UNIVERSITY OF GHANA

COLLEGE OF HUMANITIES

STATE RESPONSE TO CYBER THREATS IN AFRICA: AN EXAMINATION OF GHANA'S CYBERSECURITY STRATEGY.

BY

GIDEON NLIBE BILIJOE

(10551092)

THIS THESIS IS SUBMITTED TO THE UNIVERSITY OF GHANA, LEGON IN PARTIAL FULFILMENT OF THE REQUIREMENT FOR THE AWARD OF PhD IN INTERNATIONAL AFFAIRS DEGREE.

MARCH, 2024

DECLARATION

I, GIDEON NLIBE BILIJOE, hereby declare that with the exception of the quotes, ideas and analysis attributed to duly acknowledged sources, this study is the result of a research I conducted under the supervision of DR. AMANDA JENNIFER COFFIE, DR. PHILIP ATTUQUAYEFIO and DR. FESTUS KOFI AUBYN.

GIDEON NLIBE BILIJOE

(CANDIDATE)

.....

DATE: 10-04-2024

DR. AMANDA JENNIFER COFFIE

(SUPERVISOR)

.....

DATE: April 10, 2024

DR. PHILIP ATTUQUAYEFIO

(COMMITTEE MEMBER)

.....

DATE: April 10, 2024

DR. FESTUS KOFI AUBYN

(COMMITTEE MEMBER)

.....

DATE: 10/04/2024

ABSTRACT

The dawn of the internet-based digital era has connected global communication in the last two decades and made cyberspace more mobile, shared and integrated into human lives. However, the security concerns associated with cyber technology have engendered its securitization. Response mechanisms towards cyberspace management have equally witnessed global recognition, with developing African states not being the exception. Given the critical role of the state in this management process, Ghana has fashioned out strategies aimed at managing the space, and the extent to which the strategy adequately addresses this objective constituted the central question for

By adopting the structuration paradigm of knowledge construction and the neo-institutionalism theoretical framework and utilizing a qualitative research approach with both primary and secondary data, the study made some important findings.

Significantly, the study found that but for the dominant cybersecurity threats, the African cyber ecosystem in general and specifically Ghana, is not distinct from the general cyber ecosystem. Cybercrime, social engineering, distributed denial of service, insider-related threats, ransomware and data breaches are identified as the major cybersecurity threats in Ghana. The study further revealed that the Ghanaian state cyber management features domestic regulatory and institutional setups, as well as international and domestic collaborative mechanisms. Again, it showed that despite the gains afforded by Ghana's cybersecurity promotion, there have been some challenges. Key among these are the predominant anti-cybersecurity socio-cultural practices in the country, funding inadequacies, cyber skills and infrastructural gaps and lack of cyber awareness.

Theoretically, the study also established the need to consider both the domestic peculiarities, which comprise norms (formal and informal), and formal international structures for States' cyber threats

management. This conclusion is in sync with the core structuration philosophical paradigm and the neo-institutionalism theory's call for attention to dual structures in knowledge construction and understanding.

Based on the findings, the study recommended continued regional and domestic collaborations, a revision of Ghana's cybersecurity management and implementation strategies by incorporating both formal and informal institutional mechanisms and the development of response strategies that consider local threat dynamics.

DEDICATION

To all who aspire to make an impact in their worlds.

ACKNOWLEDGEMENT

I want to begin by expressing my heartfelt gratitude to Almighty God for His endless favors and love that surround me. Next, I would like to sincerely thank my parents for their encouragement and support throughout this journey. I also extend my appreciation to my ministers of God and pastors for their guidance and words of life throughout this journey. To my siblings, I recognise the deep gratitude I owe you all. I can only say, God bless you for the sacrifices you have made for me.

The list can certainly not end without mentioning my Supervisory Committee: Dr Amanda Coffie, Dr Philip Attuquayefio and Dr Festus Aubyn, who tirelessly helped go through this work to make it presentable. To the venerable Professor Kwame Boafo-Arthur, a million thanks is not enough. You have been a father figure who has always been there for me. Your encouragement and sturdy trust in me have been more than a fountain of motivation. I am proud and grateful to have received your tutelage, sir.

To the Director of LECIAD, Professor Emmanuel and all faculty members, I say thank you. I also would like to seize this opportunity to express my profound gratitude to Dr. and Mrs. Isaac Owusu Mensah for your immense roles in my educational journey. Finally, to my coursemates, I say thank you all for your brotherly care and love throughout the time of our being together.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

ACSS - African Centre for Strategic Security

AfricanCERT - Computer Emergency Response Team

AFRIPOL - African Union Mechanism for Police Cooperation

AITI-KACE - Ghana-Indian Kofi Annan Centre of Excellence in ICT

APT - Advanced Persistent Threats

AU - African Union

AUCSEG - African Union Cyber-Security Expert Group

BEC - Business Email Compromise

CCI - Commonwealth Cyber Initiative

CERTs - Computer Emergency Response Teams

CFCS - Centre for Cyber Security

CID - Criminal Investigation Department

CIPESA - Collaboration on International ICT Policy for East and Southern Africa

CIS - Centre for Internet Security

CMM - Capacity Maturity Model for Nations

COMESA - Common Market for Eastern and Southern Africa

CS - Cluster Sampling

CSA - Cyber Security Authority

CSEAG - Cyber Security Experts Association of Ghana

CSIRTS - Computer Security Incident Response Teams

CSOs - Civil Society Organisations

DDoS - Distribution Denial of Service

DFI - Digital Forensic Investigation

DoS - Denial of Service

EAC - East African Community

ECCAS - Economic Community of Central African States

ECOWAS - Economic Community of West African States

ENISA - European Union Agency for Network and Information Security

EOCO - Economic and Organised Crime Office

EU - European Union

GAF - Ghana Armed Forces

GCSCC - Global Cyber Security Capacity Centre

GSS - Ghana Statistical Service

GTBank - Guaranty Trust Bank

HIPAA - Health Insurance Portability and Accountability Act

HMG - Her Majesty's Government

ICANN - Internet Corporation for Assigned Names and Numbers

ICT - Information and Communications Technology

IEC - International Electrotechnical Commission

IGE - International Governmental Executives

IMPACT - International Multilateral Partnership Against Cyber Threats

IR - International Relations

IRT - Insider Related Threat

ISC2 - International Information System Security Certification Consortium

ISD - Information Society Division

ISO - International Standards Organisation

ITU - International Communication Union

KAS Konrad Adenauer Stiftung

LECIAD - Legon Centre for International Affairs and Diplomacy

LI -	Legislative Instrument
MFWA -	Media Foundation for West Africa
MISA -	Media Foundation for Sothern Africa
NCA -	National Communications Authority
NCPF -	National Cybersecurity Policy Framework
NCS -	National Cyber Security
NCSPS -	National Cyber Security Policy and Strategy
NCSS -	National Cyber Security Strategies
NERC-CIP -	North American Electric Reliability Corporation Critical Infrastructure Protection
NIST -	National Institute of Standards and Technology
NITA -	National Information Technology Agency
OCWAR-C -	Organised Crime: West African Response on Cybersecurity and Fight Against Cybercrime
OECD -	Organisation for Economic Co-operation and Development
PoC -	Points of Contact
QCA -	Qualitative Content Analysis
RCM -	Rational Choice Model
SADC -	Southern African Development Community
SOC -	Service Organisation Control
SRS -	Simple Random Sampling
SS -	Stratified Sampling
SS -	Systematic Sampling
STC-CICT -	Specialized Technical Committee on Communication and Information Communications Technology

UK -	United Kingdom
UN -	United Nations
UN EGDIS -	United Nations E-Government Development Index Surveys
UNCTAD -	United Nations Conference on Trade and Development
UNGA -	United Nations General Assembly
UN GGE -	UN Group of Governmental Experts
UNHRC -	United Nations Human Rights Commission
UPSA -	University of Professional Studies, Accra
WSIS -	World Summit on Information Society

CHAPTER ONE

INTRODUCTION

1.0 BACKGROUND TO THE STUDY

Security constitutes an indispensable objective in states affair and remain central in International Relations (IR) discourse (Herrington, 2013; Barkawi & Laffey, 2006, p.329; Kolodziej, 2005). Notwithstanding its ubiquity and significance, diverse perspectives exist on its meaning and why/how states seek it (Peou, 2021; Baldwin, 1997). These contestations about the concept have lingered among security scholars and theorists, resulting in a forest of literature.

A paradigm shift in the meaning of the security concept emerged with the turn of the Cold War. A broader definition of the concept beyond the national security that bothered mainly on the state gained much momentum during this era. Threats from issues previously perceived as falling outside the scope of security but which were increasingly challenging the survival of countries and the people living within them, became a core consideration (Attuquayefio, 2012, p.88). This sharp departure from the realists' inclined viewpoint got termed as the concept of human security. The concept aimed to bring into the security discourse an alternative design to understanding such emerging security threats to states citizens and the appropriate approaches for discussing them. While the scope of the specific threats contributing to human insecurity remains indeterminate, agreement over the importance of making people the referent object has been far-reaching among its proponents (Attuquayefio, 2012, p.89; Baylis, 2008, p.496). In the broader security discourse, the threat to the security of citizens who are the ultimate beneficiaries of a safe state and the fact that most of the threat elements to states' citizens emanate from non-traditional sources offer this school of thought much credence even amid the continual recognition of the state as an essential

level of analysis in security governance (Attuquayefio, 2012, p.89; Tankebe, 2008, p.67). In other words, contemporary security concerns at both national and international levels involve multiple domains (Newman, 2010; Hirsch et al., 2020). The dangers associated with the internet as a driver of globalisation have, thus, acquiesced cyberspace and its threats into this broader domain of security conceptualisation (Newman, 2022, p.431; Baylis, 2008, p.496).

