforcement in cybercrime investigation. Arguably, effective cybercrime investigation and prosecutions requires a concerted effort from all the key stakeholders. This research therefore analyses the adequacy of the regulatory framework for multistakeholderism in combating cybercrime in Kenya.

1.4.Objectives of the Study

The key objective of the study is:

To understand the concept of multistakeholderism and critically examine its efficacy in combating cybercrime in Kenya.

The subsequent specific objectives of the study are to:

a. To understand the nature of cybercrime and expose the stakeholders directly involved in the governance of the cyberspace

[28]Available at https://www.unodc.org/e4j/en/cybercrime/module-1/key-issues/cybercrime-trends.html#:~:text=The%20main%20legal%20challenges%20to,authorities%20can%20access%20digital%20evidence last accessed on 13th September 2023 at 1424 hrs.

b. To assess the national and international best multistakeholderism practices in combating cybercrime
c. To review the adequacy of the regulatory framework for multistakeholderism in combating cybercrime in Kenya
d. To elucidate recommendations based on the findings of the study.

1.5.Research Questions

The main research question in this study is this:

How effective is multistakeholderism in combating cybercrime in Kenya?

The ensuing specific research questions are:

a. Which stakeholders are involved in combating cybercrime?
b. What is the international and national best multistakeholderism practices in countering cybercrime?
c. How adequate is the regulatory framework for multistakeholderism in combating cybercrime in Kenya?
d. What recommendations can be elucidated from the findings of the study?

1.6.Hypothesis

This research is predicated on the following hypothesis:

a. The trans-border nature of cybercrime coupled with anonymity pose a serious challenge to law enforcement agencies in investigation and prosecution of cybercrime;
b. Effective cybercrime investigation and prosecution requires the involvement of all stakeholders;
c. The existing regulatory framework for multistakeholder engagement in countering cybercrime in Kenya is inadequate

1.7.Justification of the Study

In an age where individual abilities are hailed and heroic acts celebrated by communities. It is important to underscore that this mutual cooperation can be extended to the fight against the offences committed in the cyber space. Through this study, the reader will understand and appreciate the importance of unity of purpose in combating cybercrime in Kenya.

The study gives society a chance to expand its scope and thinking and realize that the victory over cybercrime cannot be won by the state alone. Each stakeholder has a role to play in facilitating the investigative and prosecutorial role of law enforcement agencies.

Though States are separated by defined geographical borders, the internet places States in virtual and borderless situations that call for mutual cooperation to determine the identity and physical location of the criminal behind the screen. Additionally, variation in legal systems of States calls for mutual legal assistance to facilitate prompt sharing of crucial evidence needed for investigations and judicial proceedings. It is therefore necessary to have increased and enhanced collaboration among states, international agencies, and private sector and non-state actors in countering cybercrime.

This research not only opens the mind to the existing legal framework on countering cybercrime, but also exposes national and international best practices that have been successfully adopted by Singapore and Ghana towards combating cybercrime. Accordingly increasing utility to the society by encouraging a culture of cooperation among State and non-state actors.

1.8.Literature Review

This literature review focuses on how various authors have addressed multistakeholderism as a suitable model for governance of the cyberspace. It looks at the competing interests in multistakeholder models in governing the cyberspace. The main issues addressed in considering multistakeholder models of governance is the aspect of State sovereignty. This leads to challenges such as suspicion and lack of openness in engaging stakeholders in addressing issues of mutual concern.

With sovereignty, States can claim, and are mutually recognized as having exclusive authority and control within a specific geographical boundary. Consequently, the state is the only entity that can set and enforce rules within a territory. Sovereignty gives States the power to define the activities to be controlled and the manner that they will be controlled. The private sector is crucial in promptly recovering evidence on cybercrime, alerting law enforcement agencies on any data breaches and expunging of private sector holds much of the evidence of cybercrime, reporting data breaches and elimination of illegal content from the cyberspace. John Perry[29] dramatically

[29]Barlow, John Perry. "*A Declaration of the Independence of Cyberspace*." (1996). Available at https://wac.colostate.edu/ rhetnet/barlow/barlow_declaration.html

announced in 1996 that the sovereignty of states did not extend to the cyberspace. He is quoted to have stated that:

> *"Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather."*

The limitations of this perspective are evident in the manner in which the cyberspace has exponentially grown. Increasingly, the need to address challenges unique to the cyber space has been realized. Privacy, security and protection of consumer interests among others should be given attention as most cybercrime largely impacts these rights.[30]

In view of the above, there is need to develop a multistakeholder approach in the realm of governance of cyberspace towards countering cybercrime. The Global Commission on internet governance opine that multi stakeholder[31]refers to a model in which affected stakeholders desirous of participating in decision making can without granting any single entity absolute control. The multistakeholder approach envisions collaboration among governments, academia, private sector, civil society organizations, the public and international organizations.

According to Glekmann[32]multistakeholderism is a global governance system that unites actors with an interest in an issue or a subject. Subsequently, the stakeholders are required to collaboratively develop a solution. This is often contrasted with multilateralism which vests the ultimate decision-making power on governments. As representatives of their citizens, they consequently require international organizations to implement the decisions as directed.[33] He opines that this definition falls short of defining who a stakeholder is. The multistakeholderism approach presents a situation where there are equal actors, who make decisions and develop policies and programs. [34]

---

[30]Sivasubraminian Muthusamy, "*Building Suitable Frameworks for Internet Governance*" in Collaboratory Discussion Paper: Internet Policymaking, Multistakeholder Internet Dialog (2013), 81. Available at http://www.collaboratory. de/w/Building_Suitable_Frameworks_ for_Internet_Governance_The_Interplay_ between_Technology_and_Policy

[31]Global Commission on Internet Governance, "One Internet," Centre for International Governance Innovation and The Royal Institute for International Affairs, (2016) https://www.ourinternet.org/report

[32]Haris Glekkmann, *Multistakeholder Governance and Democracy: A Global Challenge* (Routledge 2018)

[33] Ibid

[34] Ibid

Though this approach assumes that every stakeholder has equal rights in governance Glekkmann argues that there is power imbalance between the various stakeholders in the cyberspace. While there are some who are openly powerful, private actors and civil society may lack the wherewithal to represent an equal voice at a governance forum. Though this observation is commendable, he fails to provide a solution on how stakeholders ought to address this power imbalance. Especially where arguments for sovereignty and the role of the State in ensuring the security of its citizens take prominence. In most countries, countering cybercrime has taken a security approach. As a result, intelligence agencies and law enforcement are reluctant to involve key stakeholders in making key decisions that impact investigation and prosecution of cybercrime.

He also takes a law-based approach where he posits that Nation States have the capacity to address the challenges posed by cyberspace through the use of law.[35] Further, he points out that the multistakeholder approach ought to embrace aspects of corporate partnerships, volunteering, decision making on different subjects in order to put up a united front in countering cybercrime. To achieve global representation, it is important that Nation States demarcate the territorial sphere of operation to avoid superiority conflicts between the State parties.

Glekmann[36]proposes that multistakeholderism approach works best in situations where there is mutual understanding on the need for inclusivity, openness, accountability, shared responsibility and effective decision making. As this would readily promote collaboration and information sharing without restriction.

It has been observed that a multistakeholder model does not take an exclusionary approach in providing solutions to issues. It provides a mechanism for solving specific problems or assisting institutions in transition to find a best approach to handling challenging situations.[37] In the cyberspace, it envisions the sharing of responsibility for continued vitality of the cyberspace for the benefit of societies and the global economy. Indeed, successful identification and implementation of solutions for countering cybercrime requires collaboration among stakeholders in the cyberspace. International organizations, States, Civil Society Organizations, Academia and

[35]Ibid
[36] Ibid
[37]www.internetsociety.org/what-we-do/internet-issues/internet-governance last accessed on 7th February 2022 at 1923hrs

the Private Sector are key stakeholders in countering cybercrime.[38]Though this stakeholder collaboration is not as easy as passing a domestic legislation, mutual interests in the security of the cyberspace coupled with hard work make its implementation a success.[39]

Holt[40] suggests that cybercrime can be suitably regulated through law enforcement and industry mechanisms. He opines that this approach creates a balanced approach in the regulation of cybercrime since it ensures that neither law enforcement nor industry is a dominant player. Whereas Holt appreciates the jurisdictional challenges posed by cybercrime, he does not specifically propose multistakeholderism as the most suitable strategy in the regulation of cybercrime. This research therefore posits that not only should law enforcement and industry be involved in countering cybercrime, but also all who have a stake in the internet be involved combating cybercrime.

Goldsmith decries the stand taken by regulation skeptics who opine that the State should not regulate Cyberspace at all. He states that the regulation skeptics allege that the special treatment of cybercrimes makes no sense as the unique elements of a criminal offence can still be identified whether an offence was committed offline or online.[41] The regulation critics further argue that regulation of cyberspace activity in one jurisdiction may cause a spillover negative effect in another jurisdiction. Accordingly, the regulation skeptics argue that cyberspace participants are better placed to regulate activity in the cyberspace. This would not only internalize the costs of cyberspace activity but also notify cyberspace participants of the regulations developed.[42]

In challenging the argument of the regulation skeptics, Goldsmith avers that the role of regulating harmful activities with a view to protecting the citizens' best interest is vested on the State.[43] Whether the activity is carried out in cyberspace or in the real world.[44] Additionally, he opines that the state has the mandate to set mandatory laws that protect third parties and places limits on the power of private parties in the cyberspace. He further points out that traditional justice tools can still be handy in addressing conflict of laws in the cyberspace. Consequently, he affirms that

[38] Ibid
[39] Ibid
[40] Ibid
[41]Jackson L. Goldsmith, *Against Cyberanarchy*, The University of Chicago Law Review, vol 65 (1998) p. 1200
[42] Ibid
[43] Ibid
[44] Ibid

regulation of cyberspace is feasible using arguments on jurisdiction and choice of law. Although this is a progressive read on jurisdiction and choice of law in cyberspace, it fails to acknowledge the uniqueness of cybercrime investigation and prosecution in terms of appreciating the specific roles played by other stakeholders in dealing with jurisdictional challenges.

It has been argued that relying on the traditional mechanisms of formal cooperation on cybercrime matters is not effective in granting timely and expedited access to digital evidence needed in cybercrime investigation and prosecution.[45]Large scale cybercrime poses significant challenge, as law enforcement agencies have to access industries located across divergent geographic regions and sectors.

In highlighting the nature and forms of cybercrime, R. Sabillon et al discuss the complexity and vastness of cybercrime as the greatest argument in favour of a concerted approach towards countering it.[46] They propose that combating cybercrime begins with first taking personal measures for protection. Hence highlighting the need for creation of national mechanisms for combating cybercrime, international cooperation in prosecuting cybercrime, clear laws for prosecution, extensive academia research and enhanced private sector engagement in cybersecurity and cybercrime. The authors have however failed to enunciate the manner in which these stakeholders, especially industry, ought to be involved in cybercrime investigation and prosecution.

Arief and Azeem opine that the best way to combat cybercrime is to understand it in detail beginning with the stakeholders involved.[47] Some of the proposals for combating cybercrime that they further propose include partnerships and shared responsibility among governments, individuals and private industry. Admittedly, in protecting the interests of its citizen, the State is required to skillfully balance the dual interests of the right to security and privacy. Such an approach would curtail the misuse of security solutions to cybercrime.[48] In highlighting the importance of multistakeholderism in combating cybercrime, the authors emphasize the need for government, organizations, industry, education and research institutions to work closely to

[45]UNODC Comprehensive study on cybercrime, 2013
[46]R. Sabillon et al, *Cybercrime and Cybercriminals: A Comprehensive Study*, International Journal of Computer Networks and Communication Security, vol 4, 2016
[47]B. Arief and M. Azeem, *Understanding Cybercrime from its Stakeholder's Perspective*, Defenders and Victims, Newcastle University, 2015
[48] Ibid

construct a coherent strategy for combating cybercrime. It is commendable that the authors propose that a regulatory body needs to be established that receives reports on cybercrime. However, it falls short of describing the nature of the regulatory body.

Kenya has specifically enacted a law that deals with cybercrimes.[49] Whereas the law provides for a series of cybercrime related offences, it is noteworthy that the law is silent on multistakeholderism in combating cybercrime. This therefore calls for the need to embed multistakeholder approach to facilitate effective investigation and prosecution of cybercrime.

Fighting cybercrime is an ongoing effort, cybercriminals are continually evolving their skills with every technological advancement. Though multistakeholderism is fronted as the best way to combat cybercrime, there is a dearth of information and literature on effective multistakeholder models in countering cybercrime.

1.9.Limitations

The limitations of this study include:

a. The changing face of cybercrime makes it difficult to ascertain a model that can best be employed to combat cybercrime.
b. Lack of qualitative sources on materials on the efficacy of multistakeholderism in combating cybercrime. This has not been widely explored in Kenyan scholarship.

1.10. Theoretical Framework

This study is premised on the social contract theory and the digital realist theory.

1.10.1. Social Contract Theory

The main argument of this theory is the recognition of enforcement of sanctions as a key tenet of societal order and wellbeing.[50]According to Gauthier, a theory of morals can only serve a useful purpose if its propositions are accepted and adopted in the individual reasoning of each member

[49]The Computer Misuse and Cybercrimes Act, 2020

[50] Available at https://ethicsunwrapped.utexas.edu/glossary/social-contract-theory#:~:text=Social%20contract%20theory%20says%20that,a%20divine%20being%20requires%20it. Last accessed on 14th September 2023 at 1313hrs

of the society.[51] Ultimately positing that societal norms can be justified on the basis that each member is capable of agreeing to a certain rule or principle.[52]

In relying on this theory, this research seeks to establish that the borderless nature of the internet creates a global village that can collectively agree on principles suitable for their wellbeing. Netizens on cyberspace voluntarily binds themselves to the rules, principles and obligations 'agreed upon by other users. The cyberspace affords a space where people who share unique sets of values regarding various concepts meet for different activities, likes and perceptions. As a result, it is prudent that they be involved in addressing key challenges that impact their experience in the cyberspace.

Furthermore, the social contract theory requires collective enforcement of societal norms by all members of the society. Hence it is in the interest of society to enforce rules that ensure safety and security for everyone, even the weakest. Through this theory, it is possible to create a flourishing society by involving all stakeholders in countering cybercrime. At the heart of this theory is the assurance that the contract ensures the security and wellbeing of all. The theory offers the basis to understand why society implements rules, regulations and laws capable of being enforced. In fact, it justifies the power that law enforcement can exert over the population as a whole.

The main criticism of this theory is the disturbing element of consent. Variation in cultures and legal systems makes it difficult to assume a uniform moral code binding upon all netizens. Accordingly, without clearly set rules, guidelines and principles, it is difficult to identify rules that can be used to hold netizens accountable in the cyberspace. Therefore, the most prudent way to address this would be to identify stakeholders, who not only formulate policies but also actively engage in holding netizens accountable. Positivists such as Bentham posit that whereas it is morally right to protect rights in society, variation in societal contexts demonstrate that what is prioritized in one society is materially different from that which is prioritized in another.[53] Especially since it is almost impossible to justify principles to all reasonable citizens or persons.

---

[51]Gauthier, David, 1986. *Morals by Agreement*, Oxford: Clarendon Press.
[52]Scanlon, Thomas, 1998. *What We Owe to Each Other*, Cambridge, MA: Harvard University Press.

[53]Jeremy Bentham, *Anarchical Fallacies*, vol. 2 of Bowring (ed), Works 1843

1.10.2. The Digital Realism Theory

The digital realism theory is one of the theories that attempts to explain the governance of cyberspace. This theory rests on the fact that challenges arising out of the cyberspace can be dealt with under the existing legislative framework without having to come up with specific legislation for the cyberspace. The realists opine that the impact of the law alone on behaviour is limited. However, the law has the power to shape the environment in which an individual's action occurs.[54] In this regard, technology creates the environment in which the criminal conduct takes place. Accordingly, neither law nor technology is solely considered as a driver for social action.

The digital realists argue that technology is in constant flux, subsequently, no legislation can adequately predict and address all the issues or frontiers of technology and the cyberspace.[55] It is therefore important to find a way in which the various legal systems of States can offer solutions to issues and conflicts arising from the cyberspace without enacting new legislation. This theory is premised on the rule of law can be extended into cyberspace, as it has been extended into every other field of human endeavor.

In an attempt to explain internet governance, this theory emphasizes the existence of state sovereignty within its territorial borders. Accordingly, in as much as the cyberspace is a borderless village, individual states have control and jurisdiction over activities done on cyber spaces within its geolocation. This position is supported by Goldsmith who avers that regulation of the cyberspace is feasible and legitimate on the basis of jurisdiction and choice of law rules.[56] He further says that actions in cyberspace and the real world are similar as they both have territorial consequences.[57]For instance, if internet users in one jurisdiction sends a malware attack on a computer system in another jurisdiction, the rationale for regulating such conduct is similar to the rational for regulating harm in the real world.[58]

While emphasizing the aspect of State sovereignty, the digital realists elevate the crucial role of law in regulating human behaviour. This can be satisfactorily achieved through the application of existing laws to the cyberspace issues. The digital realist's theory emphasizes the role of law as a

[54]Wall David, *Digital Realism and the Governance of Spam as Cybercrime*, vol.10 European Journal of Criminal Policy and Research, 2004
[55] Ibid
[56]Jack.L Goldsmith, *Against Cyberanarchy*, vol. 65 No. 4 The University of Chicago Law Review, p. 1201
[57] Ibid
[58] Ibid

key governance device while emphasizing on national legislation as opposed to international legislation.

This theory is relevant to this study to show the limitations of law in governance. It appreciates that in as much as legislation can be put in place to address certain aspects of technology and the internet, such regulation cannot adequately keep up with the advancements in technology. The main criticism of this theory is its failure to appreciate the unique and distinct characteristic of cybercrimes and the unique response that is required in addressing them.

1.11. Research Methodology

This study shall heavily rely on desk-based research of both primary and secondary sources. This has been achieved through the use of online resources including journals, articles and other resources available on the internet. The research has also utilized library resources such as books, reports and statutes that are relevant to the question at hand.

It takes a best practice approach by studying multistakeholderism in combating cybercrime Singapore and the Republic of Ghana. Though Singapore has not ratified any international treaty or convention on cybercrime, it has a robust cybersecurity framework premised on stakeholder engagement. It has been proactive in Cyber capacity building[59] in the Association of South East Asian Countries, making it a force to reckon with in cybersecurity. On the other hand, Ghana has a robust legal framework on multistakeholderism in combating cybercrime. It is one of the African countries that is a party to both the Budapest Convention and the Africa Convention on Cyber Security and Personal Data Protection. Consequently, it is positioned to deal with issues of international cooperation, technical assistance and capacity building on cybercrime and cybersecurity.