The dawn of the internet-harnessed digital era in the international system has seen significant improvement in global communication in the last two decades and made cyberspace more mobile, shared and integrated into human lives (Savaş & Karataş, 2022). Innovations in cyber technology, coupled with their affordability and accessibility, have increased internet availability, usage and performance and consequently boosted its user community numerically. The various facets of individuals, governments and non-governmental entities' lives, spanning economic, commercial, socio-cultural, are now conducted within cyberspace worldwide (Aghajani & Ghadimi, 2018). For example, the global supply chain has witnessed a significant boost due to the improvement of consumers' access to various goods, products, and information through cyberspace. This essential role has placed cyberspace at the heart of states' political, economic and social development agendas. It has interwoven different aspects of citizens' lives such that a threat to one facet affects several others (Li et al., 2020). Deductively, a breakdown of mobile networks in contemporary times, for instance, not only truncates communication flow but also affects the usage of telecommunication-driven financial products like mobile money and online banking. Similarly same occurrence could also shut off energy-controlled systems and plunge a region or country into darkness.

It is imperative to indicate that, notwithstanding the fortunes associated with the cyberspace, its development is accompanied by new vulnerabilities, risks and challenges to individual users and

national security (Reveron & Savage, 2020; Domingo, 2016, p.246). The low cost of entry and loopholes in the space are often exploited by governments, individuals, organised crime and terrorist groups in conducting cyber warfare, cybercrime, cyber terrorism and cyber espionage. These constitute worrying developments that presents the space as a top security threat haven of the 21st century (Bullock et al., 2021; UNGA, 2010, p.2). Moreover, unlike traditional national security threats, which have governments and nations as actors and impacts limited to defined territorial boundaries, cyber threats are diverse with far-reaching effects (Sarker, 2021). Their transboundary penetration and operations, which defy the immunity of states (Muller, 2015, p.4) and capability to shutter states' economies and cause destruction through remote attacks, have resulted in states instituting processes towards securitizing the space (Shin et al., 2021; Snehi & Bhandari, 2021; Ahmed et al., 2021).

Following the increasing cyber threats and vulnerabilities concerns, policymakers and academics have attended to threat mitigation and cyber usage norm formation discourse (Domingo, 2016, p.246; Brito & Watkins, 2011). Governments' concern about systems and infrastructure susceptibility to espionage, critical state information compromises and criminal or hostile cyber activities such as bugging and hacking have also prompted the adoption of holistic redress mechanisms. These efforts have manifested in national and international policy approaches and infrastructural response mechanisms (Graham et al., 2016; Libicki, 2021; and Buja, 2021). States and international organisations have also framed and implemented medium to long-term policies and programs tailored to address cyberspace challenges.

The foremost binding international attempt to address cyber threats emerged with the 2001 Budapest Convention on Cyber Security (the Budapest Convention). The Budapest Convention inspired the formation of regional cyber security frameworks, including the European Union

Agency for Network and Information Security (ENISA) (Seger, 2016). The extension of this development saw the enactment of the Cyber Security Act and the EU digital certification scheme that mandates and empowers ENISA in its operational cooperation and crisis management across Europe (European Commission, 2022). The United Nations General Assembly, on its part, has also engaged in discussions on cyber-related issues through its ad hoc intergovernmental committees, leading to the birthing of crucial resolutions such as the 2021 Resolution A/75/L.87/Rev1 for countering criminal use of information and communication technologies (UNGA, 2021, p.1). Its International Governmental Executives (IGE) have similarly been instrumental in designing strategic plans for cyberspace management (Walker & Ian Tennant, 2021). Cyber-related international organisations have also been crucial in this development by providing their member states with early warning systems and aiding them in the adoption of efficient cyber security policies and infrastructure through programs such as the ITU's IMPACT and the Commonwealth Cyber Initiative (CCI) (Ministry of Communications, 2015, p.6). In Africa, the AU has institutionalised the African Union Convention on Cyber Security and Data Protection (the Malabo Convention) to address the threats and enhance cyber users' rights and safety (AU, 2014). The Malabo Convention also mandates AU member states to improve their cyber safety with policy frameworks with domestic policies.

Inspired and obligated by provisions of the various treaties and desiring to safeguard their cyberspaces and interests, states across regions have initiated country-level cyber security policy responses (Turianskyi, 201; Kshetri, 2010, p.1064). While these responses are influenced by different orientations and capabilities, leading to variations in cyber governance frameworks and strategies, they all seek to address the prevailing cybersecurity threats in these countries (Kshetri, 2010, p.1064).

Africa's unsavoury label as a cyber threats and crimes hub (Kshetri, 2019) and the quest to maximise the opportunities of the space for development triggered state and regional bodies' actions. The AU's Malabo Convention and the ECOWAS Directive on Fighting Cybercrime are among the regulatory responses by the regional and sub-regional bodies. A number of the states have ratified these and other international cyber conventions and protocols and attempted to domesticate the same as national policies and strategies aimed at securing cyberspace (Interpol, 2021; Kshetri, 2019, pp.77-79).

Ghana is among the few African countries that have ratified all the major international and regional cybersecurity protocols and drafted national policies and strategies as it seeks to maximise the benefits of cyber technology. The state's accelerated internet penetration, access and digitalisation drive have influenced the quest for cyberinfrastructure development and a nuanced framework to govern the cyber ecosystem (Motiwala, 2017). Ghana has made significant investments towards the realisation of this feat. Among these is a multi-million dollar 600-rack National Data Centre, the largest in West Africa. The state has also successfully rolled government sectors and ministries onto internet interconnectivity through fibre optic rings. Again, its 13 million internet subscribers in 2017 rose to 23.5 million, thus almost doubling at the beginning of 2023 (Kemp, 2023 & Motiwala, 2017).

It is worth revealing that the above developments have manifested alongside a heightening in the manifestation of cyber threats in the country. The many naïve cyber users, which soared further in the wake of the COVID-19 pandemic with increased activities on the internet, aggravated the country's cyber threat rates (Nyavor, 2014, NCA & GSS, 2020, p.23; Opoku-Afari, 2021). The Ghanaian state has, however, not relented in safeguarding its cyberspace and users. This determination has manifested in establishing governing and management mechanisms for the

space. The drafting of a National Cyber Security Policy and Strategy, a Cyber Security Act with other subsidiary cyber legislations such as the Data Protection Act and the National Signals Bureau Act, and a regulatory Authority (Cyber Security Authority) have all since been established. While the Authority's mandate involves the managerial oversight of the space, the Act functions as the regulatory legal framework for its activities (CSA, 2020). These actions and interventions constitute Ghana's policy strategies and frameworks towards addressing its 21st-century cyber security threats and sanitising its cyber ecosystem and serve as the background to this study.

1.1 STATEMENT OF THE PROBLEM

The digital revolution encompassing data collection, communications, and management of economic and political processes has presented both incredible opportunities and serious vulnerability challenges (Ndungu & Signé, 2020; Betz & Stevens, 2011). Against this background is the call for appropriate actions at both national and international levels to address the nagging security concerns within the space. The calls for such measures in Africa have been very inviting because of the continent's unsavoury tag as a cyber threat hub (Interpol, 2021; Kshetri, 2019, pp.77-79).

Like many other sister countries, Ghana, having been cited among the top-ranking cybercrime-originating countries (FBI, 2013), set its sights on maximizing the opportunities of cyberspace and minimizing its threats. This resolve occasioned several efforts, including the ratification of the Budapest Convention on Cyber Crime and the AU Convention on Cyber Security and Personal Data Protection as international and regional protocols, respectively (Guermazi, 2021; Adu-Amanfoh & Allen, 2023, p.1; Council of Europe, 2023).

The fast-paced innovations in cyberspace have also influenced several domestic efforts by the state to complement the provisions and dividends offered by international protocols and treaties (GOG, 2015; Adu-Amanfoh & Allen, 2023). Several legislations, policies, and institutional setups have hence been provided in Ghana (Adu-Amanfoh & Allen, 2023, p. 1; Council of Europe, 2023). The National Cybersecurity Policy and Strategy, which constitutes one such, offers the baseline framework of strategies for the country to ensure a secure and stable connected internet community. Its ultimate objective is to ensure that Ghanaians can use the internet to work and create wealth in a safe cyberspace and enhance the state's security in the cyber-characterized international system. Indicators of cybersecurity enhancement requirements, such as a well-functioning professional cyber community, protective infrastructure of global standards for swift cyber concerns response, and up-to-date legislation enactments for adjudicating possible conflicts within the cyber ecosystem, have been essential suggestions in the strategy (Ghana National Cyber Security Policy, 2015, p.21).

Despite these efforts in Ghana's management strategies and frameworks, which have earned it the international community's plaudits, cyber security threats have continually manifested within its cyber ecosystem. The danger of such threats to national and human security and their evolving nature have required continual solution-driven examinations (ITU, 2020; p.28, Adu-Amanfoh & Allen, 2023; Ghana Chamber of Communication, 2020). The continual threat manifestations exemplified by indicators such as the mounting figures reported by the 2018, 2019, and 2020 Banking Industry Fraud and Points of Contact (PoC) Reports, reaffirms this phenomenon. The 2,295 reported cybercrime figure of 2019 signified an increase of 120 cases from the previous year's (Bank of Ghana, 2019). Again, between October 2019 and October 2020, the Cybercrime Incident Reporting Points of Contact (PoC) data subsequently published 11,550 cybercrime cases

(Ghana Chamber of Communication, 2020). While this sharp rise could be attributable to the operationalization of the Cyber Reporting Point of Contact and the expansion of focus areas beyond the financial sector, the levels are still indisputably high and concerning. A projection by cyber experts of the likelihood of the situation spiralling in the coming years further asserts the pervasiveness of the phenomenon in the country (World Economic Forum, 2023; Nartey, 2023).

From the above, the bewildering question is, to what extent has Ghana's cybersecurity response strategy adequately and effectively responded to its cyber security concerns of a 21st-century cyber ecosystem? This question is critical considering the alarming rates of cyberattacks' and their effects on national security, socio-economic development and citizens' security. It is also timely because of the relatively little attention such development has received within the cybersecurity literature in Africa and Ghana. Thus, while there is no attempt to suggest that Ghana's cyber ecosystem is not studied, it is the position of this thesis that much of the existing literature has not considered a holistic examination of the country's response strategy and reflected on the combined effect of the framework, its implementation and practice. For instance, Forson-Adaboh (2022), Agbeko (2021), Affum (2019), Adu & Adjei (2018), and Botchwey (2018) have examined cyber awareness and perceptions in the country. Others, such as Baylon and Antwi-Boasiako (2016), Warner (2011) and Motiwala (2017), concentrated on profiling the country's cyber threats. Those that came close to examining the state's cybersecurity threat response strategy, which relates to the central objective of this study, are Apau and Koranteng (2020) and Ouassini and Amini (2021). However, their studies scope limited them to examining only the country's cyber security capabilities and legal reforms, respectively. Lebogang et al. (2022) equally attempted a study of Ghana and other African countries national cyber security strategies and also had their objective limiting them to how those strategies met the ITU cyber security management standardization. This focus therefore

sidestepped the domestic dynamics and their implications on the cybersecurity management process.

Based on these broad considerations, this study attempts to address this gap by examining Ghana's cybersecurity ecosystem as a case study. In line with this task, the central objective advanced in this study is an examination of the adequacy and effectiveness of Ghana's cybersecurity response strategies in the face of cyber threats in its 21st-century cybersecurity ecosystem.

1.2 RESEARCH OBJECTIVES

The specific objectives of the study are to:

1. Examine Africa's cybersecurity threat landscape and the associated continental/sub-regional responses.
2. Assess the specific cybersecurity threats of Ghana as a developing African state.
3. Discuss Ghana's responses to addressing its cyber security threats/challenges.
4. Analyse the adequacy and effectiveness or otherwise of the structures and norms in Ghana's cybersecurity strategies for addressing her 21st-century cybersecurity threats.

1.3 RESEARCH QUESTIONS

1. What is the nature of the African cybersecurity threat landscape, and how have developing African states responded to their cybersecurity threats?
2. What are the specific cybersecurity threats in Ghana?
3. How has the Ghanaian state responded to addressing its cyber security threats/ challenges through the provision of structures and norms?
4. How adequate are Ghana's cyber security strategies in responding to the cybersecurity threats of the 21st century cyber ecosystem?

1.4 SIGNIFICANCE OF THE STUDY

This empirical study is relevant for International Relations scholars, security scholars, analysts and state policymakers. For IR scholars, the study highlights the behaviour of developing countries in policy response to issues of international concern and their rippling effects. In terms of International Security, the study provides an understanding of how Ghana and, by extension, African states have fared in managing their cybersecurity space and its security implications for each state and the international community. Political scientists also get to appreciate the role of institutions in managing cyber security and the effects of cybersecurity threats and management on domestic political outcomes. Finally, the study contributes to our understanding of cybersecurity as a nagging security issue of the 21st century and provides insight into the growing cybersecurity literature in Ghana.

1.5 SCOPE OF THE STUDY

This study assesses how developing African states have responded to managing their cybersecurity threats, with Ghana as a case study. While the focus is on Ghana as the case study, applicable examples from other African states and the combined efforts by African states were drawn to help advance the discourse. The scope of the study thus encompasses an understanding of developing African states' threat landscape and response strategy since 9/11, which has witnessed a massive evolution from a virtual standpoint attack and dovetails into the Ghanaian experience and situation.

The choice of Ghana as a case for the study is influenced by several factors, including the country's being among the few African states that have ratified all the major international cybersecurity treaties/conventions. Statistically, it forms part of the 12 African states with a national cybersecurity strategy and incident response capabilities. It is also one of the four states that have ratified the two international treaties addressing international dimensions of cyber threats (the

Budapest and Malabo Conventions) and one of nine African countries that are members of the UN Group of Governmental Experts (UNGGE) (Adu-Amanfoh & Allen, 2023, p.1; van Raemdonck, 2021, p.33). The country has also distinguished itself with a Cyber Security Act and Cyber Authority to manage its cyberspace and other cybersecurity-related issues. It again has a National Cybersecurity Policy and Strategy that defines the country's visions and strategic approaches to managing cyberspace.

It is worth noting that Ghana's cybersecurity initiatives are particularly noteworthy in the current landscape, where many African states have yet to establish foundational cybersecurity policies. In this context, Ghana has emerged as a leader in cybersecurity management on the continent, setting a precedent for other nations. The Ghanaian ecosystem, therefore, serves as a crucial reference point for evaluating the effectiveness of deployed cybersecurity strategies.

1.6 THEORETICAL FRAMEWORK

An essential aspect of academic research lies in simplifying the somewhat complex constructs of linked prepositions through theoretical concepts (Kaufman, 2013, p.31). While several theoretical constructs for such a task exist in IR, this study employed the Neo-Institutionalism framework for its analysis.

1.6.1 Theory in International Relations (IR)

The core of IR studies relates to the theoretical elucidations on states' behaviour (Hudson, 2005; Peou, 2021, p.1; Burchill & Linklater, 2005, p.4). The Realists' famed classical propositions of physical survival, power politics and its attendant zero-sum game outturns and the state as the leading actor in the international system constitute one breath of this explanation (Burchill & Linklater, 2005, p.4). Their proposition of the nation-state (state) as the principal actor in

international relations did indicate that it existed with other bodies (organisations, institutions, individuals) which commanded but limited power (Antunes & Camisao, 2017, p.15). Liberals who rebuffed the theoretical potency of realism concerned themselves with creating institutions to protect individuals and their freedom by limiting and controlling political power (Meiser, 2017, pp.22–25). Much of the liberals' scholarship focused on international organisations and how they foster cooperation by providing states with more incentives that lure them against absolving from international agreements, otherwise termed neoliberal institutionalism or neoliberalism (Meiser, 2017 pp.22–25).

Regarding constructivism, whose central thesis argues that reality is not fixed but subject to change, institutions play vital roles in how things turn and run in the international system. As noted by Theys' "reality" is shaped by actions and interactions and their resultant thoughts and actions construct international relations (Theys, 2017 p.41). With constructivism, therefore, states' behaviour explains not only the distribution of material power, wealth and geographical condition but also ideas, identities and norms (Theys, 2017, p.41). The international society concept of the English school or constructivism, which is concerned with creating and maintaining shared norms, rules, and institutions to guide behaviour, puts institutionalism at the centre of international relations (Stivachtis, 2017, p.28). From the above meta-theories, institutions and institutionalism remain central in understanding how systems function and shape or affect state policies, including security, at both domestic and international levels (Bodnieks, 2020, p.84).

1.6.2 The Origin of the Neo-Institutional Theory

Neo-institutionalism evolved from the weaknesses identified with institutional theory. Institutional theory, applied variously in political science and international relations to describe constitutions, legal systems, and government structures, dates back to the 1960s and 1970s behavioural

revolution discourse that attempted to understand individuals' actions and their determinants. It projected that such actions were not entirely limited to structures, as was popularly held at the time (Lowndes, 2002, p.90). The Rational Choice Model (RCM), which influenced most of the 1980s analytical discourse, assumed politics as the interplay of individuals' self-interests with people doing what they generally believed guaranteed their overall best interest in the space of several courses of action (Lowndes, 2002, p.95). By the 1980s, institutionalism emerged with a consideration of structures as contributing to the actions of states and their actors in political science and was similarly deployed in other disciplines (Scott, 2005, p.2). Divergent perspectives and variants, including old/traditional and neo-institutionalism, emerged as the deployment of the idea as a theoretical construct continued.

1.6.3 The Traditional Institutionalism

Institutional theory attends to the deeper and more resilient aspects of social structure. It considers the processes by which structures, including schemas, rules, norms and routines, become established as authoritative guidelines for social behaviour (March & Olsen, 1989, p.2). It enquires into the creation, diffusion, and adoption over time and space of these elements, as well as how they fall into disuse and decline (Scott, 2006, p.2). Institutions, on the other hand, references the regular, stable, recurring patterns of behaviour.