This methodology is suitable in dealing with the research questions as it offers an in-depth perspective on the issues surrounding cybercrime and multistakeholderism. Additionally, it exposes the international standards that have been successfully adopted by Ghana and Singapore towards countering Cybercrime.

[59] Available at https://ccdcoe.org/incyder-articles/asean-cyber-developments-centre-of-excellence-for-singapore-cybercrime-convention-for-the-philippines-and-an-open-ended-working-group-for-everyone/ last accessed on 15th March 2023 at 1203 pm

The information gathered through review of books, journals, articles and online sources has been analyzed to find out the outcome of the study in general.

1.12. Chapter Breakdown

This research work shall consist of five chapters.

Chapter one is the introduction that outlines the general framework of the research work. This chapter also includes the theoretical framework of the research, the research methodology as well as the literature review. The general framework of the research is covered in this chapter.

Chapter two seeks to understand the nature of cybercrime while exposing the stakeholders directly involved in investigation and prosecution of cybercrime. Additionally, it highlights the importance of stakeholder engagement in countering cybercrime.

Chapter three assess the international and national best multistakeholderism practices in combating cybercrime with a focus on the practice in Singapore and Ghana.

Chapter four analyses legal and institutional framework for multistakeholderism in countering cybercrime in Kenya.

Finally, the last chapter concludes the study by enunciating the recommendations based on the findings of the study.

CHAPTER TWO: NATURE AND FORM OF CYBERCRIME ANDTHE STAKEHOLDERS INVOLVED IN COMBATING CYBERCRIME IN KENYA

2.1. Introduction

Emerging technologies create new opportunities for committing crime without necessarily changing the type of offences committed. In fact, most offences that would have otherwise been committed offline, are replicated with more intensity, greater ease, greater speed and magnitude through the online/ virtual/ internet platform. Hence, it is safe to say that the main difference between cybercrimes and traditional crimes is the use of ICTs in the former.

The cyberspace provides a platform for extension in criminal behaviour as well as novel criminal activity. Using the cyberspace, cybercriminals attack information about individuals, corporations and governments to the detriment of the victim of the crime. Interestingly, cybercrime has a transnational element as it can involve jurisdictions separated by vast distances, hence the need for effective international cooperation and mutual legal assistance. Interestingly, cybercriminals often leave behind a digital footprint that can be used to track their identity and location despite their best efforts to cover their tracks.

This chapter focuses on the nature and form of cybercrime with a view to expose the stakeholders involved in cybercrime investigation, prosecution and adjudication in Kenya.

2.2. Nature and Form of Cybercrime

Though there is no globally accepted definition of cybercrime, there are certain elements that comprise cybercrime. For instance, the use of ICTs in the commission of the unlawful act. The definition of cybercrime can thus be derived from the elements of cybercrime.[60]In Kenya, the offence is defined as an unlawful act that is perpetrated using ICT to either target networks, systems, data, websites and or technology or facilitate a crime.[61] Essentially, it is an offence against a computer system.[62] In cybercrime, a computer is either the subject of the crime: as is the case in ransomware or the instrument to further illegal ends, such as committing fraud, infringement of intellectual property, or violating privacy.[63]In situations where a computer is the target of the

[60]Available at https://www.unodc.org/e4j/en/cybercrime/module-1/key-issues/cybercrime-in-brief.html last accessed on 18th May 2023 at 1032 hrs

[61]Preamble of the Kenya Computer Misuse and cybercrimes Act, no. 5 of 2018

[62] The Budapest Convention on Cybercrime defines a computer system as any device which performs automatic processing of data.

[63] Available at https://www.britannica.com/topic/cybercrime, last accessed on 18th May 2023 at 0844hrs

offence, the crime negatively impacts the integrity, confidentiality and availability of a computer data or systems. The concept of cyber-dependent crimes and cyber enabled crimes emanate from this dual definition of cybercrime.[64]

2.2.1. Categories of Cybercrime

Just like in real world crimes, cybercrimes may also be committed by individuals or criminal gangs. Cybercrime in one jurisdiction can negatively impact citizens in another different jurisdiction. Hence the need to enact and harmonize definitions of cybercrime to facilitate accountability. There is no global treaty on cybercrime under the United Nations. However, it is noteworthy that State there is a draft UN Convention on Use of ICT for criminal purposes that is being negotiated. Upon its adoption, it will be the first global instrument on cybercrime.

Regional bodies have stepped up to develop legal frameworks on cybercrime in the absence of a global binding treaty on the same. The Council of Europe Convention on Cybercrime, 2001 (The Budapest Convention) was the first of its kind to identify cybercrime and provide a framework for mutual legal assistance in investigation and prosecution of Cybercrime.[65] The African Union (The Malabo Convention) has also developed a Convention to address the mushrooming cybercrime menace.[66]

The Budapest Convention identifies four categories of cybercrime: offences against the confidentiality, integrity and availability of computer data systems such as illegal access to a computer system;[67]computer related offences including computer related forgery[68]. In these offences, a computer is necessary for the unlawful action to be undertaken. In a bid to balance the freedom of expression with competing rights, the Convention criminalizes content related offences. Criminalization of content offences has generated a lot of debate by activists who opine that such laws might be used by authoritarian governments to curtail freedom of expression. The Convention also criminalizes offences related to child pornography[69]. This is in tandem with the Convention on the Rights of the Child that mandates all states to take measures to ensure the best interest of the child is upheld at all material times. This is specially envisioned as a means of

[64]McGuire and Dowling, 2013, p. 4; Europol, 2018, p. 15
[65] The Council of Europe Convention on Cybercrime (Budapest Convention)
[66] The African Union Convention on Cybercrime and Personal Data Protection (Malabo Convention)
[67] Article 2 to 6
[68] Article 7
[69] Article 9

protection children from sexually explicit content. A major win for the Convention is the classification of intellectual property rights as cybercrime.[70]

While maintaining the tempo set by the Budapest Convention, the Malabo Convention classifies cybercrime into four categories. However, contrary to the Budapest Convention, it does not consider intellectual property infringement as cybercrime, instead, it introduces another category of cybercrime to wit, offences relating to electronic message security measures.[71]

Part III of the Computer Misuse and Cybercrimes Act, No. 5 of 2018 outlines cybercrimes recognized in Kenya. Though the Act does not classify the offences as in the Budapest and Malabo conventions, it incorporates the offences envisioned in both conventions for example unauthorized access[72], access with intent to commit further offence[73], unauthorized interference[74], unauthorized interception[75], cyber espionage[76]cyber terrorism[77] among many others.

The widespread adoption and usage of computers and internet has increased the opportunities available for criminals to commit cybercrimes. The borderless nature of cybercrime creates a challenge with law enforcement to effectively respond to cybercrime. This is exacerbated by the limitations of variations of legal frameworks across the globe. Hence, a multistakeholder collaboration is necessary in combating cybercrime for effective information sharing and cooperation on areas of mutual interest.

2.2.2. Cybercrime Trends

Cybercrime continues to grow in both market and fervency. This has been exacerbated by technological advancements that have seen cybercriminals prove themselves to be skilled and relentless. Hiding behind anonymity, cybercrime escalates as new levels of ransomware attacks remain as powerful reminder that stakeholders must work together to combat cybercrime. Cybercriminals continuously evolve and increase their sophistication, employing methods that make them harder to detect and threatening even the most alert targets. They have no respect for

[70] Article 10
[71] Article 29 (4)
[72] Section 14
[73] Section 15
[74] Section 16
[75] Section 17
[76] Section 21
[77] Section 33

international borders and tend to hide in jurisdictions that do not have the legal frameworks that would allow for their prosecution, that lack the capability to track them down, that tacitly support the activities, or that simply have no interest in the cross-border cooperation needed to contain this global threat.[78] Similarly, the trans-border nature of Cybercrime requires international cooperation in holding cybercriminals accountable. While ultimate law enforcement powers are vested on the State, multistakeholder voices and expertise must be included to support States in combating the forms of cybercrime

Technology is in constant flux, hence affecting the manner and form of cybercrime. In fact, law enforcement agencies monitor the trends in cybercrime based on the intensity and impact of the crime. In 2018[79], it was discovered that by infecting a computer system with a malicious code (malware), data within computer systems was made unavailable and inaccessible to legitimate users until a fee was paid to the intruder.[80] With time, the intensity, frequency and impact of such attacks have increased. The victims of these attacks range from individuals, to corporations to governments. Critical infrastructure installations are not exempt from cyber-attacks. Hence the need for law enforcement to develop effective measures to countermand this emerging trend.

Combating cybercrime is a challenging task due to the various technical, social, financial and even ethical issues. Law enforcement agencies contend with the dynamic nature of the cyberspace when attempting to hold cybercriminals accountable. Among the obstacles are technical, legal and operational challenges. Computers that are connected to the internet have capacity to communicate with each other. Though each computer has its own unique Internet Protocol (IP) address, some cybercriminals have managed to hide their IP addresses hence evade detection by law enforcement agencies. Additionally, vulnerabilities in different software make them susceptible to attacks by cybercriminals. As long as the software vulnerability remains unknown, the software affected can neither be patched nor the vulnerability detected by an anti-virus. Such vulnerabilities only get exposed when the software is attacked by cybercriminals. Also, the uptake of cloud computing has

[78]Microsoft's submission on a possible Cybercrime Convention Page 1 available at https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/Statements/Microsoft_position_-_first_session last accessed on 16th August 2023 at 12.12pm

[79]Holt, Thomas, J., Adam M. Bossler, and Kathryn C. Seigfried-Spellar. (2018). *Cybercrime and Digital Forensics*,2nd edition. Routledge.

[80]Available at https://sherloc.unodc.org/cld/en/education/tertiary/cybercrime/module-1/key-issues/cybercrime-trends.html last accessed on 22nd May 2023 at 01.01pm

enhanced the complexity of combating cybercrime as users shift the cybersecurity burden to the cloud service provider. Therefore, when a breach occurs, the user has to partner with the cloud service provider to find a solution, which may lead to further technical and legal challenges.

Since cybercrime is a transnational crime, investigators may need access to information or data stored across borders. This may result in serious legal challenges especially where there is no existing mutual legal assistance framework. International cooperation with other countries requires harmonized laws between cooperating states.

From the foregoing, cybercrime has become the reality of our society. However, there are certain steps that users of technology can take to avoid being victims of cybercrime. Such steps include using up to date software and operating system. Moreover, any software that is no longer in use should be uninstalled to secure the system from unwarranted ransomware. A reputable anti-virus company goes a long way in securing the integrity of a computer system. Overall, there is need to exercise care when entering personal or financial information to a website.

2.3. The Stakeholders Involved in Combating Cybercrime

Advancements in mobile phone technology have resulted in increased global internet penetration rate. A majority of the world's population has access to the internet. In fact, most critical services are increasingly offered online. Hence more opportunity to abuse technology and to commit crime, making citizens vulnerable to cyber-attacks and cybercrime. Law enforcement agencies play a huge role in fighting cybercrime. Technical, legal and operational difficulties are the main issues that law enforcement agencies are able to meet the emerging challenges of cybercrime. Cyber criminals operate under the guise of anonymity and may be far removed from the jurisdiction where the effect of the cybercrime is felt. Moreover, crucial evidence needed by law enforcement agencies is often contained in firms controlled by private entities. Hence the need for a multi stakeholder approach in cybercrime investigation and prosecution.

Cybercrime investigations bring many stakeholders together: private companies, national security agencies, civil society organizations, international organizations and individuals among many others.

2.3.1. Reporting Cybercrime

No investigation can commence unless an incident is observed or reported. The type of cybercrime committed influences an individual's willingness to report to the relevant authorities or not. It is

safe to say that some victims shy away from reporting cybercrime for fear of shame or embarrassment associated with some cybercrimes[81]. In some instances, the victim may fear negative publicity arising from the cybercrime investigation or reprisal from the perpetrator. Notably, there are victims who fail to report solely for lack of awareness that the conduct in question amounts to a crime. Likewise, some shy away from reporting having lost hope in the ability of law enforcement to grant them justice for the loss, damage or pain suffered at the hands of the cybercriminal.[82] Similarly, failure to know where to report has also contributed to victims failing to report on incidents of cybercrime.

Noting the importance of reporting in cybercrime investigation, governments in partnership with other stakeholders have put in place mechanisms to ease reporting of cybercrime Through the use of websites and hot lines, the government has ensured that the citizens have increased avenues where cybercrime can be reported[83].Also, audio and visual commercials supported by government and other stakeholders imploring the members of the public to report any cybercrime to the nearest police station have been put in place. Notably, most agencies in the criminal justice sector[84] are also open to receiving complaints from members of the public on cybercrime. The receiving institution is thus obligated to transmit the information to the relevant agency for investigation.

To assess the effectiveness of these initiatives, it is important that government monitors and evaluates the impact of all these initiatives on the reporting of cybercrime. This would ensure that state resources are invested in initiatives that effectively meets the demands of the citizens.

2.3.2. Cybercrime investigation and Prosecution

Investigation into cybercrime take a dualistic approach. The investigation may be commenced in response to intelligence or pursuant to a report made to the appropriate authorities. In the latter, the person to whom the report is made is best placed to determine the proper entity to investigate the conduct. It is trite that when it comes to cybercrime, the police and law enforcement do not

[81] https://www.unodc.org/e4j/en/cybercrime/module-5/key-issues/reporting-cybercrime.html#:~:text=Existing%20research%20identifies%20several%20reasons,is%20a%20business%2C%20loss%20of

[82] https://www.csoonline.com/article/567307/why-businesses-don-t-report-cybercrimes-to-law-enforcement.html

[83] Websites such as https://nc4.go.ke/Report%20Cybercrime%20Incident/ hosted at the National Computer and Cybercrimes Coordination Committee offer an avenue for reporting cybercrime. Additionally, the Communication Authority of Kenya also allows for reporting of cybercrime incidents through its website https://ke-cirt.go.ke/report-an-incident/.

[84] The National Police Service, the Directorate of Criminal Investigation, the Office of the Director of Public Prosecution, the Commissioner for Administrative Justice among others

have all the answers; hence the need to form strategic partnerships to combat cybercrime. International organizations, private sector, academia, civil society organizations among others can offer such expertise to law enforcement agencies. Through collaborative efforts, expertise that assist with information sharing, digital forensic experts, intelligence analysis, training and capacity building can be obtained on a need basis.

Upon observing or receiving a report on cybercrime, the first crucial step is to secure the digital evidence at the scene. This may be in the form of the target of the cybercrime or the device used to perpetrate the cybercrime. It is proper and prudent that the first responder be a person with adequate knowledge on incidents of cybercrime. This is because digital data is often volatile and may be easily altered or destroyed. Since the first responder may either be a law enforcement officer, a digital forensic expert or an information and communication technology specialist; all the activities undertaken to search, seize or preserve the digital evidence must be done in accordance with the law. The relevant national laws on admissibility and collection of evidence must be adhered to at all material times.

Law enforcement officers, prosecutors and judicial officers are responsible or detecting, investigating, prosecuting and adjudicating cybercrime. Depending on the nature of cybercrime, multiple agencies may be involved to ensure effective and efficient investigations into the matter. In many jurisdictions the Criminal Investigation agency is adequately trained to investigate incidents of cybercrime.[85] In compliance with the right to privacy[86] and data protection laws[87], the investigating officer must obtain a court order from a competent court to search or seize any digital evidence in an investigation. At the end of the investigation, the officer must avail a cybercrime report outlining the outcome of the investigations conducted on the devices.

A cybercrime investigator should thus possess adequate skills in preserving evidence integrity according to standard operating procedures or national standards; and collecting, processing, packaging, transporting, and storing electronic evidence to avoid alteration, loss, physical damage,

[85]For example, in Kenya the Directorate of Criminal Investigation is the key agency mandated to investigate criminal conduct.
[86] Article 31 of the Constitution of Kenya, 2010
[87] Data Protection Act, No. 24 of 2019

or destruction of data.[88] Similarly, prosecutors and judicial officers handling cybercrime cases should be adequately trained on cybercrime, digital forensics, admissibility of digital expert witnesses and evidence among many others.

A significant challenge in the prosecution of cybercrime is that all the elements of the crime are rarely found in the same jurisdiction. In most cases, the offender, the victim or the evidence may be located in different jurisdictions. Consequently, it calls for a high level of cooperation between law enforcement agencies and key stakeholders, to wit international organizations, private sector and academia to effectively investigate and prosecute cybercrime.

2.3.3. International and Regional organizations

There is a large and growing dependency, in modern societies, on information and communication technologies (ICTs). ICTs have become essential to national security, economic well-being and social cohesion for all nations. Consequently, criminal groups have wasted no time in embracing today's globalized economy and the sophisticated technology that goes with it.[89] The internet has created room for the commission of cybercrimes through computer systems. The far-reaching consequences of cybercrime are a concern to humanity scattered across the globe; Cybercrime has no limitation since it is not bound to any known country. Hate crimes, child pornography, fraud, identity theft, data corruption, disruption of network and other similar activities are part of criminal activities in the cyber space.

International organizations such as INTERPOL and regional organizations such as Africa Union Mechanism for Police Cooperation (AFRIPOL) provide avenues for mutual cooperation and collaboration in investigation of transnational crime and criminals.

2.3.3.1. International Criminal Police Organization (INTERPOL)

Cybercrime is predominantly transborder in nature. Consequently, there is need for international cooperation in the investigation, prosecution and adjudication of cybercrime.

INTERPOL is an intergovernmental organization with one hundred- and ninety-five-member (195) states based in Lyon, France. It works with police officers in the member countries to make

[88]US National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework, pg. 79 available at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf last accessed on 25th May 2023 at 1234 hrs.

[89]Koffi Annan, Former UN Secretary General comments on the United Nations Convention on Transnational Organized Crime

the world a safer place. It operates in each of the member states through the National Central Bureaus (NCBs) which provide the central point of contact between the member country and the General Secretariat of INTERPOL.[90] Through its communication system I-24/7, member countries are able to access databases and services in real time, hence enhancing overall police effectiveness in handling transnational cybercrime. [91] INTERPOL promotes international law enforcement cooperation in cybercrime investigation.