Institutionalism connotes a general approach to studying political institutions, a set of theoretical ideas and hypotheses concerning the relations between institutional characteristics and political agency, performance and change (Scott, 2006, p.2). "Institutionalism" specifically examines how institutions structure social and political behaviour (North 1990). The literature on the concept argues that policy, politics, and behaviour can only be understood in the context of the institutions in which they occur. The approach covers the rules, procedures and formal organisations of

government and governance and the employment of law and historical tools for the explanation of constraints on both political behaviour and democratic development (Lowndes, 2002, p.92).

1.6.4 Characteristics of Traditional Institutionalism

In the 19th and early half of the 20th centuries, political science had traditional institutionalism as its basis. Its characteristics included structuralism, legalism, holism, historicity and normality. Law emerged as a major characteristic of traditional institutionalism, which offered it a central role in the governance of states (Peters, 2005, p.6). Law, thus, constituted the basis for the framework of the public sector and a major way through which government affects the behaviour of citizens and shapes national affairs effectively (Peters, 2005, p.7).

Secondly, traditional institutionalism views structures as important determiners of behaviour (Peters, 2005, p.8). In talking about structure, old institutionalism focused on major institutional features of the political system. To obtain their desired variations, old institutionalists also relied on comparative analysis of political systems and holism, focusing on constitutions and formal structures (Peters, 2005, p.9). It also oriented its scholars towards comparing whole systems rather than selective institutional or system units' analysis.

Furthermore, traditional institutionalists analysed political institutions within the socio-economic conditions and the historical development context they operated within (Peters, 2005, p.10). To them, the knowledge of how political systems function was based on researchers' understanding of the developmental trajectory which produced the system. Moreover, political elites' behaviour, argued the proponents, was a function of their collective history, and so people's history constituted a solid basis for understanding their politics (Peters, 2005, p.10). Clearly, this characteristic of the approach affirmed its strong normative undertones and given that political

studies had normative roots, old institutionalism held the view that, such a descriptive understanding of politics was the yardstick for good governance (Peters, 2005, p.11).

1.6.5 Criticisms of Traditional Institutionalism

The behavioural and rational choice theorists criticised old institutionalism for being a-theoretical and emphasising on structures other than the individuals involved (Peters, 2005, p.8). Critics again held that the variant's normative clouded perspective undermined the subject matter of political science and starved it of scientific character (Peters, 2005, p.10).

The traditional institutionalism critics further held that its proponents' focus on formal governance institutions, constitutional issues and public law clothed with formalistic and old-fashioned outlook (Peters, 200511). Its concentration on whole systems for comparison was critiqued as rendering generalisation and theory-building tasks difficult to execute (Dewey, 1996, pp.191-204). Finally, the variant tagged as relatively inconsiderate of the non-political determinants of political behaviour. These concerns, according to critics, influenced its proponents' undervaluation of non-political governmental institutions' relevance in states' behaviour analyses (Mecridis, 1963).

These criticisms, cumulatively signalling the need for a more in-depth, expansive, and analytical conception of institutionalism, ushered in the processes to replace the overly descriptive, a-theoretical and parochial Old-Institutionalism (Lecours, 2005). Consequently, the efforts resulted in the emergence of the new/neo-institutionalism.

1.6.6 Neo Institutionalism

James March and Johan Olsen in their contribution on Institutionalism posited that political institutions are crucial in shaping political outcomes with political life organisation being crucial element. Their perspective prompted thought-provoking questions such as (a) what constituted a

political institution, (b) the way institutions work, particularly how they define and defend interest, and (c) the capacity of individual actors to influence the functioning of relatively autonomous political institutions (Lowndes, 2002, p.94).

Though a relatively new theoretical construct, neo institutionalism has generally been accepted and adopted social scientists. This variant of institutionalism constitutes a belief in the usefulness of established institutions, defined as a set of rules that guide and constrain the actors' behaviour (Appiah, 2014, p.10). North defines it as the formal and informal rules, procedures, routines, norms and conventions embodied in the organisational structure of the state or political economy (North, 1990, p.46). New institutionalism further attempts to explain how institutions are transformed and run. Its central argument characterizes states as distinct organisations, vested with authority to make binding decisions and implement them, sometimes with force, for people and organisations within its jurisdiction (Rueschemeyer & Evans, 1985). The construct embodies a broad spectrum of actors, including individuals and groups (domestic, external, states and non-state actors and interest) (Appiah, 2014, p.11).

It is imperative to note that unlike the a-theoretical traditional institutionalism, neo institutionalism has embraced and engineered the development of diverse theoretical projects through deductive approaches from theoretical propositions on how institutions function (Lowndes, 2002).

1.6.7 Approaches to Neo-Institutionalism

Discourse on the neo-institutionalism theoretical perspective has birthed several approaches. Although three of these variants, including normative, historical and rational choice, are widely acknowledged and discussed by institutional theorists, several others exist (Olsson, 2016, p.12; Appiah, 2014, p.13; Bodnieks, 2020, p.87). For instance, Guy Peters extends them to seven

approaches by adding sociological institutionalism, international regimes, interest groups and empirical institutionalism, to the famed ones (Peters, 2000, p.2-3). However, as Peters argued, these variations are due to differences in perspectives and contexts within which an author seeks to apply the theory (Peters, 2000, p.2). The mergers and reclassifications, thus, render any general capping attempt impracticable and subjective. On this basis and taking into cognizance the issues of interest of this study, four approaches, including normative, historical, rational choice and sociological, are explicated. A further expatiation of each is provided below;

Normative institutionalism is associated with the writings of March and Olsen and reflects the critical role norms and values play in explaining actors' behaviour within organisations (Peters, 2005, p.26). As posited by March and Olsen (1984; 1989; 1996), a "logic of appropriateness", which people acquire through institutional membership, helps to understand the political behaviour of individuals and groups. In other words, the actions and inactions of people within institutions result from the institutions normative standards rather than the individuals' desired maximization of utility. The acquisition of standardised behaviour is, therefore, engineered by people's involvement with one or more institutions which serve as the major social repositories of value (Appiah, 2014).

Historical institutionalism, on the other hand, is associated with the works of Steino, Thelen and Longstreth (Peters, 2005, p.71). The proponents of historical institutionalism built on the old tradition of political science that assigned importance to formal political institutions (Hall & Taylor, 1996, p.6). Historical institutionalism argues that the policy and structural choices made at the inception of institutions, influence them throughout their lifespan (Peters, 2000, p.3). Historical institutionalism further maintains the need for historical analysis of institutions through

the “path dependency” concept (i.e. the persistence of organisations after their formation other than on the fact of their initial creation) in any attempt to understand political behaviour.

The third approach, Rational Choice Institutionalism, intimates that institutions are arrangements of rules and incentives, and members of the institutions behave in response to those basic components of institutional structures (Peters, 2005, p.3). The main goal of rational choice institutionalism is to uncover the laws of political behaviour and action (Peters, 2005, p.72). Scholars of this tradition believe that the successful discovery of these laws would help in constructing models for social scientists to understand and predict political behaviour (Levi 1988). Rational choice institutionalism, thus, relies on four basic assumptions. These include a set of fixed preferences of actors’ behaviour, politics as a series of collective action dilemmas, the role of strategic interaction in political outcomes determination and, finally, institutions originate and persist over time (Hall & Taylor, 1996, p.12).

Lastly, the Sociological Institutionalism that emerged from sociology and organisational studies is also centrally concerned with understanding culture and norms as institutions (Selznick, 1949). The proponents of this variant emphasize the relevance of “folkways", “behavioural patterns,” and “cognitive maps”, which they argued constituted critical social institutions for understanding the structure of social, political, and economic interactions (March & Olsen 1989; DiMaggio & Powell, 1991). Building upon complex organisations analyses, these scholars attempt to establish a relationship between formal institutions and the structure or patterns of behaviour and beliefs. They, thus, contend that institutions that inform political and social behaviour are formal and informal in nature (Peters, 2005, p.72). To them, the informal institutions are central in any attempt to understand the “non-rational” aspects of human communication and exchange.

The four approaches, as discussed above, while offering different perspectives and focusing on different aspects of political life, human behaviours, explanatory factors, and strategies for political systems improvement, are not mutually distinct from one another. Most political systems, groups, and individuals' actions function through a mix of principles, and with perspectives that are not always easily distinguishable (Lowndes, 2002). The practicality of Neo-institutionalism, thus, involves a combination of these variants in a way that helps to understand states and human behaviour in political settings.

1.6.7.1 Core Assumptions of Neo-Institutionalism

The core assumptions of Neo-institutionalism include the following;

Firstly, neo-institutionalism assumes that institutions create elements of order and predictability. They fashion, enable and constrain political actors, who are expected to act within the defined logical appropriateness. Therefore, institutions are the carriers of roles and identity and act as makers of polities' character, history and vision. They equally provide affinity ties that binds citizens' together despite their different perspectives and needs (March & Olsen, 2005, p.5). Against this backdrop, they influence institutional change and define elements of "historical inefficiency" (March & Olsen, 2005, p.5).