INTERPOL'S cybercrime strategy assists member countries to identify cyber-attacks and their perpetrators. Through this strategy, INTERPOL conducts threats assessment, analysis and trend monitoring to detect and positively identify cybercrime.[92] Moreover, it facilitates member countries to access, collect and exploit data linked to cyber-attacks. Upon successful collection of the data, it assists member countries to lawfully manage, process and preserve the digital evidence for purposes of investigation and prosecution.[93] Using their technical expertise, they are able to use the digital evidence to trace the location of the perpetrator.[94] Hence bridging the gap between the cyber space and the geo location. Since such cooperation can only be achieved with enabling legislation, it improves operation interoperability by encouraging legislative harmonization.[95]

INTERPOL has put in place measures to meet its vision of enhancing cooperation among law enforcement. It has put in place a set of policing capabilities to member countries on police data management, criminal analysis, forensic support, fugitive investigative support, a Command and Coordination Centre, capacity building and training, innovation and special projects.[96] With regards to cybercrime, it has specifically created secure and flexible services with a view to facilitating cybercrime related communication among police and other stakeholders. The Cybercrime Knowledge Exchange workspace, which is open to all authorized users, deals with general non-police information.[97] Through this platform, stakeholders are able to discuss the latest

[90]Available at https://www.interpol.int/en/Who-we-are/What-is-INTERPOL last accessed on 25th May 2023 at 0100pm
[91] Ibid
[92] INTERPOL Cyberstrategy 2017 Summary pg 2 available at file:///C:/Users/user/Downloads/Summary_CYBER_Strategy_2017_01_EN%20LR%20(2).pdflast accessed on 27th May 2023 at 0120hrs
[93] Ibid
[94] Ibid
[95] Ibid
[96] Ibid
[97] Available at https://www.interpol.int/en/Crimes/Cybercrime/Cybercrime-Collaboration-Services last accessed on 25th May 2023

trends, prevention strategies, detection equipment and investigation techniques with authorized colleagues globally.[98] On the other hand, the Cybercrime Collaborative Platform has been set up to support law enforcement operations with access restricted to operational stakeholders only. [99] Thus, stakeholders are able to share intelligence in an interactive and secure environment.

Moreover, the dynamic nature of cybercrime has caused INTERPOL to run regular awareness campaigns[100] to not only highlight major forms of cybercrime but also provide tips on how to stay safe.[101] The #YouMayBeNext campaign focusses on sextortion, ransomware and Distributed Denial of Service (DDoS) attacks. It offers practical assistance to individuals and businesses on how to safeguard their networks, products and services.[102]

Policing cooperation through INTERPOL has enabled law enforcement to successfully investigate and intercept cybercriminals. Kenya has benefited heavily from INTERPOL services in investigation of several transnational crimes. Through the National Central Bureaus (NCB), Kenya has obtained technical assistance to investigate crime or criminals in other countries including sharing of criminal data and intelligence. In 2019, Kenya successfully utilized INTERPOL's International Child Sexual Exploitation (ICSE)[103] database to track and arrest perpetrators of child online exploitation. In the process, victims were rescued and reunited with their families.[104] Such cooperation can be employed to ensure effective investigation and prosecution of cybercriminals.

As a key stakeholder in transnational criminal investigations, INTERPOL, provides a platform upon which cross border cooperation on investigation of cybercrime, arrests and operations are undertaken.

2.3.3.2. African Union Mechanism for Police Cooperation (AFRIPOL)

AFRIPOL is a technical institution of the African Union mandated to strengthen cooperation among police agencies of AU member states. To achieve this, it cooperates with numerous

[98] Ibid
[99] Ibid
[100] #JustOneClick which focused on the impact of a simple click in protecting computer networks; #OnlineCrimeIsRealCrime which underscored the seriousness of online crime; #WashYourCyberHands during the Covid 19 Pandemic; and #BeCareful which highlighted prevention tips on Business Email Compromise fraud
[101] Available at https://www.interpol.int/en/Crimes/Cybercrime/Awareness-campaigns last accessed on 25th May 2023 at 01.27 pm
[102] Ibid
[103] The ICSE is a victim identification tool that helps investigators to analyze and compare child sexual abuse images.
[104] https://www.interpol.int/en/News-and-Events/News/2019/Kenya-first-African-country-to-connect-to-the-International-Child-Sexual-Exploitation-database last accessed on 13th July 2023 at 1230 hrs

international police organizations such as INTERPOL, through the INTERPOL Support Program for the African Union (ISPA).[105]

In a bid to combat Cybercrime, AFRIPOL is focusing on three limbs which involve training with non-proprietary and license free technologies.[106] Additionally, it has established a fund for combating cybercrime with contributions from all partners interested in the field.[107] Finally, it seeks to strengthen collaboration with the private sector to harmonize and standardize procedures and technologies and for intelligence gathering.[108]

From its inception, it has promoted effective operations and investigations, criminal analysis and exchange of information and best practices among member countries.[109]

2.3.4. Private Sector

Private sector plays an essential role in the detection, prevention, mitigation and investigation of cybercrime. It has the requisite human, financial and technical resource to effectively conduct cybercrime investigation.[110]

Just like law enforcement, private companies and corporations conduct investigations in response to detected or reported crime. It assists law enforcement to expeditiously preserve and collect crucial digital evidence. Furthermore, the sector provides expert testimony to give law enforcement an understanding of the technical aspects of the cybercrime. The private sector is critical in providing tools for attribution hence enabling law enforcement trace the physical location and identity of cybercriminals.[111]

In spite of the crucial role played by the private sector, there is little consensus on the legal framework for effective and trust-based cooperation between private sector and law enforcement agencies. Accordingly, privacy and data protection regulations breed reluctance by private sector cooperation with law enforcement. Effectively creating the need to standardize rules of

---

[105]Available at https://afripol.africa-union.org/ last accessed on 14th September 2023 at 1457 hrs
[106] Ibid
[107] AFRIPOL Cybercrime strategy available at https://rm.coe.int/afripol-strategy-on-cybercrime-v01-en/1680a30050#:~:text=AFRIPOL's%20Cybercrime%20Strategy%20presents%20the,during%20the%20period%202020%2D2024. Last accessed on 14th September 2023 at 1503 hrs
[108] Ibid
[109]https://afripol.africa-union.org/joint-afripol-interpol-press-release/ last accessed on 14th September 2023 at 1506 hrs
[110]Europol and Eurojust, *Common Challenges in Combating Cybercrime*, 2019 Joint Report p. 17
[111]Ibid p.12

engagement between private sector and law enforcement by outlining the legally allowed parameters of engagement in countering cybercrime.

2.3.4.1. Internet Service Providers (ISPs)

ISPs play significant roles in Cybercrime investigation and prosecution It is through ISP's that citizens are able to access all the wealth of information available online.[112]The ISPs can rightly be called the middlemen of the cyberspace as they are the pipeline through which online communications flow. Increasingly, more ISPs are in a position to observe and record everything that we say and do online. Thus, they are charged with the arduous task of not only safeguarding our personal communication and private information, but also ensuring that our personal information does not fall into the hands of third parties.

The online space provides an opportunity for users to share information under the guise of anonymity. However, with advancement in technology, there is increasing commercial interest on the activities of users online. Consequently, certain companies have set up cookies and other surveillance technologies that give information on the activities of customers online. Criminal enterprises have also leveraged on these to engage in cybercrime. As a result, there is a move by governments to develop legislations that would mandate ISPs to collaborate with law enforcement by granting them access to telecommunications transmitted over their facilities. [113]

Two competing interests emerge in assessing the role of ISPs as intermediaries. In the first instance, ISPs are entrusted as stewards and custodians of crucial personal information and communication of its customers. On the other hand, they have access to crucial information that might assist law enforcement agencies. This calls for a delicate balance between the right to privacy and the right to personal security. Consequently, ISPs are generally seen as a reservoir of personal information and communication that the state can tap into on a need basis purposes of law enforcement. for example, towards this end the Constitution of Kenya[114] and the Data

[112]https://www.verizon.com/about/blog/isp meaning#:~:text=An%20internet%20service%20provider%20(ISP)%20is%20a%20company%20that%20provides,mobile%20carriers%2C%20and%20telephone%20companies.last accessed on 13th July 2023 at 1239 hrs

[113] Mendina, Johannes Britz, *Information Ethics in the Electronic age: Current issues in Africa and the world*, 2004 pg. 164 Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=907483 last accessed on 13th July 2023 at 1317 hrs

[114] Article 31 and Article 24

Protection Act, 2019[115] in guaranteeing the right to privacy not only outline various instances when the said right can be limited but also the manner in which it can be limited.

ISPs are often faced with the dilemma of how to comply with a request from law enforcement while protecting the rights of their customers. In most countries, access to personal or private information in the hand of ISPs requires prior judicial preauthorization through a search warrant. With that, investigators are able to access customer name, address, local service provider identification, traffic data and content data. Hence, cybercriminals who have hitherto operated under the guise of anonymity can be uncovered through lawful cooperation between law enforcement and the ISPs. In granting search and seizure warrants, the judiciary plays a key role in the preservation, production and interception of crucial evidence needed in cybercrime investigation and prosecution.

The Council of Europe convention on Cybercrime specifically calls for cooperation between state and private industry in combating cybercrime and the need to protect legitimate interests in the use and development of information technologies.[116]

The shifting architecture of our communications infrastructure must incorporate various safeguards that will not only further the goals of national security and law enforcement, but will also preserve and promote personal privacy.[117]

2.3.5. Academia

Academia is seized with the role of promoting research and education in areas of mutual concern. Academia ensures that all students and academicians are certified for digital literacy. Since digital literacy is a prerequisite in combating cybercrime, academic institutions are handy in knowledge sharing, policy and legislation development for purposes of developing technical standards. If properly structured, academic institutions are crucial to establish specialized educational programs, training centres and curricula to consolidate research and knowledge.[118]

---

[115] Part IV

[116] Paragraph 7 of the Preamble

[117] https://www.researchgate.net/publication/228188863_The_Role_of_ISPs_in_the_Investigation_of_Cybercrime Last accessed on 13th July 2023 at 1304hrs

[118] MUTIJIMA Asher Emmanuel, *The Role of Academia in Cyber Crimes Prevention,* International Journal of Innovative Science and Research Technology ISSN No:-2456-2165

The African Union Convention on Cybersecurity and Personal Data Protection obligates each State Party to adopt measures to develop capacity building with a view to offering training on all areas of cybersecurity to different stakeholders, and setting standards for the private sector. Further, State Parties are to promote technical education for information and communication technology professionals, within and outside government bodies, through certification and standardization of training; categorization of professional qualifications as well as development and needs-based distribution of educational material.[119]

As centres of academic excellence, universities offer degree, diploma and certificate courses on cybersecurity and cybercrime, hence creating awareness on digital literacy. This approach has seen an increase in journals and academic papers on cybercrime and cybersecurity. Arguably, it is through the institutions of learning that crucial information on cybercrime is imparted to students and new strategies of fighting crime incubated.

2.3.6. Civil Society

Civil society is a valuable partner in the anti-cybercrime fight, they assist is setting the right balance between state's intervention for security and private sector agenda for profit. The issue of fighting cybercrime raises several major challenges for human rights protection.[120] Civil society is at the forefront to ensure that the fight against cybercrime is not used to undermine human rights and freedoms. The civil society movement is known for ensuring accountability and protecting human rights. This is done not only through capacity building but also through activism, legislative and policy proposals. In Kenya, civil society organizations have been key in ensuring that cybercrime legislation is in tandem with the Constitution.[121]

2.4. Conclusion

Cybercrime is exceedingly complex and multifaceted. Cybercriminals boast of anonymity as attribution is often difficult. Moreover, time lapses may result in challenging the admissibility electronic evidence. Hence, investigation of cybercrime requires expediency in identification, collection, preservation and analysis of digital evidence. The internet revolution has created the need for nations to develop new strategies in fighting cybercrime. Arguably, the cyberspace relies

[119] Article 26 (4)
[120]Ibid
[121]Article 19participated as an Interested Party in the case of *Geofrey Andare versus Attorney General & 2 others* [2016] eKLR where the Petitioner had challenged the constitutionality of section 29 of the Kenya Information and Communication Act for limiting the freedom of expression.

on many stakeholders for its services, innovation and development and growth. It is therefore important to develop cybercrime policies in an inclusive way. States should ensure that the development and implementation of cyber-related policies are open, inclusive and transparent.[122] The stability and security of cyberspace both affects and relies on a wide range of stakeholders, and as such requires their meaningful engagement to be effective and sustainable.[123] Multistakeholder approach is useful in combating cybercrime as it provides practical cooperation between law enforcement, the private sector, academia and the civil society.

[122]In its submissions to the GCSC'S Consultation on the draft Singapore norm package, the Global Partners Digital on the norm against offensive cyber operations by non- state actors.
[123]Available at https://www.gp-digital.org/multistakeholderism-the-missing-cyber-norm/ last accessed on 15th March 2023 at 01.18 pm

CHAPTER THREE: BEST PRACTICES FOR MULTISTAKEHOLDERISM IN COMBATING CYBERCRIME

3.1. Introduction

Although multistakeholderism is fronted as the best governance model for the internet, nation states are still unwilling to fully engage stakeholders in dealing with sensitive issues of cybersecurity and cybercrime. The delicate nature of cybercrime has led many states to treat it as a security issue warranting security intervention. Another reason for this could be the interest of the state in safeguarding its jurisdictional sovereignty from interference by third parties. Geopolitical tensions and national security threats are key concerns in countering cybercrime. It is possible that commitment from a range of stakeholders can adequately aid in implementing global cybercrime measures.

Many nations have achieved this through legislative initiatives at both the national, regional and international level. The fact that technology keeps advancing means that these legislations have to adapt to the evolvements in information and technology. A robust judicial system enables these states to effectively achieve stakeholder engagement in fighting cybercrime by ensuring that laws are interpreted in a manner that conforms to the trends in information and technology. An effective mutual legal assistance framework is key towards ensuring cooperation and collaboration in fighting trans-border cybercrime. Deliberate domestic legislation coupled with formal and informal partnerships ensure effective investigation and prosecution of cybercrime.

The Global Cybersecurity Agenda under the stewardship of the International Telecommunication Union identifies five key pillars of an effective cybersecurity and cybercrime mechanism. These pillars are the foundation of multistakeholderism in combating cybercrime. Remarkably, international and regional instruments on cybercrime have incorporated these principles as crucial areas of focus in countering offences against computer systems. Similarly, national jurisdictions have also embraced these mechanisms in their national cybersecurity and cybercrime plans for action. The five key pillars that underpin multistakeholderism in combating cybercrime include: Legal Measures; Technical and Procedural Measures; Organizational Structures; Capacity building and International cooperation.

This chapter will focus on the international and national best practice in combating cybercrime in the context of the five key principles in countering cybercrime through multistakeholderism. The

study will highlight the best practice models for combating cybercrime as espoused in international and regional instruments as practiced by Singapore and Ghana. The main purpose of this approach is to provide a basis for critiquing the Kenyan scenario and identifying the gaps that may require both legislative and policy interventions.

Singapore's commitment towards running a smart economy makes it heavily susceptible to cybercrime; as a number of government service and commerce is conducted in the cyberspace. Additionally, Singapore is the Association of South East Asian Nations (ASEAN) voluntary lead shepherd on cybercrime, responsible for charting ASEAN's initiatives against cybercrime. Similarly, Ghana, being the first African country to gain independence offers opportunities for wonderful lessons and insights on countering cybercrime. Especially, following the successful implementation of its 2015 Cybersecurity Strategy. Through the strategy, Ghana has successfully put in place a legislative and policy framework for countering cybercrime, including signing and ratifying both the Budapest Convention and the Malabo Convention on Cybersecurity and Personal Data Protection. Moreover, in 2019 the Economic Community for West African States (ECOWAS) requested Ghana to champion the fight against cybersecurity and cybercrime in the region.[124] Studying the mechanisms that both Ghana and Singapore have put in place to address cybercrime would be useful to Kenya; especially because Kenya is not only a member of the Commonwealth but also styles itself as a digital economy.

3.2. Global Instruments towards Combating Cybercrime

It is now recognized globally that cybercrime has grown in both sophistry and magnitude. Cybercrime transcends existing national borders as cybercriminals in one jurisdiction can engage in an act that negatively impacts another jurisdiction. Accordingly, nations desirous of effectively countering cybercrime can no longer afford to work in silos. Instead, there is need for collaboration on areas of mutual interest. Especially on investigation and prosecution of cybercrime.

Though widely acclaimed as the crime of this age, there is no globally binding Convention or Treaty on cybercrime. Notwithstanding, the Council of Europe and the African Union have developed Conventions that address cybercrime. Similarly, the United Nations, having recognized the need for a global instrument on cybercrime, has developed the draft UN Convention on

[124] Available at https://police.gov.gh/en/index.php/cyber-crime/ last accessed on 01.12.2023 at 0014 hrs. The Ghana Police force has established a Cybercrime Unit that engages in Cyber investigations, cyber intelligence and child protection digital forensics laboratory

countering the use of ICT for criminal purposes. Since cybercrime might also be committed by organized criminal groups, some States have found the UN Convention against Transnational Organized Crime useful in dealing with trans-border organized cybercrime.

3.2.1. United Nations Convention against Transnational Organized Crime

The former UN Secretary General Koffi Annan in making remarks on the UNTOC decried the manner in which criminal groups have enhanced their sophistry as a result of advancements of technology.[125] The Convention was adopted in 2000 with the view to exploit the openness and opportunities of globalization to uphold human rights and counter the forces of transnational crime.

Though the convention does not expressly list cybercrime as an offence, it recognizes the transnational element of offences committed through the use of computers, telecommunications networks or other forms of modern technology. It mandates state parties to undertake capacity building on effective strategies for countering transnational organized cybercrime.[126]Towards this end, it requires state parties to collaborate and cooperate on areas of mutual interest with a view to countering transnational organized cybercrime.[127]

In recognition of the effectiveness of stakeholders in combating transnational crime, the Convention obligates member states to facilitate effective coordination among relevant agencies. This is to facilitate effective information sharing through exchange of personnel and experts. By entering into bilateral agreements, state parties can assign liaison officers to different jurisdictions as required by the concerned State Parties.[128]

It is instructive that the Convention identifies sharing of strategies on countering transnational organized cybercrime as a key area for collaboration and cooperation. Such cooperation can strengthen existing frameworks by nation states for combating cybercrime.[129]Accordingly, formal and formal cooperation among stakeholders forms an effective strategy against cybercrime. As a result, law enforcement might be better placed to not only investigate cybercrime, but also detect and prevent it.[130]

---

[125] Koffi Annan, Former UN Secretary General comments on the United Nations Convention on Transnational Organized Crime.
[126]Article 29, United Nations Convention on Transnational Organized Crime
[127]Article 27 (3)
[128] Article 27 (1) (d)
[129]Article 27 (1) (e)
[130] Article 27 (1) (f)

The Convention obligates State parties to develop mechanisms for direct cooperation with law enforcement. In fact, in the absence of any other arrangement for cooperation, it forms the basis for direct cooperation among member states. Essentially, it implores member states to promote its implementation through economic and technical assistance, including persuading states and financial institutions to participate in countering transnational organized cybercrime.[131]Accordingly demonstrating the effectiveness of involving the private sector in combating cybercrime. It is noteworthy that this approach is key in combating cybercrime as financial institutions are not only targets of cyber-attack but also have the financial muscle and technical expertise to invest in combating cybercrime.

In the spirit of collaboration and cooperation, it mandates member states to vail mutual legal assistance to each other in investigations, prosecutions and adjudication of transnational organized cybercrime.[132] However, it is noteworthy that obligations under a bilateral agreement or treaty that provides for mutual legal assistance are guided by the Convention on mutual legal assistance.[133]

Though the convention is specific to organized crime, it offers a mechanism upon which organized cybercrime syndicates can be effectively investigated and prosecuted within the realm of international cooperation. Moreover, it underscores the shared responsibility of states and stakeholders in combating crimes committed using modern technology. Accordingly, it points out strategies such as knowledge sharing, exchange of experts and personnel and mutual legal assistance in investigation, prosecution and adjudication of transnational organized cybercrime.

3.2.2. Draft United Nations Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes[134]

This Convention is the first attempt by the United Nations to develop an instrument on cybercrime. Though still at the draft stages, it deals with substantive cybercrime provisions. It also addresses key issues in cybercrime investigation such as cooperation and mutual legal assistance in accessing

[131] Article 30 (2) (d)
[132] Article 18 (1)
[133] Article 18 (6)
[134]In December 2019 the UN General Assembly passed Resolution 74/247 and established the *Adhoc* intergovernmental committee to prepare a comprehensive convention on use of ICT for criminal purposes.

digital evidence.[135] As a UN document, it also addresses the human rights and procedural safeguards that emanate from the cyberspace.

The main purpose of the Convention is to enhance mechanisms for preventing and countering other unlawful acts in the field of ICT. Towards this end, it curtails cybercrime by creating offences that relate to misuse of ICT for criminal purposes. It empowers law enforcement agencies to effectively investigate cybercrime by providing mechanisms for international cooperation. Especially as regards capacity building and provision of technical assistance towards countering cybercrime.[136]

In this regard, the Convention recognizes the crucial role that stakeholders in academia, private sector and civil society play in capacity building and training on ICT based crimes. The Preamble to the draft Convention specifically recognizes the need for states to involve stakeholders including public-private partnership, business, individuals and groups from outside the public sector, such as civil society, as an effective strategy towards combating ICT crimes.

The draft convention criminalizes myriad criminal acts believed to fall within the scope of cybercrime.[137]Consequently, it mandates state parties to enact domestic legislations that recognize such offences. Furthermore, it calls upon state parties to enact legislations to establish such offences under their domestic laws. While recognizing of the crucial role of the private sector in countering cybercrime, it enunciates principles and code of conduct that private providers of ICT services are required to abide by.[138] Accordingly laying the basis for stakeholder engagement in combating cybercrime. Facilitating cooperation among ICT service providers and creating room for collaboration in developing standards for netizens is a good starting point.[139]While recognizing capacity building as a key component in combating cybercrime, the convention obligates states to intentionally take steps to raise public awareness on cybercrime prevention.[140]

---

[135] Available at https://www.eff.org/issues/un-cybercrime-treaty#:~:text=The%20proposed%20Convention%20will%20likely,human%20rights%20and%20procedural%20safeguards. Last accessed on 5th April 2023 at 3.13pm EAT

[136]Article 1 of the draft UN convention on Countering the Use of Information and Communication of Technologies for criminal purposes

[137] Section 1 of the draft Convention

[138] Article 43

[139] Article 43 (2) (b)

[140] Article 44

Further to this, state parties ought to take appropriate measures to enhance involvement of both public and international organizations in prevention of cybercrime. Including raising awareness on the nature of cybercrime and the threats that cybercrime poses to individual rights and freedoms. The Convention specifically mandates the United Nations Office on Drugs and Crime (UNODC) to provide specialized technical assistance to State parties. Through this support, state parties will be adequately equipped to implement and undertake programs and projects towards countering cybercrime.[141] Furthermore, the private sector is singled out as a key stakeholder in technical assistance and capacity building towards countering cybercrime.[142].

The proposed Convention, if approved, would be the first binding international instrument on cybercrime. Its focus on stakeholder engagement through international cooperation, mutual legal assistance, technical assistance and measures of prevention, including training, is crucial in combating cybercrime. Though crime eradication is primarily a mandate of the state, this draft convention demonstrates that countering cybercrime requires a multistakeholder approach and thus state parties should adopt domestic laws and policies that enhance effective stakeholder engagement in fighting cybercrime.

3.2.3. The Council of Europe Convention on Cybercrime (the Budapest Convention)

This is the first convention on cybercrime of a global nature. Though it was developed by the Council of Europe, it was opened for ratification by states both within[143]and out of the Council of Europe.[144]It not only criminalizes cybercrime but also provides procedural law tools for investigation of cybercrime, including securing of evidence. It has been commended as the most consequential treaty on cybercrime. In fact, most domestic legislations on cybercrime are modelled as the Convention. It is instructive that it recognizes the crucial role played by INTERPOL in facilitating international cooperation in the investigation of transnational crimes, especially cybercrime.[145]

By calling on state parties to embrace cooperation and collaboration, the Convention underscores key tenets of multistakeholderism in combating cybercrime. This is adequately balanced with state sovereignty to protect the legitimate interests of its citizens in the use and development of

[141] Article 75 (4)
[142] Article 75
[143] Article 36
[144] Article 37
[145] Article 27 (9) (b)

ICTs.[146]It recognizes the import of balancing the competing interests of law enforcement and human rights in the cyberspace.[147]Though the Convention criminalizes content offences, it still enjoins state parties to protect fundamental rights and freedoms including the freedom of expression, protected by the International Covenant on Civil and Political Rights.[148]The rights to privacy are significantly protected by the Convention. In a similar fashion, state parties are obligated to uphold such rights, especially in light of automatic processing of personal data.

The Convention supplements existing legal framework on investigation, prosecution and adjudication of cybercrime. Therefore, State parties have the freedom to model their domestic laws in a manner that addresses their unique challenges. This may include forming of associations that facilitate cooperation in emergency cases that were not factored in the Convention.[149]State parties to the Convention benefit from capacity building and technical assistance opportunities from both private industry and other stakeholders.[150]The capacity building programs facilitate multistakeholder cooperation and synergies. The Convention makes provision for guidance notes and additional protocols that empowers it to adjust to changes in technological advancements.

Kenya is yet to ratify the Budapest Convention despite its numerous benefits. As a result, Kenya is missing out on capacity building programs and platforms for stakeholder engagement. There is need to ratify the Convention to enhance stakeholder engagement in combating cybercrime by cooperating in areas of mutual interest.

3.3. Regional Instruments

3.3.1. African Convention on Cybersecurity and Personal Data Protection (The Malabo Convention)

The Malabo convention was developed in response to cybercrime that has become a growing concern to African states. The Convention not only identifies cybercrime but also provides a framework for mutual cooperation and collaboration. In regulating electronic transactions, data protection, cybersecurity and e governance, it recognizes that they are susceptible to cybercrime.[151]

[146] Preamble to the Budapest Convention
[147] Ibid
[148] International Covenant on Civil and Political Rights, 1966
[149] Available at https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac last accessed on 16th August 2023 at 1130hrs
[150] Ibid
[151]Available at https://ccdcoe.org/organisations/au/ on 11th April 2023 at 10.00am

In spite of the rapid rise of cybercrime, the uptake of the Convention among African is dismal. Only sixteen (16) of the fifty-five (55) AU member states are parties to the Convention.[152]On the other hand, only thirteen (13) member states have adopted it.[153] Notable African countries such as South Africa, Nigeria and Kenya have been reluctant to ratify the Convention.

It offers member states a platform for collaboration with member states of the Budapest Convention on capacity building, technical assistance and international cooperation.[154]The two regional bodies essentially have an international cyber cooperation with a view to developing a coherent approach on cybercrime and related criminal justice issues in Africa.

Accordingly, State parties are obligated to adopt effective legislative and regulatory measures to combat cybercrime.[155] It further requires state parties to create institutions and confer them with statutory authority and legal capacity to respond to cybersecurity issues including cybercrime.[156]A commendable step is the emphasis on cooperation on forensic investigation and prosecution, not forgetting restorative justice.

It envisions collaboration of stakeholders in developing national cybersecurity policies that outlines the importance of Critical Information Infrastructure.[157]Stakeholders are also called upon to embrace suitable strategies towards implementing a cybersecurity strategy.[158] Some of the key stakeholders identified by the Convention include governments, civil society organizations and enterprises which develop, own, manage, operationalize and use information systems and networks.[159]

Again, member states are enjoined to promote international cooperation. This may be achieved by harmonizing legislation on double criminality to facilitate extradition of cybercriminals.[160]The

[152]As at 14th February 2023
[153]Available at https://au.int/sites/default/files/treaties/29560-sl-African_Union_Convention_On_Cyber_Security_And_Personal_Data_Protection_0.pdf last accessed on 11th April 2023
[154]In April 2018, a workshop on cybersecurity and cybercrimes policies was organized to raise awareness on cybersecurity matters and the importance of political, legislative and diplomatic efforts, cooperation and commitment necessary in tackling inherent cross border cybercrimehttps://au.int/en/pressreleases/20180412/african-union-commission-and-council-europe-join-forces-cybersecurity
[155] Article 25 (1)
[156] Article 25 (2)
[157] Article 24 (1)
[158] Article 24 (2)
[159] Article 26(1)
[160] Article 28 (1)

signing of bilateral agreements of mutual legal assistance between state parties promote exchange of information and efficient data sharing bilaterally.[161] In recognizing the crucial role played by a robust institutional framework, the Convention mandates member states to establish institutions that promote exchange of information on cyber threats and vulnerabilities.[162]

Summarily, it calls on state parties to leverage on formal and informal cooperation towards countering cybercrime. It is instructive that stakeholder engagement is at the heart of an effective strategy for countering cybercrime.[163]

3.4. Multistakeholder initiatives for combating Cybercrime in Singapore and Ghana

The effective implementation of the international standards in combating cybercrime is dependent on several factors including socio economic and political readiness to adhere to international standards. In fact, there is no tangible mechanism for measuring a state's progress in adhering to these standards. However, certain countries have put in place amiable mechanisms for stakeholder engagement in combating cybercrime in line with the ITU principles.

3.4.1. Singapore[164]

In Singapore, Cybercrime includes both offences where the computer system is the target of the criminal act and offences where traditional crimes are committed using computer systems.

Rapid growth of internet use in Asia has been witnessed over the years leading to an increase in cybercrime. The emergence of monetization of malware by criminal networks have amplified the risks of cybercrime. As a result, several Asian Countries, including Singapore, have put in place mechanisms to address these problems.

---

[161] Article 28 (2)
[162] Article 26 (3)
[163] Article 26 (4)
[164]Cybercrime accounted for 48 % of the crimes committed in Singapore. Fifty-five thousand cases of phishing were detected in 2021, being an increase from the forty-seven thousand cases detected in 2020. The Social networking sector was the most commonly spoofed sector, with the financial and online cloud service sectors following closely. Three thousand seven hundred and thirty-one offences under the Computer Misuse Act were recorded in 2021. This was an increase from one thousand seven hundred and one cases recorded in 2019. Online cheating cases increased significantly to a record eighteen thousand and sixty-eight in 2021from seven thousand four hundred and ninety in 2019. Four hundred and twenty cases of cyber extortion were recorded in 2021. Summarily, the Singapore Computer Emergency Response Team handled a total of seven thousand, three hundred and forty-two cases in 2021.

This is influenced by the Government's heavy investment in digital technologies has made several corporations to set shop in Singapore.[165]Consequently, making it a centre for technological development and creativity and by extension, a target for cybercrime.[166]The cybercrime menace in Singapore has been fueled by well-resourced scam syndicates that make use of technology to commit scams across national boundaries and to cover their tracks.[167]

As developments in technology increase, Singapore's vulnerability to cyber-attacks increases in scale and sophistication.[168] As a result, the Cyber Security Agency of Singapore undertakes a robust stakeholder engagement with sector leads to ensure that Critical information infrastructure owners are empowered to detect, respond and recover from cyber threats and cyber-attacks. This mutual sharing amongst stakeholders develops herd alertness, saves time, reduces duplicate efforts, and allows an organization's identification of threats to become another's prevention. Singapore has a robust legal, policy and institutional framework for addressing cybersecurity and cybercrime.

Singapore has a holistic approach towards combating cybercrime, the government is committed to countering cybercrime through effectively deterring, detecting and disrupting cybercriminal activities. As a result, the Singaporean cybercrime strategy is hinged on prevention. Consequently, the government has put in place mechanisms to facilitate agile responses to the challenges posed by technological advancements. Accordingly, effective laws have been enacted to enhance law enforcement efforts in countering cybercrime. While recognizing that countering cybercrime is a shared responsibility, the government has embraced robust stakeholder engagement with the public and industry. Avenues of international cooperation have also been explored towards countering transnational cybercrime.

---

[165]Research suggests that 96.9% of Singaporeans have access to the internet. Available at https://www.meltwater.com/en/blog/social-media-statistics-singapore last accessed on 30th June 2023 at 1507 hrs

[166] Ibid

[167]In 2021, victims of scams in Singapore lost at least S$633.3 million. This was an increase by 52.9 per cent from the year before and making up more than half of all crimes https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/Singapore_statement.pdf

[168]. In February 2017, MINDEF's – net system in Singapore was breached where the personal data of eight hundred and fifty national servicemen were leaked. Moreover, in May 2017, Advanced Persistent Threat (APT) actors targeted two top universities in Singapore. Available at Cybersecurity Act (csa.gov.sg) last accessed on 13th April 2023 at 3.22pm

3.4.1.1. Legal Measures

Legislation on cybercrime has often proved to be a challenge due to the ever-changing face of cybercrime. Singapore has surmounted this legislative challenge by constantly updating and amending their policy and legislative framework to reflect the current cyber landscape. Towards this end, three main pieces of legislation have been developed to effectively counter cybercrime: the Computer Misuse Act, the Cybersecurity Act and the Personal Data Protection Act.

The Constitution of Singapore offers human rights safeguards that protect the integrity of any cybercrime investigation. As a result, law enforcement agencies are required to obtain judicial preauthorization prior to conducting any search or seizure in cybercrime investigations. Such safeguards are necessary to prevent the abuse of human rights under the guise of countering cybercrime.

Notwithstanding, amendments to substantive laws on cybercrime, Singapore has equally updated procedural laws to facilitate cybercrime investigations and prosecution. The Evidence Act and the Criminal Procedure Code have been updated to do away with the outdated and cumbersome requirements for admitting evidence from computer output.[169] Similarly, amendments to the Criminal Procedure Code have empowered the police to require production of evidence in machine readable formats consequently easing evidence analysis.

3.4.1.1.1. Singapore Cybersecurity Act, 2018[170]

The Singapore Cybersecurity Act is the main legal framework for monitoring and maintenance of cybersecurity in Singapore. Other than strengthening the protection of Critical Information Infrastructure (CII) against cyber-attacks, the Act authorizes the Cybersecurity Agency to prevent and respond top cybersecurity incidents and threats. Furthermore, it establishes a framework for information sharing on cybersecurity and cybercrime, including providing a licensing framework for cybersecurity service providers.

The Act establishes an independent Commissioner of cybersecurity[171] who is empowered to not only detect, but also investigate and prevent cybersecurity incidents. Accordingly, it creates a framework for information sharing between government and the private sector that facilitates

[169] Available at https://www.agc.gov.sg/docs/default-source/newsroom-doucments/Speeches/ag's-speech-for-11th-capgc.pdf last accessed on 23.11.2023 at 1304 hrs
[170] Assented into law on 2nd March 2018.
[171] Part 2

prompt identification of vulnerabilities hence preventing cyber incidents. The authority to issue licenses to cybersecurity service providers is vested on the commissioner. Therefore, anyone who violates the terms of the license is held accountable, whether a legal or natural person.[172]

Towards this end, the commissioner has established a cybersecurity code of practice for owners of critical information infrastructure. The code sets out minimum standards which include involving stakeholders in the development of a communication plan.[173]Consequently, communication on cybersecurity and cybercrime is coordinated consistently to all stakeholders, especially in a crisis.[174]

A Cyber Incident Response Team is established within the Act and adequately trained to promptly that is adequately trained and equipped to effectively detect, prevent and combat cyber-attacks. Critical Information infrastructure owners are mandated to identify target audiences and stakeholders for each type of cybersecurity incident scenario. Such stakeholders include the Cyber Incident Response Team, Service Providers, Corporate Communications, crisis management team and business management team participate in cybersecurity exercises.[175]

It is commendable that the Act recognizes the crucial role that stakeholders play in combating cybercrime. As a result, there is clarity on the parameters of engagement among stakeholders. Thus, alleviating any sought of confusion, suspicion or distrust among stakeholders. This multistakeholder approach ensures seamless collaboration in countering cybercrime.[176]The communication plan, developed through stakeholder engagement ensures consensus among stakeholders on the manner of responding to cyber incidents.

In establishing the Cyber Security Agency, Singapore provides an independent agency that facilitates cooperation among stakeholders on cybercrime.

[172] Section 36 and 37 of the Act
[173] Section 11 (1) (a) of the Act
[174] Paragraph 13.17 Response to feedback received for proposed revisions to the cybersecurity code of practice, 2nd edition
[175] Section 7.3.4 of the Cybersecurity Code of Practice for CIIOs
[176]In July 2022 responses were received from over forty-three (43) stakeholders drawn from both the public and private sector towards revising the 2nd edition of the Cybersecurity Code of Practice for CIIO's.

3.4.1.1.2. Singapore Computer Misuse Act, 1993[177]

The Act was enacted to secure computer material from unauthorized access or modification.[178] It deals with the substantive and procedural law that guides investigation and prosecution of cybercrime perpetrators.[179]

In embracing universal jurisdiction, it grants jurisdiction on Singaporean courts to adjudicate cybercrime not only where the perpetrators are citizens but also where the unlawful act negatively affects Singaporeans. This recognition amplifies the transnational nature of cybercrime where the perpetrator of the offence might be in a different jurisdiction from where the effect of the crime is felt.[180]The Computer Misuse Act was renamed the Computer Misuse and Cybersecurity Act between 2013 and 2018. However, it reverted to the Computer Misuse Act upon operationalization of the Cybersecurity Act in 2018. The Commissioner of Cybersecurity established under the Cybersecurity Act, cooperates with law enforcement in detecting, preventing and addressing any threats to computer systems, including the offences established under this Act.

3.4.1.1.3. The Singapore Personal Data Protection Act, 2012

The Act was established in 2012 as a data protection law to govern collection, use, processing and disclosure of personal data.[181] It was later amended[182] to strengthen consumer trust on responsible use of personal data. It outlines mechanisms for processing or harvesting personal data for innovation purposes.

Essentially, it recognizes the competing right to privacy and the economic right of organizations to collect, use or disclose personal data for legitimate and reasonable purposes. As a result, organizations collecting personal data are mandated to establish mechanisms for protecting personal data from unauthorized access or such other similar risks.

---

[177]It was revised in 2021 and came into operation on 31st December 2021

[178]Section 2

[179]Part 2 of the Act criminalizes offences such as hacking and Denial of service attacks. Further, it provides for enhanced sentences for offences committed against protected computers.