Secondly, neo-institutionalism assumes informal institutions play critical roles in state management affairs. Defined as "socially shared rules, usually unwritten, that are created, communicated and enforced outside of officially sanctioned channels", informal institutions differ from formal institutions, which are the "rules and procedures created, communicated and enforced through officially recognised channels" (Waylen, 2014, p.214). neo-institutionalists have conceive informal institutions differently from the popular standpoint and developing polities' scholars'

view of informal institutions undermining good governance with particularism, clientelism, patronage etc, and subverting and undermining of formal institutions (Casson et al. 2010; Lauth 2000; O'Donnell, 1996; and Pejovich, 1999). They see informal institutions as not being counter-productive to formal institutions but as complementing them to a greater extent (Helmke & Levitsky 2004, 2006). Neo-Institutionalists hence argue that rules, norms and practices, either formally codified or informally accepted conventions and norms (Peters, 2019), are instrumental in management processes and co-existence. Moreover, the unwritten and non-formal institutions provide an opportunity for dynamism in responding to phenomena.

Again, neo-institutionalism assumes that clear and routine processes leads to the translation of structures into political actions and actions into institutional continuity and change (March & Olsen, 2005, p.5). Informed by the normative variant, this neo-institutional assumption portends that structures engineered by routined processes apprise the actions of political actors and function as the basis for either continuity or change. Political actors' behaviour could, therefore, be better explained through as needing continuity or abrogation through a careful analysis of the prevailing routined processes.

Additionally, neo-institutionalism assumes that political order is created by a collection of institutions that fit more or less into a coherent system. Political actors organise themselves and act based on rules and practices, which are socially constructed, publicly known, anticipated, and accepted. These rules, norms, and practices define basic rights and duties, shape or regulate how advantages, burdens, and life chances are allocated in society, and create an authority to settle issues and resolve conflicts in a polity (March & Olsen, 2005, p.8). This assumption plays out significantly in every sphere of life in a polity and much more on issues of cybersecurity where there are various contestations and conflicting interests.

Neo-institutionalism further assumes that institutions give meaning to social relations, reduce flexibility and variability in behaviour, and restrict the possibility of a one-sided pursuit of self-interests or drives (March & Olsen, 2005, p.8). Rule-following, which poses as the fundamental logic of action in a polity, is provided by institutions. Thus, prescriptions based on the question of appropriateness and a sense of rights and obligations, derived from an identity and membership in a community and the ethos, practices and expectations are all sourced from institutions. Neo institutionalism, therefore maintains that rules are followed not because of the use of naked power but because they are seen as natural, rightful, expected, and legitimate, and so members of institutions are expected to obey and be the guardians of its constitutive principles and standards (March & Olsen 1989, 2005).

Lastly, neo-institutionalism assumes that institutions are not static and irreversible. While admitting that the ostensible subject involving institutions is stability and order in social life, students' of institutions are admonished to consider not just consensus and conformity but also to the conflict and change in social structures (Scott, 2004). In this regard, the evolution of institutions is guided by new developments and suggested modifications based on reflections on contemporary demands. It is significant to note that because institutions gets defence from insiders and validation from outsiders, and given that histories are encoded into rules and routines, internal structures and rules of institutions would rarely suffer arbitral changes. The changes that occur are largely reflected upon and are expected to mirror the adaptation to local experience, and as such, appear relatively myopic and meandering, rather than optimizing, as well as inefficient, in the sense of not reaching a uniquely optimal arrangement (Peters, 2000, p.2).

1.6.7.2 Strengths of Neo-Institutionalism

Neo-institutionalism rides on some key strengths that make it favourable for consideration among security, policy and political scholars. Among these strengths are outlined below;

First, neo-institutionalism provides a broad meaning and function for institutions. Institutions are presented not simply as representing constraints or opportunity for action, but are central in constituting the process of preference formation. Institutions are therefore presented as being involved in every dimension of politics and shape every step of the political processes (Locours, 2005, p.11)

Again, new institutionalism provides the analytical tools for determining institutional change. As succinctly reasoned by rational choice theorists, the demand for institutions is premised on their enhancement of rational actors' welfare (Locours, 2005, p.11). The rationality identified with their functioning becomes a logical measuring frame for their effectiveness or otherwise, consequently feeding into their continuity or change.

Moreover, neo-institutionalism provides a theoretical base for examining the nature of institutions in a political system. It offers an explanation for the persistence of institutions and their policies in both inductive and deductive studies (Peters, 2005, p.42).

Furthermore, neo-institutionalism emphasizes the relationship between institutions and actions. Actors are deemed to adapt their behaviour to existing institutional frameworks, leading to institutional legitimization and promotion of institutional continuity and vice versa (Locours, 2005, p.11).

Finally, neo-institutionalism emphasizes the origins of institutions. Neo-institutional theorists focus primarily on the functions that these institutions perform and the benefits they provide.

Hence, the theory appears very helpful in explaining how existing institutions continue to exist, given that institutions continued existence often depends on the benefits they can deliver (Hall & Taylor, 1996, p.46).

1.6.7.3 Criticisms of the Neo-Institutionalism

Despite the insights the theory offers and the understanding it brings to human behaviour in a polity, it attracts some criticisms. One of its common critiques bothers the question of whether the neo-institutional theory presents anything new and whether its' theoretical and empirical claims can be sustained. Guy Peters argues that neo-institutionalism harbours some theoretical inconsistencies. He argues that using different versions of the approach may yield varying empirical evidence, leading to different predictions about behaviour (Peters, 2000, p.7). Peters further observed that neo-institutional theories are better at explaining differences among different types of institutions other than the development of one or another individual institution. To him, this comes as a result of the several variances of the theory. This argument, however, does not apply in this study which is case study and whose findings are not intended for generalization.

Finally, neo-institutionalism is critiqued for the difficulty in falsifying the predictions from its theoretical underpinnings. Critics argue that it is generally difficult to find a situation in which individuals could be said to have not acted rationally within the context of a set of possible incentives (Peters, 2005, p.7). Each actor definitely has a justifiable cause for action and the judgment on the soundness or otherwise of decisions is always subjective. While agreeing to this view, it is important to note that rationality could also be measured.

1.6.8 The Deployment of Neo-Institutionalism in this study

Neo-institutionalism applies to a broad spectrum of security studies. It is more appropriate for discussions on cybersecurity management issues with a human security orientation, where institutions are considered significant for management. Therefore, the management mechanisms and frameworks designed by states and other organisations are central to assessing the efficiency of cyber security promotion efforts.

The central assumptions of neo-institutionalism, which conceives that institutions entail formal and informal schemes (regulative, normative, and cognitive), set the basis for an appropriate analytical framework for this study. As Mackenbach and McKee (2013) persuasively argue, the gains associated with the process and outcome hinge on following best practices. However, the substantial barriers relating to will and means of implementation create the need for an institutionalized scheme. Thus, given that no substantially meaningful changes will likely occur when processes are left to the whims of consumers and policymakers (Willett et al. 2019, p.478), the need for policy interventions in the form of laws, fiscal measures, penalties, etc., in management becomes imperative. This neo-institutionalism perspective on this study implies that Ghana's cybersecurity could be significantly enhanced through the efficient and effective operation and functioning of institutions that constitute frameworks and strategies. Assigning rights and duties, regulatory tasks, and defining punishment and rewards for the stakeholders (policymakers and end users) constitute necessary conditions for securing the sanctity of the state's cyberspace. Its absence would render the desire for a resilient cyberspace a mere aspiration, giving the varied opposing interests at play in cyberspace. Additional justifications for the use of the theory in this study are as follows;

Firstly, neo-institutionalism provides grounds for ensuring order and predictability by defining rules of engagement for actors and stakeholders. Actors are often expected to act within the logical appropriateness of the institutional setup. In this study, this assumption applies to the extent that the Ghanaian state has both authority and duty to protect its citizen's interests (Ghana Constitution, 1992, Article 35(2)). To carry out this duty, it has fashioned institutional frameworks and strategies that spell out roles, identities, and vision on issues of national interest, including cybersecurity. These roles, identities, and visions form the basis for measuring the appropriateness or otherwise of the State's approach to dealing with such issues (March & Olsen, 2005, p.5). This understanding offers a theoretical yardstick for measuring Ghana's cybersecurity strategy adequacy and appropriateness.

Secondly, the affinity ties of institutionalism that bind citizens together despite their varied interests and perspectives (March & Olsen, 2005, p.5) are also applicable to state cybersecurity management. Thus, while some users of cyberspace seek the opportunities it provides, others are only interested in exploiting the loopholes in cyberspace to prey on unsuspecting users. The latter's activities, hence, lead to threats against the former's interest. Institutions, therefore, come as the medium to manage these conflicting interests that keep both groups' interests in check.

Additionally, neo-institutionalism contends that institutions guide social relations, reduce flexibility and variability in behaviour, and restrict the possibility of a one-sided pursuit of self-interest or drives (March & Olsen, 2005, p.8). This fundamental logic of action in society applies to the study. The principle aids the study in addressing the multidimensional interest elements in cyberspace management and how they would have to be balanced.

Thirdly, the conceptualization of institutions by neo-institutionalism to encompass formal and informal offers a framework for a holistic evaluation of Ghana's cybersecurity strategy's adequacy and appropriateness. This theoretical assumption reveals that institutional structures' availability, though important is not a sufficient condition for realising policy results. To get the needed results, such structures should be all-encompassing in nature and respond to the various facets whose manifestation has implications for the phenomenon. The absence of such considerations would create a loophole and its effects in the response mechanism. The assumption in the scheme of this study, therefore, provides a holistic assessment framework that assesses Ghana's response strategy not only based on the formal structures; international and national cybersecurity infrastructure and regulatory frameworks, but also the contextual situation that translate as informal norms (unwritten institutions).