[180] Section 13 (3) of the Act

[181] Overview of legislation on cybersecurity, personal data and computer misuse, pg 5

[182] in 2020

The Act establishes an independent office of the Personal Data Protection Commissioner mandated to ensure that organizations abide by the provisions of the Act.[183]The Commissioner is authorized to receive reports on data breaches.[184]

3.4.1.1.4. Singapore National Cybersecurity Strategy

Singapore employed a multi-agency effort in 2013 that resulted in a five-year cybersecurity master plan. The formation of the Cyber Security Agency (CSA) was a direct consequence of this master plan. It was established pursuant to the master plan to develop a national strategy for tackling cyber threats.[185] The vision of the strategy was to coordinate public and private sector efforts to protect national systems and critical sectors. Towards this end, the Cyber Security Agency signed bilateral Memoranda of Understanding with key stakeholders. Thus, demonstrating Singapore's commitment to support the regional Computer Emergency Response Team (CERT). These activities ultimately led to the development of the 2016 Singapore Cyber Security Strategy.

In 2021, the government of Singapore launched an updated National Cybersecurity Strategy that responds to new technological exploits and keeps up with the evolving cyber environment. The strategy focused on simplifying cybersecurity to ensure that all relevant stakeholders adequately understood the nature of cybersecurity and the threats ensuing therefrom. It also made provision for strengthening partnerships with industry to adjust to the changes in the cyberspace.[186]

The strategy is anchored on three pillars including developing resilient infrastructure, enhancing international cooperation and building a safer cyberspace.[187] Through stakeholder engagement, Singapore took a more proactive stance towards enhancing its cybersecurity. Consequently, developing international norms and standards on cybersecurity.[188]

In 2021, Singapore developed another Cybersecurity strategy that primarily focused on enhanced relationships with international partners. Also, it places emphasis on the role of the workspace as a key enabler towards a safe and secure cyberspace.[189] It is commendable that Singapore has been

[183] Section 5
[184] Part 6A
[185] Available at https://www.fticonsulting.com/~/media/Files/apac-files/insights/white-papers/singapore-cybersecurity.pdf page 1 last accessed on 15th March 2023
[186] Available at Singapore Updates National Cybersecurity Strategy (aseantechsec.com) last accessed on 13th April 2023 at 2.23pm
[187] Ibid
[188] Ibid
[189] Singapore Cybersecurity Landscape 2021, pg 33

consistent in revising its cybersecurity strategy by making it adaptable to the changes occasioned by advancements in technology.

Singapore is committed to regularly reviewing the legal framework on cybercrime in tandem with the current trends with a view to making it difficult to commit cybercrime. It is necessary that existing legislation be updated and reviewed to continually address the transnational nature of cybercrime as well as the evolving tactics of cybercriminals.

3.4.1.2. Organizational Structures

Singapore has put in place a formidable institutional framework towards countering cybercrime. Enhancing government capacity to counter cybercrime is one of the key priorities contained in Singapore's National Cybercrime Action Plan. Through this, the government intends to leverage on existing institutions to further bolster international cooperation and strengthen legislation within the criminal justice framework towards combating cybercrime.

At the policy level, the Ministry of Home Affairs has been key in driving policies on cybersecurity and cybercrime in Singapore. Similarly, the Cybersecurity Agency of Singapore is tasked to guarantee a safe cyberspace for the people of Singapore. Likewise, the Singapore Police Force has a cyber command that is highly trained and specialized to handle cybercrime. The government has set up a Centre for Cybersecurity studies was established to guarantee continuous capacity building on cybercrime. Arguably, the government of Singapore has set up a robust organizational structure to effectively combat cybercrime.

3.4.1.2.1. Cyber Security Agency

As already mentioned hereinabove, the Cyber Security Agency[190] is mandated to guarantee a safe and secure cyberspace for Singaporeans.[191] The agency has adopted a prevention approach towards countering cybercrime. As a result, the Agency has successfully managed to not only detect but also counter cybercrime.

The Agency has developed a Cyber Safe program as a multistakeholder initiative to help Singapore enterprises raise their cybersecurity posture. Including cybersecurity certification complemented

[190] The Cyber Security Agency of Singapore (CSA) was established in 2015 and mandated to protect Singapore's cyberspace. It is administratively situated in the office of the part of the Prime Minister's Office under the stewardship of the Ministry of Communications and Information

[191] Available at https://www.csa.gov.sg/ last accessed on 01.12.2023 at 0025 hrs

with a mark of cyber hygiene for compliant organizations.[192] Moreover, the Agency undertakes cybersecurity awareness through partnership programs including the Singapore Cyber Safe Partnership program.[193]

The Agency owns and manages the Singapore Common Criteria Scheme, a globally recognized technical standard for IT security evaluation of commercial IT products targeting international markets.[194]

The agencies that deal with cybersecurity and cybercrime, such as the Cyber Security Agency and the Personal Data Protection Commission, provide continuous capacity building to citizens through Cyber Safety activity books.[195] These books provide young readers with useful tips that not only raise awareness but also protects them from cybercrime.

The Agency continually engages key stakeholders such as governments, private sector and civil society organizations to ensure a safe, secure and more resilient cyberspace.[196] Following enhanced capacity building, information sharing and openness, stakeholders have become more aware of their roles in countering cybercrime; especially members of the public.[197]

3.4.1.2.2. Cyber Emergency Response Team (CERT)

The Team is established within the Cybersecurity Agency to facilitate the detection, resolution and prevention of cybersecurity incidents in Singapore.[198] It ensures broadcasting of timely alerts in collaboration with law enforcement agencies. It is also empowered to drive education and awareness campaigns on cybercrime and cybersecurity through seminars and workshops.[199] It plays a crucial role in facilitating and enhancing international cooperation in collaboration with local CERTs to respond to cyber threats.

3.4.1.2.3. Office of the Personal Data Protection Commissioner

The Personal Data Protection Commission of Singapore has also developed a Data Breach Management Guide that offers practical actionable tips on how to monitor risks and manage data

[192] Overview of legislations on Cybersecurity, Personal Data Protection and Computer Misuse, pg. 17
[193] Ibid
[194] Ibid
[195] Ibid
[196] D. Koh, Singapore Cybersecurity Landscape 2021, pg 5
[197] Singapore Cyber landscape 2021
[198] Available at https://www.csa.gov.sg/Explore/who-we-are/our-identity/about-singcert last accessed on 01.12.2023 at 0036hrs
[199] Ibid

breaches.[200] This guide offers the much-needed awareness to stakeholders including citizens on the practical steps to be undertaken when a data breach occurs.

3.4.1.3. Technical and Procedural Measures

The government has developed mechanisms to effectively enhance its capacity and capability to combat cybercrime. Towards this end, it has developed a strategy that is premised on four key principles including: establishing a Cybercrime Command, putting in place mechanisms to boost cybercrime investigation capabilities, equipping public officers with capabilities for combating cybercrime, and enhancing coordination between the Singapore Police Force and government agencies.

3.4.1.3.1. The Cybercrime Command

Singapore has established a Cybercrime Command to oversee Cybercrime Response Teams. The Command was established to enhance the agility and effectiveness of the Singapore Police Force (SPF) to combat cybercrime.[201] Through this command, law enforcement agencies collaborate with the public, private industry and other government agencies in countering cybercrime. Through this Command, a training module has been developed to provide capacity building on recognizing, collecting and preserving digital evidence.

3.4.1.3.2. Boosting cybercrime investigation capabilities[202]

The police force has leveraged on technology to enhance its investigation capabilities; including development of tools that automate forensic processing of voluminous data. Hence expeditious investigation of cybercrime due to reduction in the time taken to process digital evidence. Furthermore, the government has also developed tools to speed up analysis of video footages, including tracking and recognition of faces and as well as optical character recognition.

3.4.1.3.3. Equipping public officers handling sensitive data with cybercrime capabilities[203]

Government agencies are often targets of malicious cybercriminals. As a result, the government of Singapore has established a Centre for Cybersecurity Studies (CCS) to facilitate capability and capacity of government officers and key stakeholders with the necessary skills to effectively counter cybercrime.

---

[200] Ibid pg. 18
[201] National Cybercrime Action Plan, Page 11
[202] Ibid
[203] Ibid

Remarkably, a cybersecurity Lab was set up for training and familiarizing trainees on approaches to not only mitigate cyber threats but also investigate cyber incidents. Such trainings are tailored to meet the officers' needs based on their professional roles. As result, public officers are also empowered to actively participate in countering cybercrime.

3.4.1.3.4. Strengthening Interagency Collaboration and Coordination [204]

There is marked collaboration and cooperation between the Singapore Police Force and partner agencies towards countering cybercrime. The Attorney General, partners with law enforcement agencies in investigating complex cybercrime cases. Such cooperation is employed at the nascent stages of investigation to enhance the quality of investigation and reduce the time taken in conducting a cybercrime investigation.[205] Time is of essence in cybercrime investigation, as a result, this approach has been effective in dealing with evidence which can easily be deleted from the server such as evidence stored in the Cloud.

Furthermore, effective cooperation towards an enhanced response to cyber related incidents has been forged between the Police force and the Cyber Security Agency. Other than information sharing, they have established a joint work flow that clearly distinguishes the mandate of the agencies and strengthens coordination in countering cybercrime.[206]

The government has also developed the National Cybercrime Action Plan that enunciates the fundamental tenets of its cybersecurity strategy. The plan outlines the importance of prevention, agile responses in countering the evolving threat of cybercrime through effective implementation of penal laws on cybercrime as well as the recognition of the shared responsibility in combating cybercrime.

In line with its 2021 cybersecurity strategy that focuses on the work environment as an enabler of a safe cyberspace, the government encourages its citizens to purchase products that are cyber hygiene compliant. Thus, ensuring consumers have access to products with better cybersecurity provisions.[207]

---

[204] Ibid
[205] Available at https://www.agc.gov.sg/our-roles/public-prosecutor/public-prosecutor-overview-of-functions . Last accessed on 30.11.2023 at 0202hrs
[206] Available at https://www.police.gov.sg/ . Last accessed on 30.11.2023 at 0206 hrs
[207] Ibid

To effectively prosecute cybercrime, the Attorney General has established the Technological Crime Unit. The Unit is comprised of prosecutors who are adequately trained on cybercrime. This level of specialization and expertise empowers the prosecutors to quickly understand technical details of cases hence efficient and timely investigation and prosecution of cybercrime. [208] Similarly, prosecutors in the Technology Crimes Unit cooperate with law enforcement agencies, including the police to facilitate proper investigation of cybercrime. Whereas specialization is important in that it creates a pool of highly specialized prosecutors to handle cybercrime, its main limitation is that the prosecutors cannot be in multiple places at the same time. Consequently, reducing the turnaround time in investigation and prosecution of cybercrime. It is thus necessary to not only have a specialized team to deal with cybercrime but also enhance the organizations' capacity and capabilities to effectively prosecute cybercrime.

Essentially, countering cybercrime in Singapore is a shared responsibility involving the public, private industry and the government. The technical and procedural safeguards put in place guarantees efficiency in combating cybercrime.

3.4.1.4. Capacity Building

Singapore has adopted prevention as the key principle towards countering cybercrime. Effective prevention is only possible when the public are aware of not only the reason but also the benefits of prevention.[209] Several initiatives have thus been developed towards strengthening capacity building on cybercrime.

3.4.1.4.1. Conducting Outreach to the General Public

The Singaporean government, in partnership with stakeholders continuously undertake robust initiatives to create awareness on cybercrime. At these awareness sessions, the public is informed of the nature of cybercrime and cybercrime prevention measures. Through these public awareness initiatives, the public are empowered to detect, prevent and report any cybercrime that might be committed within their sphere of influence.[210] Suffice to say, cybercrime investigation has been greatly hampered by failure to report, through such programs, law enforcement is enabled to map out cybercrime and develop strategies for countering them.

---

[208] Ibid. 196

[209] National Cybercrime Action Plan Singapore available at https://www.mha.gov.sg/docs/default-source/media-room-doc/ncap-document.pdf last accessed on 24.11.2023 at 1101 hrs

[210] Ibid

Singapore has also developed the Public Cyber and Outreach Resilience Program which exploits behavioural insights to influence cyber hygiene among members of the public.[211] Through this initiative, a whole of society approach is adopted in countering cybercrime through prevention. Mass media and advertisement platforms have also been employed to promote awareness on cybercrime.

In other instances community policing, through establishment of neighbourhood police centres have facilitated effective sensitization on cybercrime and cybercrime prevention measures to the communities.[212] Consequently strengthening law enforcement's capacity and capability to effectively respond to cybercrime reports by the public.

3.4.1.4.2. Creating awareness to vulnerable groups[213]

Vulnerable groups have been specially singled out in Singapore for capacity awareness on cybercrime prevention. These sessions have been made possible through partnership with civil society organizations that ordinarily champion the rights of vulnerable groups. Special focus has been placed on the elderly, who are often the target of internet scam and wire fraud.[214] Additionally, the Singapore Police Force in conducting these awareness focusses on children with a view to ensuring online protection of children.[215] This has been made possible through partnership with the Ministry of Education to provide cybercrime prevention lessons and tips to secondary school children

3.4.1.4.3. Reporting Framework

It is trite that the level of reporting of incidents of cybercrime is disproportionate to the actual incidents that occur. To counter this, the Singapore Police Force has developed a scam alert website to keep the public informed on trends in cybercrime.[216] Furthermore, the portal has been enhanced to provide an information hub on cyber hygiene to facilitate effective interaction between the public and administrators of various E-commerce platforms. Through such initiatives, real time assistance on transactions has been availed to customers and clients.[217] Additionally, the portal provides an avenue through which the public can share their experience with scammers to forewarn

[211] Ibid
[212] Ibid
[213] Ibid pg 9
[214] Ibid
[215] Ibid
[216] Ibid
[217] Ibid

those who might encounter similar experiences. Such experiences assist the police to identify emerging trends in cybercrime that warrant intervention.[218] Victims of cybercrime are sometimes shy to report their experience due to fear of reprisal or shame, as a result, the portal offers an opportunity for victims to anonymously report cybercrime to law enforcement agencies without fear of shame.

These Cyber awareness campaigns are a collaborative effort bringing together the Cyber Security Agency of Singapore the Singapore Police Force and other agencies. The Agency continually engages key stakeholders such as Governments, Industry and Civil Society to ensure a safe, secure and more resilient cyberspace.[219] As a result of enhanced capacity building, information sharing and openness, stakeholders have become more aware of their roles in countering cybercrime, especially members of the public.[220]

3.4.1.5. International and Stakeholder cooperation

The transnational nature of cybercrime calls for international cooperation towards addressing it. Remarkably, Singapore has distinguished itself as a force to reckon with in combating cybercrime. In fact, it has voluntarily steered initiatives on cybercrime in the ASEAN region.[221] Through these initiatives, the region has developed a coordinated approach on cybercrime through capacity building training and information sharing.[222] Including engaging other dialogue partners on cybercrime collaboration. The Technology Crime Unit has been instrumental in facilitating capacity building in ASEAN countries in conjunction with key partners including the Crown Prosecution Services among others.

3.4.1.5.1. Cooperation with Academia and Private Sector

Private Sector plays a key role in countering cybercrime due to the robust level of expertise that it provides. Critical private sectors such as banking and Information and Communication Technologies are often key targets of cybercrime. Therefore, it is increasingly crucial that government works closely with the private sector to combat cybercrime effectively. This partnership and collaboration are an avenue for information sharing on knowledge and expertise for combating cybercrime. Governments thus ought to reach out to the private Sector for

[218] Ibid
[219] D. Koh, Singapore Cybersecurity Landscape 2021, pg 5
[220] Singapore Cyber landscape 2021
[221] National Cybercrime Action Plan, Singapore
[222] Ibid

partnership on awareness creation as a suitable mechanism for countering cybercrime through prevention.

Similarly, institutions of higher learning spear head research in cybercrime prevention, detection, investigation and prosecution. Availing and offering courses on cybercrime and cybersecurity enhances the overall awareness of the public on cybercrime. Local research institutions in Singapore in partnership with the police force have developed new cybercrime forensic investigation capabilities to create an amiable atmosphere for cyber related innovations. Established talent labs foster collaboration and cooperation with law enforcement agencies and students form different institutions of higher learning on cyber forensics and investigations.

3.4.1.5.2. International Cooperation

Global technological advancements and internet penetration has made Singapore vulnerable to cybercrime and cyber-attacks. However, strong institutional, legislative and policy frameworks, coupled with a robust stakeholder engagement; provide both a shield and a sword for a healthy cyberspace in Singapore. Consequently, Singapore has developed key strategies for bolstering international engagement and cooperation.[223] These include: forging cooperation and connectivity both regionally and globally, robust capacity building frameworks and capability programs.[224]

Remarkably, INTERPOL's agency[225] that is responsible for incubating and facilitating innovation on cybercrime is situated in Singapore.[226] It has therefore leveraged on such formidable resources to operationalize its mechanisms and frameworks for countering cybercrime.[227]

For the period ranging December 2021 to January 2022, the Singapore Police Force and the Oversea Chinese Banking Corporation worked together to take down over three hundred and fifty phishing websites.[228] Though the cybercriminals set up other phishing websites following this crackdown, the Monetary Authority of Singapore engaged financial institutions by empowering them to beef up cybersecurity. As a result, the institutions developed strategies unique to their situations, hence countering cybercrime.[229]

---

[223] National Cybercrime Plan, Singapore
[224] Ibid
[225] INTERPOL's Global Complex for Innovation (IGCI)
[226] Available at https://www.interpol.int/en last accessed on 01.12.2023 at 0042 hrs
[227] Available at https://law.nus.edu.sg/asli/pdf/WPS001.pdf last accessed on 23.11.2023 at 0041hrs
[228] Ibid
[229] Singapore Cybersecurity Landscape, 2021 pg 29

The Cyber Security Agency working closely with the Singapore Police Force, the Personal Data Protection Commission and overseas partners successfully curtailed the criminal activities of a cybercriminal group that was engaged in cyber extortion. By issuing advisories son threats posed by the group, four small and medium enterprises were saved from the web of the cybercriminals. The Computer Emergency Response Team information sharing initiative ensured that the advisories were successfully issued and received by the targeted recipient.[230]

Singapore has an enhanced international cyber cooperation that has seen it sign Memoranda of Understanding with other nations, including the Republic of Finland, to recognize cybersecurity labels.[231] Furthermore, in 2021, Singapore hosted the 6th Singapore International Cyber Week culminating with the opening the ASEAN region cybersecurity centre.[232]Through collaboration with key partners including Governments, Industry, Institutions of higher learning and civil society organizations, the centre has delivered successful programs to senior officials from ASEAN and beyond on cyber security and cybercrime.

3.4.1.6. Conclusion

As incidents of cybercrime continue to increase in scale and magnitude, concerted effort needs to be put towards preventing cybercrime. Consequently, States ought to prioritize educating and empowering the public to uphold and create a safe cyberspace. As a result, a whole of society approach is required to build synergy with stakeholders in the private sector, academia, communities and governments to enhance solidarity and togetherness in countering cybercrime. Singapore has developed a framework in tandem with the Global Cyber Security Agenda that ensures effective countering of cybercrime.

3.4.2. Ghana

Technological restraints coupled with inadequate law enforcement expertise stifle the ability of developing countries to effectively combat cybercrime. In Ghana, uptake of ICTs has spurred growth in ICT business, consequently increasing vulnerability to cybercrime.[233]

[230] Ibid. pg 28
[231] Singapore Cyber Strategy, 2021
[232] Ibid
[233] R. Boateng et al, Cybercrime and Criminality in Ghana, Journal of Information Technology Impact,Vol. 11, no.2, pg. 85

To counter this situation, Ghana has developed a robust policy, legal and institutional framework towards countering cybercrime. It prides itself as having both a National Cyber Security Strategy and a National Incident Response Capability. Making it one, of twelve States with such a framework in Africa. Furthermore, it has distinguished itself by being numbered among the four States in Africa that have ratified both the Budapest and Malabo Conventions on cybercrime and personal data protection.[234]

3.4.2.1. Legal Measures

Ghana has a robust policy, institutional and legal framework on cybercrime emanating from both domestic legislation as well as regional and international instruments. Therefore it has largely benefited from the legal provisions on mutual legal assistance, international cooperation and technical assistance through capacity building and capabilities programs.

The operational definition of cybercrime in Ghana embodies both cyber related crime and cyber dependent crimes. It refers to committing a crime through utilization of cyberspace, information technology or electronic facilities.[235]

The key domestic legislations enacted towards countering cybercrime include: the Cybersecurity Act 2020, the Data Protection Act 2012, the Electronic Transactions Act, 2008 and the Electronic Communications Act, 2008. The Cybersecurity Authority, is established under the Cybersecurity Act as an independent body mandated with regulating cybersecurity activities in Ghana.

3.4.2.1.1. The Cybersecurity Act, 2020

The Act empowers the Cyber Security Authority to regulate and promote the development of cybersecurity in Ghana.[236]

It recognizes the intertwined nature of cybersecurity that calls for intentional involvement of other key stakeholders in cybersecurity decision making.[237]

---

[234] Available at https://africacenter.org/spotlight/ghana-multistakeholder-cyber-security/#:~:text=These%20improvements%20allowed%20Ghana%20to,sponsored%20Malabo%20Convention%20in%202021. Last accessed on 17th April 2023 at 1.47pm EAT

[235] Section 97

[236] Long title of the Act

[237]Section 1 (2) provides that the Act should be read together with the following relevant enactments: the Criminal Offences Act, 1960 (Act 29); Evidence Act, 1975 (N.R.C.D. 323); Foreign Exchange Act, 2006 (Act 723); Anti-Money Laundering Act, 2008 (Act 749); Anti-Terrorism Act, 2008 (Act 762); Electronic Transactions Act, 2008 (Act

It is noteworthy that cybersecurity incidents involving national security, public health, international relations, safety of life and property may warrant intervention by the Authority whether they happen within or outside Ghana.[238] For efficiency in investigation and prosecution of cybercrime, the Authority is mandated to provide technical support needed by law enforcement agencies during investigation and prosecution of cybercrime.[239]

It is commendable that practical steps have been taken to embed stakeholder engagement in legislation. The governing board of the Authority comprises three persons from private sector and Industry among other government appointees.[240] The Joint Cybersecurity Committee established under the Act is answerable to the Board.[241]The committee is chiefly comprised of key government agencies from various sectors of the economy. Through this Committee, the Authority coordinates collaboration with government sectors and agencies on cybersecurity.[242]Accordingly, such clear framework for engagement alleviates any suspicion that might exist among stakeholders and government security agencies as the parameters for engagement are clearly outlined.

The Computer Emergency Response Team (CERT) established under the Act is mandated to coordinate responses to cybersecurity incidents with government institutions, Industry and International organizations. [243]Similarly, sectoral Computer Emergency Response Teams are also established for effective incident coordination among government sectors.[244] The Sectoral CERT reports to the National CERT.

The Authority is also empowered to license cybersecurity service providers[245]. Further, it accredits and certifies cybersecurity professionals and practitioners.[246] Hence enhancing the number of local technical experts on cybersecurity. In appreciating the role of awareness in combating cybercrime,

772); Electronic Communications Act, 2008 (Act 775); Economic and Organized Crime Office Act, 2010 (Act 804); Mutual Legal Assistance Act, 2010 (Act 807); Data Protection Act, 2012 (Act 843); and Payment Systems and Services Act, 2019 (Act 987)

[238] Section 4 (g)
[239] Section 4 (i)
[240] Section 5 (c)
[241] Section 13
[242] Section 14 (1)
[243] Section 41
[244] Section 44 (1)
[245] Section 49
[246] Section 57

the Authority engages in programs that promote cybersecurity awareness and education among the citizens[247]. Including the development of research and competency framework for educational institutions and persons offering cybersecurity training.[248]

It is noteworthy that the Act provides the procedure for obtaining subscriber information, retention of data or freezing of assets towards countering cybercrime through investigation and prosecution.[249]

The Industry forum is an initiative for stakeholder engagement established to coordinate the industry on issues of mutual interest.[250]Its open-ended nature facilitates participation by critical actors such as cybersecurity service providers, telecommunications network operators among many other stakeholders on cybercrime.[251]

The Authority is empowered to develop mechanisms for international cooperation.[252] Consequently developing a strategic framework for operationalization of regional and international Conventions on Cybercrime in Ghana.[253] Notwithstanding the provisions on international cooperation, the Act also encourages public private partnerships with the Authority towards countering cybercrime.[254]

The Authority is committed to engaging all designated Critical Information Infrastructure owners and industry stakeholders to implement the required cybersecurity best practices for Ghana.[255]

3.4.2.1.2. The Electronic Transactions Act, 2008

The Act is chiefly concerned with creating a safe and secure environment for facilitating electronic transactions. Whether the said transactions are between private citizens, governments or international organizations.[256] It complements the Cybersecurity Act as it also creates cyber

[247] Section 60
[248] Section 61
[249] Section 69
[250] Section 81 (1)
[251] Section 81 (3)
[252] Section 83 (1)
[253] Section 83 (3) Ghana acceded to the Budapest Convention in December 2018. It also ratified the Malabo Convention of the African Union in 2021
[254] Section 88
[255] Republic of Ghana, Directive for the protection of Critical Information Infrastructure, 2021, pg. 4
[256] Section 1(d)

offences.[257] Just like the Cybersecurity Act, it also establishes the Industry Forum, which unites stakeholders to collaborate and cooperate on cybersecurity issues of mutual interest. [258]

3.4.2.1.3. National Cyber Security Policy and Strategy, 2015

It outlines the roadmap towards cybersecurity in Ghana. It sets out initiatives geared towards enhancing Ghana's cybersecurity. The National Cyber Security Council, the National Cyber Security Center, the National Computer Security Incidence Response Team (CSIRT) and the National Cyber Security Policy Working Group, are some of the critical institutions that the strategy and the policy envisioned. Operationalization of the policy was placed under two crucial institutions to underscore the dual interests in countering cybercrime: the Ministry of Communication and the National Security Council.[259]The inclusion of the National Security Council in cybersecurity and cybercrime discussions demonstrate the securitization of cybercrime.

The strategy, mandated the Attorney General and the Minister for Communication to identify areas of concern in the cyberspace and make any proposals for legislative reform.[260] Remarkably, the successful implementation of the National strategy led to the enactment of the Cybersecurity Act in 2020 and ratification of the Budapest and Malabo Conventions.

In collaboration with key stakeholders, the government was obligated to develop a clear cybersecurity technology framework and develop international cybersecurity standards.[261] Moreover, the policy targets improved awareness as a key tool in combating cybercrime through prevention.

The Policy demonstrates that Ghana is committed to research and development towards self-reliance; especially by procuring and developing technologies relevant to Critical Infrastructure and Installation. The Ministry of foreign affairs is critical in prioritizing engagements on cybersecurity, including the signing of international conventions.

3.4.2.2. Organizational Structures

Successful implementation of the Ghana Cybersecurity Strategy 2015, led to the establishment of a robust institutional framework for countering cybercrime. In fact, it set up its first Computer

[257] Section 107-123
[258] Section 88 (1)
[259] Page 28
[260] Ibid page 30
[261] Ibid

Emergency Response Team (CERT-GH) under the Ministry of Communication, by leveraging on strategic partnerships with stakeholders.[262]Consequently, these networks have enabled it to successfully recover from several cybersecurity incidents.[263]

The National Information Technology Agency has been established to enhance its governmental network infrastructure. Similarly, the National Security Council steers a working group on cybersecurity that seeks to propel Ghana's law enforcement response to cybercrime and cybersecurity. The Police Service has also operationalized a Cybercrime Unit solely mandated to undertake investigations into cybercrime incidents in partnership with key stakeholder agencies. Likewise, the Bureau of National Investigation is empowered to undertake investigations into serious crimes, including cybercrime. The Data Protection Commission is specially tasked to ensure that the Constitutional safeguards on collection and processing of data are upheld at all material times during a cybercrime investigation.

A unique tenet in Ghana's institutional framework on countering cybercrime is the creation of the Financial and Economic crimes courts, specialized to handle both money laundering and cybercrime cases. This arrangement has often been fronted as favourable as it guarantees expertise in the determination of cybercrime cases. Critics of this arrangement have however argued that it is not possible to decentralize the special courts to all parts of the country hence resulting in backlog and loss of crucial evidence. Especially since time is of essence in cybercrime investigation.

3.4.2.3. Technical and Procedural Measures

The Cybersecurity Authority is mandated to establish a platform to facilitate cybersecurity engagements. Through this initiative, there is enhanced coordination and cooperation between key public institutions and the private sector.

[262] Through the support of Forum of Incident Security Response Team (FIRST) and Africa Computer Emergency Response Team (Africa CERT)

[263]K. Adu & DF. Allen, Learning from Ghana's Multistakeholder Approach to Cyber Security, January 2023 Available at https://africacenter.org/spotlight/ghana-multistakeholder-cyber-security/#:~:text=These%20improvements%20allowed%20Ghana%20to,sponsored%20Malabo%20Convention%20in%202021.

3.4.2.3.1. Cybersecurity Authority Ghana

The Authority is vested with the mandate of coordinating stakeholder engagement. This is to be achieved through creation of platforms for cross sector engagement that facilitate collaboration and cooperation with key institutions. The institutions comprise private sector, public sector and civil society organizations.[264] Furthermore, it is the lead agency in facilitating international cooperation towards enhanced cybersecurity in the country.[265] Towards this end, it not only establishes best practice standards for cybersecurity but also monitors compliance by owners of critical information infrastructure.[266]

3.4.2.3.2. Industry Forum[267]

It is commendable that Ghana, in recognizing the crucial role of stakeholders in countering cybercrime, have, by legislation, established the industry forum that allows stakeholders to collaborate, cooperate and share ideas on enhancing cybersecurity and countering cybercrime. The Industry forum is an initiative for stakeholder engagement established to coordinate the industry on issues of mutual interest

Though Ghana still faces cybersecurity challenges, including cybercrime, the civilian centric multistakeholder approach has put it in an excellent position to combat cybercrime. By harnessing the benefits of technology and digitization, Ghana has developed an inclusive approach to cybersecurity, hence enhancing democracy. It is instructive that the stakeholder approach in countering cybercrime was first envisioned in policy and implemented through legislation by creating an enabling institutional framework. As a result, multistakeholderism is the operating model of combating cybercrime in Ghana.

3.4.2.3.3. Incident Reporting

Ghana has developed an initiative dubbed, a safe digital Ghana, to enhance incident reporting points in the country. Reports on cybercrime and cybersecurity can be made to the Ghana National Computer Emergency Response Team Ghana (CERT-GH) through social media platforms including WhatsApp, Electronic Mail (Email), Mobile Apps, Short Messaging Services (SMS) or via phone calls.[268]

---

[264] Section 3(e)
[265] Section 3(g)
[266] Section 4 (d)
[267] Established under Section 81 of the Ghana Cybersecurity Act
[268] Available at https://www.csa.gov.gh/cert-gh last accessed on 23.11.2023 at 1552 hrs

CERT -GH is specially empowered to assist critical partners at all levels in responding to cybercrime. Moreover, it is the agency responsible for collaborating with international corporations and agencies to facilitate emergency response to cybersecurity incidents.[269] Additionally, it collaborates with regional cybersecurity partners towards information sharing on countering cybercrime.[270]

3.4.2.4. International Cooperation

Having ratified both the AU Convention on Cybersecurity and Personal Data Protection as well as the Council of Europe Convention on Cybercrime, Ghana has put in place a robust legislative framework for international cooperation. As a result, it has benefitted on technical assistance through capacity building initiatives under these Conventions.

By leveraging on its INTERPOL membership, it has benefited from international cooperation on cybercrime and digital evidence. The Ghana Police Service hosts the National Central Bureau that facilitates 24/7 international cooperation.

Also, the Cyber Security Authority is empowered to coordinate international cooperation with international agencies to enhance cybersecurity in the country.[271]

3.4.2.5. Capacity Building

Ghana has been instrumental in championing capacity building on cybercrime in ECOWAS, including through sharing advice on cybercrime legislation drafting to both Sierra Leone and the Gambia. As a result of its commitment to countering cybercrime, ECOWAS requested Ghana to champion cybersecurity and the war against cybercrime in the region. The Cybersecurity Authority facilitates capacity building and awareness creation on cybercrime in partnership with other agencies.

Academic institutions including institutions of higher learning have been instrumental in championing capacity building and awareness on cybercrime.[272]

---

[269] Ibid
[270] Ibid
[271] Ibid
[272] The Koffi Annan International Peace Keeping centre, University of Ghana, Kwame University of Science and Technology among others offer training on cybersecurity and cybercrime

3.4.2.6. Conclusion

A coherent global strategy is required to effectively address the numerous challenges posed by cybercrime. Such strategy must recognize and uphold the role that stakeholders play in combating cybercrime. The practice in Ghana and Singapore demonstrates that combating cybercrime is a shared responsibility as the state alone is incapable of mounting a competent war on cybercrime.

The following components of multistakeholderism stand out as international and national best practice from the experience of Singapore and Ghana:

i. **Legal measures:** A robust legislative and policy framework that provides a platform for stakeholder engagement in combating cybercrime. It is not enough to adopt a policy on stakeholder engagement. The law must clearly spell out the modalities and manner of engagement of stakeholders in countering cybercrime. Ghana has established the Industry forum which brings together all relevant stakeholders to address issues of cybercrime and cybersecurity. Similarly, Singapore's cybersecurity strategy provides a framework that adapts to the changes brought about by technological advancements.

ii. **Organizational structures**: Strong institutional frameworks including creation of an independent agency solely responsible for receiving cybercrime reports and coordinating stakeholder engagement. Both Ghana and Singapore have independent agencies that are responsible for coordinating stakeholder engagement and receiving reports on cybercrime. A strong institutional framework facilitates openness and accountability in stakeholder engagement.

iii. **International cooperation:** Adequate regional and international legal framework for international cooperation and mutual legal assistance. Ghana is a party to both the Malabo Convention and the Budapest Convention. These Conventions provide an avenue for international cooperation and Mutual Legal Assistance for effective cybercrime investigation and prosecution. Furthermore, Ghana also benefits from technical assistance of personnel and experts within the frameworks created by these Conventions.

iv. **Capacity Building:** Effective mechanisms for cyber awareness among the citizens to facilitate prompt detection, reporting and cooperation in countering cybercrime. Both Singapore and Ghana have put in place mechanisms for awareness creating among the citizens and key stakeholders through public awareness campaigns and media engagements.

v. **Technical and Procedural Measures**: Identification of key stakeholders to be involved in combating cybercrime. The Malabo Convention recognizes the critical responsibility of stakeholders in the promotion of cybersecurity. Some of the stakeholders identified under the Convention include communities, civil society, the media and academia among many others.[273].

[273] Preamble

CHAPTER 4: THE LEGAL, INSTITUTIONAL AND POLICY FRAMEWORK FOR MULTISTAKEHOLDERISM IN THE FIGHT AGAINST CYBERCRIME IN KENYA

4.1. Introduction

Although, Kenya has enacted laws and ratified regional and international instruments that address cybercrime, the fight against cybercrime is still faced by unique challenges. This is because cybercrime is affected by the dynamics of technological advancements. As a result, the legal, policy and institutional framework is unable to cope up with the technological advancements. Another reason for this could be transnational nature of cybercrime and the different stakeholders affected by cyber issues. It is possible that a multi stakeholder approach to cybercrime would be necessary in combating cybercrime.

Since the cyberspace allows digital anonymity, it is used by persons with ill intentions in ways that undermine both state security and sovereignty.[274] Many states find themselves in limbo in combating cybercrime. The fact that cybercrime raises serious issues of security and sovereignty calls for a concerted approach to ensure that all pertinent interests are protected.

With no single entity having the ability to address all the issues of the internet especially cybercrime, all entities that have an interest in the internet should come together to combat cybercrime. The legal, institutional and poly framework should put in place measures and mechanisms for this stakeholder engagement.

Having outlined the international best practice for multistakeholderism in combating cybercrime, this chapter will critique the practice in Kenya with a view of making legislative, policy and institutional proposals for reform. Moreover, wonderful insights from the current practice in Kenya shall also be highlighted towards understanding and addressing areas of improvement.

4.2. Legal Measures

Kenya is not party to any regional or international convention on cybercrime; however, it is a party to the UNTOC. As a result, it may benefit from the provisions of the Convention on international cooperation when faced with transnational organized cybercrime. Nevertheless, Kenya needs to demonstrate its commitment to countering cybercrime by ratifying the regional conventions on

[274] J. Dache, MBS, *The State of Cybercrime: Current Issues and Countermeasures* Pg. 28

cybercrime such as the Malabo Protocol. There is hope that Kenya might ratify the UN Convention on Countering the Use of Information and Communication Technologies for criminal purposes.

4.2.1. The Constitution of Kenya 2010

As the supreme law of the republic, it recognizes international law ratified by Kenya as law.[275] Furthermore, general rules of international law are also considered as Kenyan law.[276] This therefore mean that principles and international law norms on cybercrime are applicable to Kenya.