Fourth, the neo-institutional theory helps in constructing frameworks for the empirical study of institutional life that offers a basis for institutional change or continuity arguments. As noted by March and Olsen (2005, p.5), institutions which can undergo transformation and elements of "historical inefficiency" in routinized processes, serves as justifiable grounds for changes in institutional setups. A justification for the need or otherwise of change, modification or continuity, therefore, requires a critical evaluation of the effectiveness of security strategies. In the space of this study, this assumption offers the study the opportunity to establish empirically justifiable grounds to call for either the modification, change or continuity of Ghana's institutionalized cybersecurity promotion strategy.

Fifth, neo-institutionalism offers a place for informal institutions in the management of state affairs. As socially shared rules, usually unwritten and outside the premise of officially sanctioned channels means of enforcement (Waylen, 2014, p.214), informal institutions can augment formal

arrangements in responding to issues of social concern. In the case of cybersecurity management, as considered in this study, neo-institutionalism's assumption of the significance of informal institutions is important to cater for context-specific dynamics in states' cybersecurity response strategies. To this extent, the assumption provides a framework that aids a holistic approach to assessing the adequacy of the state's response, by considering the presence and effectiveness of formal and informal structures and institutions.

Finally, neo-institutionalism's assumption of institutions not being static and irreversible is also of much relevance in this study. The assumption pre-supposes that the strategies and frameworks instituted by the state for management issues, including cybersecurity concerns, are not static. The continual innovations and the associated cyber threat variations in cyber ecosystems make this concern even truer with cybersecurity. Assenting to this view, Scott (2004 p.2) intimates that although institutions ultimately seek to instil stability and order in social life, students of institutions must necessarily attend to not just consensus and conformity but also to conflict and change in social structures. Again, the neo-institutional principle of change not being entirely arbitrary but reflecting local experience adaptations (Peters, 2005, p.2), is also of much significance to this study. The assumption implies that inasmuch as states can vary institutional arrangements for the governance of cyberspaces, including cybersecurity, such engineering must carefully consider the various domestic factors that impact the state's cyber ecosystem. In this regard, the theory offers a significant guiding principle in the analytical framework for assessing the adequacy and effectiveness of Ghana's cybersecurity response strategies against the prevailing threats.

The neo-institutional theory is crucial to this study because the Ghanaian government has the responsibility to safeguard its citizens and residents. Cyberspace is a platform used by individuals

with diverse interests and, as such, is an ecosystem with significant security concerns in contemporary times. It is, therefore, the state's duty to protect itself and its citizens from cyber threats. By creating institutions and structures, the state establishes a set of rules that guide and regulate the behaviour of stakeholders. These rules and structures establish the strategies to be deployed by the state to tackle cyber issues and the strategies are mostly pragmatic and may change depending on their effectiveness in responding to identified cybersecurity threats.

1.7 ORGANISATION OF CHAPTERS

The thesis consists of seven chapters. Chapter one deals with the introduction, which comprises the background to the study, a statement of the research problem, the research objectives and questions, the scope and significance of the study, the theoretical framework, and the organisation of the thesis. The second chapter entails the conceptualization of terms and a review of relevant literature. Broadly, the literature review is conducted on themes, including general security studies, cybersecurity and developing countries' cybersecurity experience, cybersecurity studies in Africa, and cybersecurity literature on Ghana. The third chapter looks at the research methods and details the various research methodologies and instruments for data collection and analysis. Chapter four takes an overview of cybersecurity in Africa. Chapter Five analyses the Ghanaian cybersecurity threats landscape. Chapter six then dwells on Ghana’s cybersecurity response mechanisms and their adequacy, while the last chapter provides a summary of the findings, conclusion, and recommendations.

CHAPTER TWO

LITERATURE REVIEW

2.0 INTRODUCTION

The chapter reviews literature relevant to the study. This is conducted on a thematic basis along the lines of scholarship on cyber-security and studies on cybersecurity in Africa and Ghana. The chapter opens with a section on operationalizing the key concepts used in the study.

2.1 OPERATIONALIZATION OF KEY CONCEPTS.

The key concepts used in the study and their operationalization are provided below;

2.1.1 Cyber Security

The terms' "cyber" and "cyberspace", which form the basis of cybersecurity, have a rich historical background (Azmi et al., 2016; Ottis & Lorents, 2010). The term "cybernetics" was first introduced by Wiener in 1948 to describe the "interactions between humans (or animals) with a machine that could provide an alternative environment" (Wiener, 1948, pp. 144-154). The term "cyberspace" resurfaced in the early 1980s when Gibson used it to refer to a graphical and spatial representation of the world's data in the minds of individuals connected to the system (Siegel, 2016, p. 10). This term later came to be associated with a civilisation of the Internet and the study of its information systems (Ottis & Lorents, 2010).

The cyber civilisation has distinguished the contemporary world with information dissemination and service delivery mediums. States, corporate bodies, and individuals have come to rely heavily on its operations for their daily activities (Humayun et al., 2020). All fields of life are now drawn into cyberspace, and tons of data are generated through its adoption. While these systems and data

have shown valuable significance in state planning and development, they also turn out as potentially harmful tools in the hands of miscreants (Savaş & Karataş, 2022; Humayun et al., 2020). The usage of the space for commercial and personal purposes and the fact that no technology or web applications are sacrosanct have enticed cybercriminals to exploit the faults, leading to a rise in cybercriminal activities (Lun et al., 2016; Razzaq et al., 2013). While the space's significance and potential dangers appear uncontested, the conceptualising of what cybersecurity is and what constitutes protection has generated debates among states, institutions, and scholars. Consideration of the various variants of the concept for a better appreciation of its meaning has been at the core of this debate.

Etymologically, cybersecurity is from the words "cyber" and "security." To secure signifies offering protection against harmful impact, and security connotes "the protection of systems and undesirable disclosure, destruction, or modification of data in systems" (Valeriano & Maness, 2018, p. 7). Cyber, conversely, implies anything that involves or relates to networked computers with the Internet (Craigen et al., 2014). Along with this perspective, Craigen et al. considered cybersecurity to mean the securing of the environment of a virtual realm where users create, store, and share digital information and communication online through physical infrastructure (Craigen et al., 2014). Similarly, the ISO/IEC (2013) edition puts it as relating to the "integrity, confidentiality, and timely availability of information in cyberspace" (ISO/IEC, 2013, cited in von Solms & von Solms, 2018, p.5). While integrity concerns non-authorised persons not altering the information in a data system, confidentiality implies that only the rightful people are privy to the information, and availability means the authorised persons can access the information when needed. Therefore, Cyber security entails protecting the virtual realm's activities and content in a way that ensures confidentiality, integrity, and availability.

However, it is imperative to note that the virtual realm and the activities conducted therein pass through some physical infrastructure, and that any compromise of such structures portends grave consequences on the space. This understanding, therefore, renders the earlier definitions which limited the protection to only the virtual realm and its information, as being quite narrow in scope. As suggested by von Solms and van Niekerk, it informs that the term encompasses "the protection of cyberspace itself, the electronic information, the information and communication technologies that support cyberspace, and the users of cyberspace in their personal, societal, and national capacity, including any of their interests, either tangible or intangible, that are vulnerable to attacks originating in cyberspace" (von Solms & Van Niekerk, 2013, p. 101). Ensuring the security and privacy of digital assets including networks, computing devices and processed information stored or in motion in interconnected information systems are critical components in cybersecurity (ISACA, 2016, cited in Von Solms & Von Solms, 2018, p.5). To this end, cybersecurity entails more than just protecting processed information/data but includes protecting the space, equipment, and users.

Dunn-Cavelty (2010, p.363) subscribing to this broader orientation asserted that the concept concerns the use of technical and non-technical practices in addressing the insecurities in cyberspace. Cybersecurity, from this perspective, goes beyond a computer science and information technology-associated technical issue as suggested by some cybersecurity literature such as Vacca (2013) and McLean (2013), to involve a more nuanced and complex issue with a broad scope that traverses technical, crime espionage and military-civil defence discourses (Dunn-Cavelty, 2010, pp. 364-369). Building on this broader conception, the International Telecommunication Union (ITU) concurred that the concept encompasses any breach or compromise of the interest, data, or systems or their conveyors in cyberspace and how such breaches could be addressed. It therefore

extrapolated it to mean that "set of security concepts, policies, tools, guidelines, risk management techniques, best practices, technologies, training and assurances that may be utilised to secure an organisation's cyber environment and users assets" (ITU, 2021, p.7). Cybersecurity, hence, involves deploying policies and technology to secure the interests and assert of cyber users within a space.

It is clear from the above that the cybersecurity concept is understood from different perspectives and so subjected to subjective meanings. However, the definitions generally revolve around three main things: user protection and privacy enhancement, the need to define rules and policies, and the processes and technologies to protect computing devices. Ultimately, all this helps to attain information confidentiality, integrity, and availability. Based on this understanding, this study operationalises cybersecurity to mean securing the interests, data equipment/infrastructure, and lives of individuals, organisations, and states within cyberspace by deploying policies and tool toolsets, guidelines, and risk management techniques and technologies.