The Kenya Bill of rights is binding upon all state organs. Notably, governance of the cyberspace raises serious human rights issues such as the right to privacy.[277] Furthermore, the state is to ensure the right to personal security[278] is guaranteed in both the online and offline spaces. The right to property including intellectual property rights is also protected by the Constitution.[279]

Regarding stakeholder engagement, the Constitution affirms that sovereign power is vested in the people of Kenya; and can only be exercised according to the Constitution.[280] This provision recognizes that the people of Kenya are key stakeholders, whose views must be taken into consideration when exercising any mandate vested by the Constitution. In fact, public participation is anchored in the Constitution as a key national value and principle of governance.[281]

Though the Constitution recognizes public participation, the same has not been defined, nor a legislation enacted in a manner that gives clarity as to what it entails. Parliament is obligated to facilitate participation and involvement of the public in the discharge of its legislative mandate.[282] Remarkably, the devolved government structures are also enjoined to facilitate participation and involvement of the public in legislative and committee business of the assemblies.[283]Similarly, the public service is enjoined to consider public participation in policy making.[284]

The courts have been at the forefront in giving meaning to the constitutional requirement for public participation. Consequently, the courts have since pronounced the basic tenets of public

[275] Article 2 (6)
[276] Article 2 (5)
[277] Article 31
[278] Article 29
[279] Article 40 (5)
[280] Article 1 (1)
[281] Article 10 (2) (a)
[282] Article 118 (1) (b)
[283] Article 196 (1) (b)
[284] Article 232 (1) (d)

participation including the availing of reasonable opportunity to all persons who might be affected by the decision to have adequate say. The quality of reasonable opportunity is essentially case dependent.[285]

Though public participation is justiciable in the absence of substantive legislation, guidelines or framework[286] there is need to embed it in legislation to enhance effective participation of citizens and interested parties in legislations and polices that they have an interest in.

4.2.2. Computer Misuse and Cyber Crimes Act, No. 5 of 2018 (CMCCA)

The Act is the main penal law on cybercrime. It is both a substantive and a procedural law to ensure timely and effective mechanisms for countering cybercrime.[287] It was also enacted to facilitate international cooperation and collaboration in countering cybercrime.[288] Though Kenya is not party to any international or regional convention on cybercrime, aspects of the Budapest Convention and the Malabo Convention are evident in the CMCCA.

The Act is the substantive legislation on cybercrimes in Kenya. It prescribes both the offence and their attendant penalties. It also provides a framework for governance of cyberspace through the establishment of the National Computer and Cybercrime Coordination Committee.[289]

Unlike the Ghana Cybersecurity Act[290] that establishes the industry forum where stakeholders can deliberate on issues of cybersecurity and cybercrime, this Act neither establishes nor mentions the existence of any such forum. As a result, stakeholder engagement under the Act is limited to the Constitutional requirement of public participation. It would be useful for the Act to make a provision for stakeholder engagement since countering cybercrime is a shared responsibility.

4.2.3. Kenya Information and Communication Act, No. 2 of 1999

The Act establishes the Communication Authority, which is empowered to among others develop a framework for enhancing effective and efficient investigation and prosecution of cybercrimes.[291]Towards this end, the Authority, established the National Kenya Computer

[285]Republic v Independent Electoral and Boundaries Commission (I.E.B.C.) Ex parte National Super Alliance (NASA) Kenya & 6 others [2017] eKLR
[286] Ibid
[287] Section 3
[288] Long title of the Act
[289] Section 3
[290] Section 80
[291] Section 83 C (1) (h)

Incident Response Team Coordination Centre (National KE-CIRT/CC) to mitigate cyber threats and guarantee a safer cyberspace for Kenyans.[292]

Just like the Computer Misuse and Cybercrimes Act, this Act does not make adequate provision for stakeholder engagement in countering cybercrime. The KE-CIRT/CC established by the Authority are not stakeholder bodies as they comprise government agencies. To enhance efficiency in countering cybercrime and securing the Kenyan cyberspace, it would be prudent that the National KE-CIRT/CC be housed within an independent agency solely responsible for cybersecurity and cybercrime in Kenya.

The cybersecurity and cybercrime role donated to the Communication Authority should be transferred to an independent agency to avoid duplicity of roles. Having all cybersecurity and cybercrime issues in Kenya primarily handled by one independent agency will streamline capacity building in cybersecurity and cybercrime and enhance law enforcement capacity to counter cybercrime.

4.2.4. The Data Protection Act, 2019

The Act, regulates the processing of personal data by outlining the obligations of data controllers and processors.

Law enforcement agencies find this Act useful when seeking judicial preauthorization to facilitate access, preservation and interception of information of a personal nature during cybercrime investigation.[293] The Data Protection Commissioner is mandated to collaborate with national security organs in the exercise of its powers and functions.[294]In recognition of the crucial role of time in cybercrime investigation, the Commissioner is authorized to obtain an order to facilitate expeditious preservation of personal data to avoid risk of alteration or loss.[295]

[292] Available at https://www.ca.go.ke/industry/cyber-security/overview/#:~:text=The%20Kenya%20Information%20and%20Communications,national%20cyber%20security%20management%20framework. Last accessed on 18th April 2023
[293] Section 51 (2) (c)
[294] Section 8 (2)
[295] Section 66

It mandates data controllers and data processors to safeguard personal data by preventing its transfer outside jurisdiction without the data subject's consent.[296]Remarkably, the Act empowers courts are empowered to seize any equipment or article connected to commission of an offence.[297]

In recognizing the competing rights to privacy and security in cybercrime investigation, it has provided mechanisms through which these dual rights may be achieved in the public interest. Noting of course that both rights are subject to limitation in an open and democratic society, within Constitutional safeguards.[298]

Unlike the Computer Misuse and Cybercrimes Act and the Kenya Information and Communication Act that make no mention of stakeholder participation, this Act enjoins the Data Commissioner to consult stakeholders in the development of guidelines specific to the relevant sectors in areas such as health, financial services, education and social protection among many others.[299] However, the Act falls short of stating the scope and manner of the stakeholder consultations.

Data protection is at the heart of cybercrime investigation and prosecution. Relevant and admissible evidence required in cybercrime investigation and prosecution is largely in electronic format. Hence the need for strong legislative frameworks to facilitate stakeholder engagement in gaining access to and sharing of personal data between private entities and law enforcement to facilitate effective prosecution of cybercrime.

4.3. Technical and Procedural Measures

Kenya developed the first National cybersecurity strategy in 2014 to ensure a secure online environment to conduct business and other economic activities. The strategy focused inter alia on goals including to foster information sharing and collaboration among relevant stakeholders.

In recognition of the critical role of stakeholders in cybersecurity, the 2014 strategy highlighted the government's commitment to solicit stakeholder input and feedback as appropriate.[300]It was recognized that improved cybersecurity would enhance greater cooperation with international organizations and enhance economic wellbeing and private sector growth. Successful

[296] Section 25 (h)
[297] Section 73 (2) (a)
[298] Constitution of Kenya, 2010, Article 24
[299] Section 74 (d)
[300] National Cybersecurity Strategy 2014. Pg 13

implementation of the strategy led to the development of Key ICT policies, and laws including Kenya Information and Communications Act, 1998; National Cybersecurity Strategy 2014; National Broadband Strategy 2018; Computer Misuse and Cybercrimes Act (CMCCA), 2018; Data Protection Act (DPA), 2019; National ICT Policy Guidelines 2020; and National Digital Master Plan 2022.

Successful implementation of the 2014 Cybersecurity Strategy led to the establishment of the Kenya Computer Incident Response Team and Coordination Centre (KE-CIRT/CC) and the National Digital Forensics Laboratory within the National Police Service.

4.3.1. National Cybersecurity Strategy 2022-2027

This second cybersecurity strategy was developed in 2022 to renew Kenya's efforts of having a coordinated approach towards creating a secure cyberspace. The strategy recognizes the crucial role played by various stakeholders in cyberspace and the need to involve them in cybersecurity discussions. Essentially, it calls upon stakeholders to partner with the government in securing Kenya's cyberspace for economic development.[301] Unlike the first cybersecurity strategy that was steered by the Ministry of ICT, the 2nd Cybersecurity strategy is steered by both the Ministry of ICT and the Ministry of Interior and Coordination of National Government. Consequently, balancing the ICT elements with national security interests.

The key pillars identified by the strategy include effective governance of the cyberspace, development of laws, policies and standards; capacity building on cybercrime and safeguarding of critical installations under the umbrella of collaboration and cooperation.[302]Stakeholders are required to assist in the implementation of the strategy by executing specific initiatives identified in the strategy.[303]

The strategy intends to upgrade the Kenya Computer Incident Response Team (KE-CIRT) to the National Multi-Stakeholder Computer Incident Response Team of the Republic of Kenya.[304] However, it fails to describe the composition and role of the envisioned body. The Strategy recognizes the critical role of an information sharing platform in countering cybercrime.[305] As a

[301] Kenya Cybersecurity Strategy 2022-2027
[302] Ibid Pg. 7
[303] Ibid
[304] Ibid Pg. 10
[305] Ibid

result, it provides for the establishment of an incident response framework to facilitate protection of critical information infrastructure.[306]

The strategy cements the role of academia in countering cybercrime as the government is committed to supporting research and innovation for developing cybersecurity skills and knowledge.[307]

A National Cybercrimes Alert and Warning system is to be established to mitigate cybersecurity risks and combat cybercrimes. Since cyber threats are cross cutting and transnational, collaboration and cooperation at domestic and international level is key in combating cybercrime. Through the strategy, the government shall develop a framework for national, regional and international co-operation and collaboration.[308]

The National Cybersecurity Strategy has placed a lot of emphasis on stakeholder engagement in countering cybercrime. It recognizes the crucial role that stakeholders play in facilitating investigation and prosecution of cybercrime. Proper implementation of this strategy will see Kenya ratify international and regional conventions on cybercrime as a mechanism for enhancing international cooperation in countering cybercrime.

However, the strategy falls short of establishing an independent agency responsible for cybersecurity and cybercrime, instead, it seeks to converts the KE-CIRT to the National Multi-Stakeholder Computer Incident Response Team of the Republic of Kenya. Whereas, this step is commendable for recognizing the role of stakeholders in incident response, a better approach would be to create the National incident team under an independent agency dealing with cybercrime. As it stands, the National incident team, to be established would still be under the Communication Authority. Accordingly, cybersecurity and cybercrime ought to be managed from one agency for ease of coordination, collaboration and cooperation.

4.4. Organizational Structures

The legal and policy framework in Kenya has facilitated creation of a robust institutional framework towards countering cybercrime.

[306] Ibid
[307] Ibid Pg. 13
[308] Ibid Pg. 14

4.4.1. National Computer and Cybercrime Coordination Committee

The Committee is established under the Computer Misuse and Cybercrimes Act, 2018 as the lead body on issues of cybercrime in Kenya. It is responsible for advising the National Security Council on computer and cybercrime among others. It is responsible for the analysis and response to cyber threats, whether within or outside the country. The Committee is also mandated to develop a mechanism that enhances the prevention, detection and mitigation of cybercrime by oversighting cybercrime capacity building.[309]

The Director of the Committee is authorized to designate certain systems as critical infrastructure. Owners of critical information infrastructure have a framework for information sharing towards facilitating cybersecurity, especially towards countering cybercrimes.[310] The Act makes provision for international cooperation through mutual legal assistance towards enhancing effective and efficient investigation and prosecution. Areas of cooperation include collection of evidence or expeditious preservation or disclosure of traffic data.[311]

The Committee comprises the Principal Secretary in charge of internal security, the Principal Secretary in charge of ICT, the Attorney-General, the Chief of the Kenya Defence Forces, and the Inspector-General of National Police Service, the Director-General National Intelligence Service, the Director-General Communication Authority, the Director of Public Prosecutions, the Governor Central Bank of Kenya, and the Director National Computer and Cybercrime Coordination Committee Secretariat.

Remarkably, the membership of the committee coupled with its role as the advisor to the National Security Council demonstrates that cybercrime in Kenya is largely treated as a security concern. This approach fundamentally affects the effectiveness of the Committee to detect, investigate, prosecute and prevent cybercrime as the members of the committee are still bound by their respective oaths of office. As a result, other key stakeholders might experience challenges in cooperating with the Committee in countering cybercrime due to the covertness of security operations. The Director General of the Committee heads the National Cyber Command Center,[312] a predominantly intelligence agency.

[309] Section 6 (1) (b)
[310] Section 12 (2)
[311] Section 57 (2) (c)
[312] NC3

Similarly, the operations of the committee are styled as government agenda since all the members are drawn from government agencies. In fact, the Committee reports to the Cabinet Secretary for Interior and National Administration. This model stifles multistakeholder engagement in countering cybercrime as it offers no room for effective stakeholder engagement. There is need to establish an independent agency, similar to the Ghana Cybersecurity Agency, that is responsible for securing Kenya's cyberspace and critical infrastructure at both the national and county level. This independent agency should facilitate information sharing between the private sector, government and other stakeholders.

Additionally, as a platform for multistakeholder information sharing, the agency can be responsible for receiving incident reports from relevant stakeholders in a bid to enhance the detection, prevention, investigation and prosecution of cybercrime. Consequently, the Kenya Incident Response Team, instead of being housed at the Communication Authority, will be under the proposed independent agency. The overriding objective of the agency would be to guarantee a safe cyberspace by preventing, preparing for, responding to and recovering from incidents while assisting law enforcement agencies to effectively deal with investigation and prosecution of cybercrime and cybercriminals.

4.4.2. National Kenya Computer Incident Response Team Coordination Centre (National KE - CIRT/CC)

It is responsible for the coordination of cybersecurity in Kenya.[313] It is a multiagency comprising staff from the Communication Authority and law enforcement agencies.[314] It acts as the interface between domestic and international ICT service providers and the justice sector in investigation, prosecution and adjudication of cybercrime.[315] It offers technical coordination and response to cyber incidents in partnership with stakeholders nationally and internationally. It is also responsible for cybersecurity awareness and capacity building.[316]

[313] Available at https://ke-cirt.go.ke/ last accessed on 03.12.2023 at 0329 hrs
[314] Ibid
[315] Ibid
[316] Ibid

4.4.3. Office the Data Protection Commissioner

It is established under the Data Protection Act and mandated to promote international cooperation in matters of data protection.[317] The Commissioner is also responsible for ensuring the country's compliance with international data protection obligations.[318] The Data Protection Commissioner ensures that Cybercrime investigations are undertaken in compliance with the law on processing and disclosing information or data.[319] Moreover, the Commissioner receives information on cybersecurity incidents that might have caused loss or compromise of personal data or information.[320]

4.5. Capacity Building

Capacity building initiatives on Cybercrime in Kenya have often been carried out in partnership with private industry and institutions of higher learning. Through media campaigns, several awareness initiatives have been carried out on various thematic issues including child online protection.

Increasingly, institutions of higher learning are offering Certificate, Diploma, Undergraduate and Post graduate courses on cybercrime and Cybersecurity. Similarly, professional bodies have also developed and conducted continuous professional development on cybercrime and cybersecurity. These initiatives have enhanced the overall awareness of the public on cybercrime.

Through the use of websites, government institutions and law enforcement agencies have set up digital reporting frameworks where the public can lodge complaints and make reports on cybercrime.

4.6. International Cooperation

Though Kenya has not ratified any international convention on cybercrime, the Constitution of Kenya facilitates international cooperation as it recognizes international law as part of Kenyan Law.[321] Consequently, Kenya relies on existing conventions on cooperation to facilitate effective investigation and prosecution of transnational cybercrime.

---

[317] Section 5 of the Data Protection Act, No. 24 of 2019 available at DataProtectionAct24of2019.pdf (kenyalaw.org) last accessed on 01.12.2023 at 0049 hrs
[318] Ibid Section 9
[319] Ibid
[320] Ibid
[321] Article 2(5) and 2 (6) of the Constitution of Kenya, 2010

Moreover, membership in international associations such as the International Telecommunication Union, INTERPOL and Commonwealth Association have significantly enhanced Kenya's capacity to counter cybercrime.

4.7. Conclusion

Though Kenya has a comprehensive legal framework on cybercrime; investigation and prosecution of cybercrime still faces myriad challenges as law enforcement agencies alone are incapable of adequately cracking the complex web of cybercrime investigations. A robust legislative and policy framework on multistakeholderism is key in propelling stakeholder engagement towards countering cybercrime. There is need to align the Computer Misuse and Cybercrimes Act[322], the Kenya Information and Communication Act[323] and the Data Protection Act[324] with the National Cybersecurity Strategy 2022- 2027 to create room for effective stakeholder engagement in countering cybercrime.

The current situation is that Kenya does not have a proper framework for multistakeholderism. To begin with, there is no independent agency that is responsible for cybercrime reporting and stakeholder coordination. Instead, there is a Coordination committee whose membership is drawn from agencies that deal with security operations. Moreover, cybercrime in Kenya is treated as a security issue, hence stifling information sharing between law enforcement and key stakeholders. There is more that can be done to bolster regional and international cooperation in offering technical assistance towards capacity building and effective investigation and prosecution of cybercrime, including ratification of regional and international Instruments on combating cybercrime.

[322] No. 5 of 2018
[323] No. 2 of 1998
[324] No. 24 of 2019

CHAPTER FIVE: FINDINGS, RECOMMENDATIONAND CONCLUSION

5.1. Introduction

This chapter focuses on the findings, recommendation and conclusion of the efficacy of multistakeholderism in combating cybercrime in Kenya.

The main research question is to ascertain whether there exist an adequate legal and policy framework for multistakeholderism in combating cybercrime in Kenya.

Consequently, the main research questions for consideration are: What is the nature of cybercrime in Kenya; What is the international best multistakeholderism practices in the fight against cybercrime; What is the legal and policy framework for multistakeholderism in countering cybercrime in Kenya; and the findings, recommendations and conclusion of the study.

Towards this end, the chapters were intentionally organized to meet the main objective of the study which is to understand the concept of multistakeholderism and critically examine its efficacy in fighting cybercrime in Kenya.

The specific objectives flowing from the main objective are to: To understand the nature of cybercrime and expose the stakeholders directly involved in combating cybercrime; To assess the international best multistakeholderism practices in the fight against cybercrime; To review the adequacy of the legal, policy and institutional framework for multistakeholderism in the fight against cybercrime in Kenya; and to provide recommendations for combating cybercrime in Kenya.

5.2. Findings

From the study, it is evident that the best way to combat cybercrime is through a multistakeholder approach. The practice in Singapore and Ghana reveals that a sound stakeholder approach in combating cybercrime should consist of the following elements:

1. **Legal Measures**

In Singapore, the cybersecurity strategy recognizes that crucial role that stakeholders play in securing the cyberspace and combating cybercrime. As a result, the Commissioner for cybersecurity has developed and put in place, in collaboration with the stakeholders, codes and standards of practice that guide stakeholders; especially owners of critical information infrastructure.

Similarly, The Ghana Cybersecurity Act and the Electronic Transactions Act establishes the industry forum, which brings together all stakeholders in cybersecurity to discuss and deliberate on issues that affect the industry. Therefore, the stakeholders are all aware of the need to enhance cybersecurity and counter cybercrime through effective participation in this forum.

2. **Technical and Procedural Measures**

Both Singapore and Ghana have identified the critical roles that the stakeholders play in countering cybercrime. Private sector not only owns critical infrastructure installation but also provides the technical expertise as expert witnesses in court. Singapore has also put in place mechanisms for licensing cybersecurity compliant organizations. Through licensing and certifications, it is able to effectively assess the compliance status of various enterprises. Moreover, Internet Service Providers provide electronic evidence in a manner that is admissible to the court. Hence facilitating effective prosecution of cybercrime and cybercriminals. The Malabo Convention specifically identifies government, private sector, academia, international bodies and civil society as key stakeholders in countering cybercrime.

3. **Capacity Building**

Capacity building and awareness creation is crucial I countering cybercrime. A whole society approach should be taken in enhancing capacity building. Singapore's capacity building approach is commendable in that it not only involves the general public but also specialized vulnerable groups and government agencies handling sensitive data. Consequently, ensuring awareness on cybersecurity and cybercrime. Moreover, law enforcement agencies in Singapore have partnered with institutions of higher learning to facilitate research and innovation in countering cybercrime.

4. **Organizational Structures**

There is established an independent agency in both Singapore and Ghana that is responsible for coordinating information sharing between government and private industry. This inclusion of critical elements from law enforcement and private sector reduces not only the risk but also the severity of the incidents. Moreover, this focal point provides arrangements for cooperation in a manner that respects the independence of each key stakeholder.

In both Ghana and Singapore, an independent agency has been established to specifically deal with cybersecurity and cybercrime. The UN Draft Convention on use of ICT for Criminal Purposes identifies the UNODC as a key institution for facilitating capacity building and technical assistance in countering cybercrime. Hence, reducing the securitization of the war against cybercrime. As a result, stakeholders are more open to participate in information sharing without suspicion. This level of trust facilitates prompt response to incidents with a view to facilitating effective investigation and prosecution.

5. International Cooperation

An effective stakeholder model ought to include mechanisms for international cooperation. Ghana is a party to both the Malabo Convention and the Budapest Convention. Consequently, it is able to benefit from technical assistance and capacity building program from the Council of Europe to expand its cyber capabilities. Accordingly, it profits from the mutual legal assistance and information sharing capabilities offered by the Conventions. Thus, effectively investigating trans-border cybercrime. Trust is built and enhanced through international cooperation framework as it is more transparent and gives clear parameters for the exchange of information and evidence between different parties.

The mechanisms employed by Kenya towards countering cybercrime have been instrumental in facilitating effective investigation and prosecution of cybercrime. To begin with, there is a robust legal framework that provides both substantive and procedural laws to facilitate cybercrime investigation and prosecution. As a result, there is clarity to both the citizens and law enforcement agencies on the components of cybercrime. Though the National Cybersecurity Strategy 2022 seeks to convert the KE-CIRT into a national multistakeholder CIRT, the existing legal framework neither identifies the stakeholders nor delineates their role in countering cybercrime.

Similarly, the legal framework, establishes a strong institution framework that facilitates effective countering of cybercrime. To begin with, the Constitution establishes independent institutions

empowered to undertake investigation[325], prosecution[326] and adjudication[327] on Cybercrime. Moreover, the Constitution further provides mechanisms for redress to anyone whose right or fundamental freedom is infringed pursuant to a cybercrime investigation, prosecution or adjudication.[328] The National Computer and Cybercrime Coordination Committee is specially mandated to, among others, advice the government on security issues touching on cybersecurity and cybercrime. As such, the members of the Committee are drawn from security agencies. Consequently, cybercrime in Kenya is approached from a security perspective. To bolster effective stakeholder cooperation in countering cybercrime, it is necessary that an independent institution be established to specifically address the issues of cybercrime. Such institution shall also be a focal point for stakeholder engagement for purposes of cooperation, coordination and information sharing towards countering cybercrime.

Regarding international cooperation, Kenya has membership in various international organizations that have thus far facilitated its efforts in countering cybercrime. It has benefited from capacity building initiatives from organizations such as INTERPOL, Commonwealth Association and ITU. Additionally mutual legal assistance agreements have facilitated investigation and prosecution of cybercrime with some countries. Despite there being both regional and conventions of an international nature that are available for ratification, the government of Kenya is yet to ratify the Council of Europe Convention on Cybercrime and the Africa Union Convention on Cybersecurity and Personal Data Protection. As a result, there is need to ratify these Conventions to facilitate international cooperation and collaboration in countering cybercrime. Furthermore, arrangements should be made to ratify the UN Convention on countering the use of Information and Communication Technologies for Criminal Purposes.

[325] Article 244 establishes the National Police Service that is mandated to maintain law and order including through investigation. The National Police Service Act, Section 35 establishes the Directorate of Criminal Investigation that is specially mandated to conduct investigations into criminal conduct. The Directorate has a cybercrime unit that facilitates Cybercrime Investigation

[326] Article 157 establishes the Offices of the Director of Public Prosecutions (DPP)that is mandated to institute and undertake criminal proceedings, including on cybercrime, in all courts in Kenya.

[327] Article 159 vests judicial authority to adjudicate on the judiciary. Article 160 guarantees the independence of the Judiciary.

[328] Article 22 and 23

5.3.Recommendation

States tend to focus on sovereignty, cybercrime and perceived threats to security. In an attempt to address this issue, there is danger of employing disproportionate measures that may limit fundamental rights and freedoms of citizens. On the other hand, civil society organizations may place huge premium on the personal security of individuals hence the need to focus on privacy, freedom of expression, security on the internet and equal treatment of data traffic on the internet. This biased approach to issues of the internet encompass the private companies which tend to focus on cybercrime, protection of company assets. These objectives are mutually inclusive, hence important in achieving an effective multistakeholder model. Effective multistakeholderism can only be achieved if the objectives of the various stakeholders are not only recognized but also proper mechanisms put in place to enhance synergy.

Towards this end, the following are the recommendations for effective stakeholder engagement in combating cybercrime in Kenya:

1. **Legal Measures:** Update the existing legislation on cybercrime to identify stakeholders and enunciate their role in countering cybercrime.
2. **Organizational Structures:** Establish an independent agency to be a focal point for information sharing with stakeholders and to strengthen international cooperation and coordination in countering cybersecurity and cybercrime;
3. **Technical Measures:** There is need for certification and licensing of various enterprises, imports and equipment for cybersecurity. A mechanism should be put in place to assess whether the equipment, services or personnel in various enterprises are cyber compliant. This would be a key strategy and initiative towards prevention and early detection of cybercrime.
4. **International Cooperation:** Ratify relevant international and regional conventions on cybercrime including the Malabo Convention and the Budapest Convention.[329] This would offer a platform for regional cooperation and collaboration for effective investigation and prosecution of cybercrime.

[329]Malabo Protocol, 27th June 2014 available at chrome extension://efaidnbmnnnibpcajpcglclefindmkaj/https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf. Last accessed on 7th March 2023 at 2253 hrs EAT

5. **Capacity Building:** There is need for concerted efforts towards effective capacity building with a view to having all citizens involved in countering cybercrime. The existing capacity building mechanisms can be enhanced to include curriculum initiatives at the elementary level. This would in turn institutionalize cybersecurity at all levels of learning, hence increasing the overall preparedness and awareness of the public in countering cybercrime.

5.4.Conclusion

Complexities in cybercrime continue to pose serious threat to law enforcement efforts towards countering cybercrime. The recognition by States that combating cybercrime is a shared responsibility is the starting point towards efficiency and effectiveness in enhancing cybersecurity. By putting in place effective legal measures, robust organizational structures, adequate mechanisms for international cooperation coupled with technical measures, States can effectively secure themselves from the adverse effects of cybercrime. However, without a robust stakeholder engagement framework, all these initiatives amount to nothing. Kenya should leverage on the existing global goodwill for stakeholder engagement to effectively combat cybercrime. Rather than throw our arms up in despair at the constant changes in the nature and form of cybercrime, the fight offers us an opportunity to refocus our attention on the fundamentals by working with all partners to secure our key networks towards a safe Kenyan cyberspace.[330]

[330] D. Koh, Singapore Cybersecurity Landscape 2021 pg. 5

6.0. BIBLIOGRAPHY

GENERAL REPORTS

US National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework, pg. 79 available at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf last accessed on 25th May 2023 at 1234 hrs.

Global Commission on Internet Governance, "One Internet," Centre for International Governance Innovation and The Royal Institute for International Affairs, (2016) https://www.ourinternet.org/report

INTERPOL Cyberstrategy 2017 Summary pg 2 available at file:///C:/Users/user/Downloads/Summary_CYBER_Strategy_2017_01_EN%20LR%20(2).pdflast accessed on 27th May 2023 at 0120hrs

The Kenya Gazette, Gazette No. 1043; Vol. CXXIV

BOOKS AND JOURNAL ARTICLES

Thomas Holt. Regulating Cybercrime through Law Enforcement and Industry Mechanisms. The Annals of the American Academy of Political and Social Science, September 2018, Vol. 679, Regulating Crime: The New Criminology of Crime Control (September 2018), p. 140 Published by: Sage Publications, Inc. in association with the American Academy of Political and Social Science

Jeeyoung Yun, The criminal Justice Response and Development Strategy in the age of the Fourth Industrial Revolution (II): The Internet of Things and Blockchain, Korea Institute of Criminology and Justice, No. 013 April 2021 at pg. 1.Available at https://www.kicj.re.kr/board.es?mid=a20203000000&bid=0031 Last accessed on 30.06.2023 at 1243hrs

Hutchings, Alice, and Thomas J. Holt. 2015. A crime script analysis of the online stolen data market. British Journal of Criminology 55:596–614

Furnell, Steven. 2002. Cybercrime: Vandalizing the information society. London: Addison-Wesley.

Wall, David. S. 2001. Cybercrimes and the Internet. In Crime and the Internet, ed. D. S. Wall, 1–17. New York, NY: Routledge

Hinduja, Sameer. 2004. *Perceptions of local and state law enforcement concerning the role of computer crime investigative teams.* Policing: An International Journal of Police Strategies and Management 3:341–57.

Barlow, John Perry. "*A Declaration of the Independence of Cyberspace."* (1996). Available at https://wac.colostate.edu/ rhetnet/barlow/barlow_declaration.html

Sivasubramanian Muthusamy, "*Building Suitable Frameworks for Internet Governance" in Collaboratory Discussion Paper: Internet Policymaking, Multistakeholder Internet Dialog (2013), 81.* Available at http://www.collaboratory.de/w/Building_Suitable_Frameworks_for_Internet_Governanc _The_Interplay_ between_Technology_and_Policy

Haris Glekkmann, *Multistakeholder Governance and Democracy*: A Global Challenge (Routledge 2018)

Gauthier, David, 1986. *Morals by Agreement*, Oxford: Clarendon Press.

Scanlon, Thomas, 1998. *What We Owe to Each Other*, Cambridge, MA: Harvard University Press.

Mendina, Johannes Britz, *Information Ethics in the Electronic age: Current issues in Africa and the world*, 2004 pg. 164 Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=907483 last accessed on 13th July 2023 at 1317 hrs

Dr. Rizgar Mohammed Kadir, "*The Offense of Unauthorized Access in Computer Crimes' Legislation - A Comparative Study"* Journal of Sharia & Law,2008

Aravinth Balakrishnan,"*Cyber Stalking:Challenges in regulating cyberstalking at the cyberspace"* Available at https://www.legalserviceindia.com/legal/article-214-cyber-stalking-challenges-in-regulating-cyberstalking-at-the-cyber-space.html<accessed on 02/08/2022>

Holt, Thomas, J., Adam M. Bossler, and Kathryn C. Seigfried-Spellar. (2018). *Cybercrime and Digital Forensics*, 2nd edition. Routledge.

MUTIJIMA Asher Emmanuel, *The Role of Academia in Cyber Crimes Prevention, International Journal of Innovative Science and Research Technology* ISSN No:-2456-2165

J. Dache, MBS, The State of Cybercrime: *Current Issues and Countermeasures* Pg. 28Available at https://www.eff.org/issues/un-cybercrime-treaty#:~:text=The%20proposed%20Convention%20will%20likely,human%20rights%20and%20procedural%20safeguards. Last accessed on 5th April 2023 at 3.13pm EAT

R. Boateng et al, *Cybercrime and Criminality in Ghana*, Journal of Information Technology Impact,Vol. 11, no.2, pg. 85

K. Adu & DF. Allen, Learning from Ghana's Multistakeholder Approach to Cyber Security, January 2023 Available at https://africacenter.org/spotlight/ghana-multistakeholder-cyber-security/#:~:text=These%20improvements%20allowed%20Ghana%20to,sponsored%20Malabo%20Convention%20in%202021.

Jackson L. Goldsmith, *Against Cyberanarchy*, The University of Chicago Law Review, vol 65 (1998) p. 1200

R. Sabillon et al, *Cybercrime and Cybercriminals: A Comprehensive Study*, International Journal of Computer Networks and Communication Security, vol 4, 2016

B. Arief and M. Azeem, *Understanding Cybercrime from its Stakeholder's Perspective*, Defenders and Victims, Newcastle University, 2015
Wall David, *Digital Realism and the Governance of Spam as Cybercrime*, vol.10 European Journal of Criminal Policy and Research, 2004

Jeremy Bentham, *Anarchical Fallacies*, vol. 2 of Bowring (ed), Works 1843

Europol and Eurojust, *Common Challenges in Combating Cybercrime*, 2019 Joint Report p. 17

ONLINE RESOURCES AND LINKS

https://sherloc.unodc.org/cld/en/education/tertiary/cybercrime/module-1/key-issues/cybercrime-trends.html last accessed on 22nd May 2023 at 01.01pm

https://www.unodc.org/e4j/en/cybercrime/module-5/key-issues/reporting-cybercrime.html#:~:text=Existing%20research%20identifies%20several%20reasons,is%20a%20business%2C%20loss%20of

https://www.csoonline.com/article/567307/why-businesses-don-t-report-cybercrimes-to-law-enforcement.html

https://www.interpol.int/en/Who-we-are/What-is-INTERPOL last accessed on 25th May 2023 at 0100pm

https://www.interpol.int/en/Crimes/Cybercrime/Cybercrime-Collaboration-Services last accessed on 25th May 2023

https://www.interpol.int/en/Crimes/Cybercrime/Awareness-campaigns last accessed on 25th May 2023 at 01.27 pm

https://www.interpol.int/en/News-and-Events/News/2022/Cyber-enabled-financial-crime-USD-130-million-intercepted-in-global-INTERPOL-police-operation Last accessed on 25th May 2023 at 02.16 pm

https://www.interpol.int/en/News-and-Events/News/2019/Kenya-first-African-country-to-connect-to-the-International-Child-Sexual-Exploitation-database last accessed on 13th July 2023 at 1230 hrs

https://www.verizon.com/about/blog/ispmeaning#:~:text=An%20internet%20service%20provider%20(ISP)%20is%20a%20company%20that%20provides,mobile%20carriers%2C%20and%20telephone%20companies. last accessed on 13th July 2023 at 1239 hrs

www.internetsociety.org/what-we-do/internet-issues/internet-governance last accessed on 7th February 2022 at 1923hrs

https://www.unodc.org/e4j/en/cybercrime/module-1/key-issues/cybercrime-in-brief.html last accessed on 18th May 2023 at 1032 hrs

https://www.unodc.org/documents/data-and-analysis/tocta/10.Cybercrime.pdf< accessed on 28/07/2022>
https://www.bbau.ac.in/dept/Law/TM/1.pdf< accessed on 28/07/2022

https://www.researchgate.net/publication/228188863_The_Role_of_ISPs_in_the_Investigation_of_Cybercrime Last accessed on 13th July 2023 at 1304hrs

https://www.gp-digital.org/multistakeholderism-the-missing-cyber-norm/ last accessed on 15th March 2023 at 01.18 pm

http://kenyalaw.org/caselaw/cases/view/209135/

https://ccdcoe.org/organisations/au/ on 11th April 2023 at 10.00am

https://au.int/sites/default/files/treaties/29560-sl AFRICAN_UNION_CONVENTION_ON_CYBER_SECURITY_AND_PERSONAL_DATA_PROTECTION_0.pdf last accessed on 11th April 2023

https://au.int/en/pressreleases/20180412/african-union-commission-and-council-europe-join-forces-cybersecurity last accessed on 14th July 2023 at 1231hrs

https://www.ca.go.ke/industry/cybersecurity/overview/#:~:text=The%20Kenya%20Information%20and%20Communications,national%20cyber%20security%20management%20framework. Last accessed on 18th April 2023

https://nc3.go.ke/roles-and-responsibilities/ last accessed on 18th April 2023

https://nc3.go.ke/services/information-sharing/ last accessed on 18th April 2023

https://repository.kippra.or.ke/handle/123456789/3580 last accessed on 12th April 2023

https://ccdcoe.org/incyder-articles/asean-cyber-developments-centre-of-excellence-for-singapore-cybercrime-convention-for-the-philippines-and-an-open-ended-working-group-for-everyone/ last accessed on 15th March 2023 at 1203 pm

https://www.meltwater.com/en/blog/social-media-statistics-singapore last accessed on 30th June 2023 at 1507 hrs

https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/Singapore_statement.pdf

https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/Singapore_statement.pdf last accessed on 15th March 2023 at 12.32 pm

Cybersecurity Act (csa.gov.sg) last accessed on 13th April 2023 at 3.22pm

https://www.fticonsulting.com/~/media/Files/apac-files/insights/white-papers/singapore-cybersecurity.pdf page 1 last accessed on 15th March 2023

Singapore Updates National Cybersecurity Strategy (aseantechsec.com) last accessed on 13th April 2023 at 2.23pm

https://africacenter.org/spotlight/ghana-multistakeholder-cybersecurity/#:~:text=These%20improvements%20allowed%20Ghana%20to,sponsored%20Malabo%20Convention%20in%202021. Last accessed on 17th April 2023 at 1.47pm EAT

https://www.bbau.ac.in/dept/Law/TM/1.pdf< accessed on 28/07/2022>

https://www.unodc.org/e4j/en/cybercrime/module-1/key-issues/cybercrime-trends.html#:~:text=The%20main%20legal%20challenges%20to,authorities%20can%20access%20digital%20evidence last accessed on 13th September 2023 at 1424 hrs.

https://www.agc.gov.sg/docs/default-source/newsroom-doucments/Speeches/ag's-speech-for-11th-capgc.pdf last accessed on 23.11.2023 at 1304 hrs

National Cybercrime Action Plan Singapore available https://www.mha.gov.sg/docs/default-source/media-room-doc/ncap-document.pdf last accessed on 24.11.2023 at 1101 hrs

https://law.nus.edu.sg/asli/pdf/WPS001.pdf last accessed on 23.11.2023 at 0041hrs