2.1.2 Cyber Security Threats

Cyber-technology has assumed great significance in global communication and has become pivotal in human lives and states' socio-economic and political development (Tan et al., 2021; Judge et al., 2021). The 21st century's private and public sector activities have been interwoven into this phenomenon, with governments and organisations relying on cyber technology for essential social services delivery (Mishra et al., 2022; Li et al., 2020). However, these great potentials and contributions are not insulated against vulnerabilities, risks, and challenges to the users (Reveron & Savage, 2020; Domingo, 2016, p.246). Thus, cyberspace is prone to interruptions and disruptions by individuals, states or organisations who seek to gain or benefit from systems breaches and adversely exploit them (Humayun, 2020, p.3).

The various forms that these craftily orchestrated plans of interrupting the flow of function in cyberspace constitute what is termed cyber threats. This study adapts Tunggal's definition of the concept in this regard. It, hence, references it as those "malicious acts that seek to damage data, steal data, or disrupt digital life in general" as well as "the possibility of a successful cyberattack that aims to gain unauthorised access, damage, disrupt, or steal an information technology asset, computer network, intellectual property, or any other form of sensitive data" in cyberspace (Tunggal, 2022, p.1).

2.1.2.1 Types/Kinds of Cybersecurity Threats

The threats come under three broad overlapping kinds: disruption, destruction, and exploitation threats. Disruption threats involve malicious software created and deployed to damage and disrupt critical business functions (Li& Liu, 2021, p. 8178; Motsch et al., 2020). Distributed Denial of Service (DDOS) or Denial of Service (DOS) is the most common of these threats. The disruption threats could have lasting effects on business operations. The second kind, the destruction threat, involves those possible dangers to computer systems that may destroy computational resources or other systems (Li & Liu, 2021). Such threats could result in personal injury or death or significant damage, destruction, or manipulation of information, data, or software, rendering them unfit for use unless extensive restoration is ensured (Danish Centre for Cybersecurity, 2021, p.4). An example of these threats is malware infestations. A typical manifestation of the destructive threat is the 2010 Stuxnet malware attack on Iran, which destroyed its uranium enrichment centrifuges (CFCS, 2021, p.7). The third kind is the exploitation threat, which targets to cause significant harm to the victims' security, personal, or professional lives (Li & Liu, 2021, p. 180). Threat actors use exploitation threats to gain confidential information on individuals or organisations for material (financial) or non-material (emotional distress) exploits. Examples of these threats include the non-

consensual distribution or publication of intimate photos or videos of persons, ransomware, phishing and social engineering.

In their categorisation, Razzaq et al. (2013, p.1) also suggested that cybersecurity threats could broadly come under two major groupings: (1) those that seek to harm computer networks or devices directly, such as malware, viruses or denial of service attacks and (2) those facilitated by using computer networks or devices to commit crimes such as defrauding, stealing users' identity or engaging in information warfare. It is indicative from the above that the techniques deployed by cyber criminals are defined by the threat actors' motives or objectives. The president of cyberlaws.net and consultant, aligning with this criminals-target categorisation indicator of cyber threats, further classified them as:

1. Cybercrimes against persons. This is exemplified by threats such as the transmission of child pornography, harassment through email, dissemination of obscene materials or violation of the privacy of citizens.

2. Cybercrimes against all forms of property. Among these include computer vandalism (destruction of others' property), the transmission of harmful programs and the use of various spyware to steal corporate confidential data.

3. Cybercrimes against Governments or states. These include terrorist activities and attempts to break or crack state, government, or security services' sites and databases.

Cybersecurity threats are, therefore, diverse, proceed from varied sources and have a wide range of targets (Wong, 2016, p.14). The targets, sources, and forms of threats influence threat actors' techniques and define the dominant threats that organisations and states encounters. It is crucial to note similarity of cyber threats across all cyberspaces because the same technologies are deployed

all over. Again, these cyber threats are not mutually exclusive of one another, as cybercriminals or threat actors could employ several types within a single attack. Continuous advancements in cyberspace technology have led to new vulnerabilities prone to exploitation by threat actors. This phenomenon renders any attempt at putting a seal on the types of threats impossible (Johnson, 2015, p.288). Nevertheless, some common ones are malware, ransomware, spyware, social engineering, physical device alterations (e.g. ATM skimmers), email-related threats, and crypto-jacking. Others are DoS, mis/disinformation, supply chain attacks, data spills, hacking, identity theft, malicious insiders, phishing, and email scams (Wong, 2016, p.14, ENISA Threat Landscape, 2021, Australia government, 2022).

Table 1 Cybersecurity Threats

Threats/Threat Agents	**Meaning**
Hacking	The Malicious scammers intrusion into connected digital networks such as computers, laptops, tablets, and phones to steal sensitive data such as passwords, usernames, bank information, and other personal details.
Phishing	A method of social engineering used to obtain sensitive information such as online banking, credit card credentials username/password etc. from users to get access to their money and confidential information.
Ransomware	A sort of malicious software designed by criminals to prevent users from accessing their computers until they fulfil an obligation termed “ransom”.
Botnets or bot attacks	This refers to infecting devices or networks that work collectively under an attacker's command. They are used to carry out phishing scams, spam campaigns, and distributed denial of service (DDoS) attack and prevent a network from serving genuine requests.
Advanced Persistent Threat (APT)	This is when an unauthorized user uses advanced and sophisticated ways to obtain access to a system or network. APT usually deploys techniques such as ransomware, phishing, malware, and data breaches to launch attacks on their targets (Mohamed et al., 2018).
Malware	This refers to software or code meant to harm computers by encrypting files, damaging, disabling, stealing data, or gaining unauthorized access to a

	computer. The phrase refers to a variety of harmful software, including trojans, worms, and ransomware.
Malicious social media messaging	These are malicious messaging and misinformation spread on social media mainly to misinform people and to alarm them. It is mainly used to disseminate fake news, conspiracy theories and alarm fear in communities.
Distributed denial-of-service (DDoS) attack	DDoS attack is a type of attack that cybercriminals deploy to render online services unavailable to users by generating a large amount of traffic.
Spam emails	Unsolicited or anonymous messages sent in bulk by emails are known as email spam, or junk email or simply spam. The name stems from a Monty Python joke in which the packaged pork product's name is mentioned.

2.1.3 Cyber Security Framework

A *cybersecurity security framework* describes the guidelines, standards, and best practices for cyber risk management. It seeks to provide the foundation, structure, and support to an organisation's security methodology and effort, and comes either as a control program or risk framework. An organisation's choice of which type of such framework to deploy depends mainly on its capacity and what it seeks to achieve. Some popular frameworks within the cyber industry includes that of the National Institute of Standards and Technology (NIST), whose elements comprise identifying, protecting, detecting, responding, and recovering. Other frameworks are the Centre for Internet Security (CIS) Controls, the International Standards Organisation (ISO) Frameworks eg. ISO/IEC 27001 and 27002, the Health Insurance Portability and Accountability Act (HIPAA), the Service Organisation Control (SOC2), and the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC-CIP).

2.1.4 Cyber Security Norms

The mix of opportunities and grave threats that cyber technology engenders for states and non-state actors cannot be over-emphasized. Such reality have triggered a common sense of need in moderating behaviour on ICT usage and intensifying efforts at preventing potential situations that endanger peace and security at both domestic and international levels (Dunn-Cavelty & Wenger, 2020). According to Osula & Rõigas (2016), cyber norms or cyber norms of behaviour have been highly acknowledged in security discourse for their ability to do such bidding by upholding strategic stability within the cyberspace (p.11). Norms, generally, are those internalized rules based on commonly held values (Benedict, 2015, p.157). They constitute the "collective expectations about the proper behaviour of actors with a given identity" (Katzenstein, 1996, p.18). One common feature that characterizes them is that they are shared beliefs among actors within a community. Thus, a prescribed normative expectation does not become a norm until it receives endorsement from relevant community groups or actors (Finnemore, 2017). Norms also entail a broad spectrum and could differ substantially in scope and legal "bindingness" and feature legal, political, technological, ethical, or social characteristics (Osula & Rõigas, 2016, p.12). When such norms are engineered to guide behaviour in cyberspace, they are termed cyber norms.

The primary justification for deploying cyber norms in cybersecurity management is their ability to help increase predictability, promote trust and stability in ICT usage and prevent possible conflicting state arising from misunderstandings. These norms also constitute the guiding principles for shaping states' domestic and foreign policies and form the basis for international partnerships (Osula & Rõigas, 2016, p.11). Cybersecurity norms are, hence, used in this study to connote those collective expectations on the proper behaviour capable of keeping states and other cyber actors in check within cyberspace.

2.1.5 Cyber Capabilities

Cyber capabilities refer to the resources and assets a state can use to resist or exert influence in cyberspace (Craig, 2020, p.1, 2018). States deploy these assets and resources in various ways for their strategic interest advancements. Craig (2018) asserts that such abilities generally come as latent or active. The latent capabilities consist of the societal-based resources such as citizens' computer science knowledge and the IT industry available for government use for its strategic interests in cyberspace. The active capabilities, on the other hand, are the operational capabilities directly controlled by the governments that could be deployed in computer network operations to advance the states' cyber interest (Craig, 2018). The security implications of capacity disclosure that make states secretive about their cyber capabilities, complicates the measurement of states capabilities. However, researchers could ascertain a state's cybersecurity capability to a greater extent by observing and measuring aspects such as computer response teams, cyber units, and national cyber strategy instruments. "Cyber capabilities" is therefore used in this study to refer to states' readiness to tackle cybersecurity challenges, measured by the presence or absence of key cybersecurity indicators.

2.1.6 Cyber Resilience

According to Borky and Bradley (2018; p.7), the cyber capabilities of states involve three elements; Technical measures (e.g. Key public infrastructure, security testing, policy servers), Physical measures (placing sensitive information or other protected resources behind barriers) and Procedural measures (operational and practical procedures aimed at maintaining the effectiveness of security controls and eliminating vulnerabilities). Protecting cyberspace is a challenging task due to the possibility of system compromises and circumventions. In this regard, the protective and defensive configurations also continually evolve towards more dynamic and sophisticated

approaches (Borky & Bradley, 2018; p.6). Based on this understanding, Makridis and Smeets (2019) justify why states need to pay attention to a broad spectrum of threats from both the external environment and domestic political variables, when building their cyber capabilities. The robustness of the resultant systems by the states or organisations to respond effectively to these threats is termed the resilience of their cyberspace.

2.2 Governance of the Cyberspace

Governance involves the practices and responsibilities of those in charge of an enterprise to provide strategic direction, ensure objectives are met, manage risks appropriately, and use resources responsibly (Bodeau, 2012, p. 10). It also includes the setup of rules, the authoritative management or implementation of the rules, including sanctions, and the engagement of the system with users. The complexity of cyberspace domains, with associated risks and resources such as information security, finance, legal, and regulatory compliance, necessitates specialised management expertise (Bodeau, 2012).

Cybersecurity governance is premised on the conviction that cyber risk elimination is possible through effective cybersecurity strategies (Savaş & Karataş, 2022). Governance is preferred to management in the cyberspace because the former attempts redresses of all cyber concerns from strategies design and effective implementation and involve all stakeholders within the management circles (Savaş & Karataş, 2022). Cyber governance is, therefore, the more encompassing approach that offers firms' the adequate frameworks to oversee their activities within cyberspace. From this perspective, cyber governance is construed as an organisation's governance component that directs and controls information security systems in the presence of adversaries (Bodeau, 2012, p. 10; ISO/IEC, 2014). This study, hence, uses the term to refer to a multi-disciplinary approach that

adopts meticulous policy designs for hardware, software, and people (users) to prevent or minimise cybercrimes and their impact.

The watershed moment in cyber governance arrived in 2014 when the United States government committed to relinquishing its internet's technical back-end, the Internet Corporation for Assigned Names and Numbers (ICANN) (de Guzman, 2014). According to the United Nations World Summit on Information Society (WSIS), the oversight interest of stakeholders in cyberspace widened over time due to the continual realisation of the internet's utility to society and the economy (WSIS, 2003). Stakeholders in the cyberspace expanded from just states and organisations to include private industry and civil society organisations (CSOs), and the governance process assumed a multi-faceted form, encompassing activities from technical standards coordination to regulation and advocacy.

The Tunis Agenda document, which distinctively delineated each internet stakeholder's responsibilities and recognised the state's authority in Internet policymaking, brought further definiteness to cyber governance (WSIS, 2005, 35(a)). While recognizing the state as the lead actor in cyber governance, the multi-stakeholder model which involved governments, private sector players, technical communities, civil society groups and other entities' got further backing in internet governance during the April 2014 NetMundial in Brazil.

The NetMundial Statement, unlike the Tunis Agenda, offered varying functions to different stakeholders in different contexts to allow for flexibility in collaboration. Its call also signalled the need for better coordination between the technical and non-technical communities to ensure a better appreciation of the policy implications of technical issues and the technical implications of policy decision-making. Again, its call sought a proper alignment of Internet security and

Universal Human Rights principles because of their conflictual relationship. The UN Human Rights Council had in June 2014 adopted a parallel resolution, stressing the need to protect people's rights and freedom. It argued that individuals have rights online, just as in physical space, which should be respected (UN Human Rights Council, 2014). These rights include the right to express opinions, share information and ideas, associate with others on social media platforms, and maintain privacy in their online activities.

It is imperative to note from the above that the state has two contrasting tasks: upholding rights and addressing cybersecurity threats. (Ibrahim et al., 2020; UNGA, 2010, p.2). Prompt and adequate policy measures by states to achieve this objective have essentially preoccupied their responses to cyber threats (Ibrahim et al., 2020). Practical steps, including fashioning sets of policy measures and strategies and collaborations among the various actors in the space, have been taken towards realising this objective. The attempt has transformed efforts to manage cyberspace from ordinary mitigation measures to detailed and systematic design and implementation of governing rules. Despite attempts to secure the space without infringing on users' rights, implementation challenges persist for stakeholders (de Guzman, 2014).

States can navigate the complex world of cyber governance by admitting that absolute security is unattainable. To this extent, governance processes must proceed with caution after a thorough identification of problems and vulnerabilities. Policymakers can render a better protection for the internet as a global asset by adopting security paradigms that go beyond preventing perceived harm. They require continual innovations and revisions in preventive actions due to the constantly evolving nature of cyber threats (Wong, 2016, p.8). This perspective influenced the five task information/cyber security governance processes elements of the ISO/IEC. These include

evaluating, directing, monitoring, communicating, and assurance. Clarity on such practices, argues de Guzman (2014, pp.11-12), helps organisations or states to make informed and justifiable decisions on security measures investment, cyber risk management alignment and organisations' security posture.

The above understanding is essential to this study, which aims to assess states' responses to cybersecurity via their adopted strategies. It highlights a need for the Ghanaian state's adoption of a cyber governance strategy that assumes a balanced posture vis-à-vis security and human rights.

2.3 National Cyber Security Strategies

Sanity in cyberspace is realised through carefully designed strategies by and for the interest and protection of stakeholders in cyberspace, such as the states, organisations and corporations (Luiijf et al., 2013; Merriam-Webster, 2016a; von Solms & van Niekerk, 2013). Against this view, Azmi, Tibben and Win (2016 p.1) quip that cyber security strategies involve the overall socio-technical policies for shaping the information security environment in a manner that best accommodates the interest of stakeholders (government, industry and civil society) in a state. Such practices reflect the nation's cyber risk goals that impact government activities, the private sector and civil society (Azmi et al., 2016). Again, states' designing strategies to guide activities within their jurisdiction has become inevitable because of their responsibility to secure citizens' interests and exclusive authority to control the actions of entities and individuals within their jurisdiction. Such carefully planned strategies for securing the state's cyberspace by national policymakers are what is termed here as national cybersecurity strategies.

2.4 GENERAL LITERATURE ON CYBERSECURITY IN IR

The cybersecurity concept has its roots in the 1980s, when the first cyber-attack was detected. Various cyber concerns such as threat landscapes, cybersecurity capabilities, strategies and mechanisms of states, institutions and organisations, and the impact of cyberspace on persons, institutions and economies have subsequently received some attention within scholarship. International Relations scholars got invited into the cyber discourse because digital technology signalled a new power source capable of altering the existing power distribution system of the international system (Nye, 2011). Cyberspace has since become a critical avenue for states' domestic and foreign security policies with a window to offset the obsolete "Use of Force" principle (Mussington, 2019; p.59).

Cyber security issues have subsequently been increasingly discussed as a stimulus and consequence in IR and have been integrated into power play dynamics and cooperation in international politics (Dun-Cavelty & Wenger, 2020). These attributes have pushed cyber discourse and analysis into international relations literature, which is presented under technical, crime espionage and military-civil defence sub-issues (Dunn-Cavelty, 2010, pp.364-369; Dunn-Cavelty, 2013; p.105). Whilst the technical discourse primarily concerns assessments of technicalities involved in the operationalisation of the system and its sacrosanctity, crime espionage and the military-civil defence look at states', groups' and other organisations' deployment of the technology for either attack or defence purposes.

The national security implications of digital technology have also featured as a major issue in international relations scholarship. Efforts by scholars in this endeavour have sought to explain the impacts of cyber technology on critical security infrastructure, security and defence operations, and intelligence gathering (Dawson, 2021). From this perspective, Mussington (2019) argues

forcefully that much of states' international defence capabilities have been impacted by ICT technologies. While this conclusion might have been relative to states' level of cyber technology or capabilities, incorporating cyber defence mechanisms into states' security architecture and operations has become a common practice worldwide. It is imperative to observe also that this co-opting not only increases the security capability of states but also poses a significant challenge, especially for the developing and cyber-infant ones. Such dire implications of the phenomenon and its rippling effects on other states have resulted in securitizing cyber redress as an international security issue and for IR scholars to formulate concepts and propose measures towards it responds (Kello, 2013; p.39). This has rendered the phenomenon a pivotal international security concern and a justification for the increased arguments for international collaboration and response to it.

Security and IR scholars have since taken a keen interest in the implication of cyberspace on security balance in the contemporary international system. In this regard, a plethora of studies, including Colarik (2006), Buchan (2018) and Dunn-Cavelty (2013), have examined how cybernetics influences the global security environment through practices such as cyber terrorism and espionage. Their studies underscored that the 9/11 tragedy spurred the securitisation of cyberspace. It moved the discourse on cyber-attacks and national security nexus from a mere possibility mantra to real-life threats that warranted attention like other security threats. Following this understanding, a body of studies, including Shin, Son, and Heo (2015) and Karake-Shalhoub and Al Qasimi (2010), argued in support of the internationalisation of the cybersecurity management processes for improved international safety systems, particularly for developing countries.

The complexities of the space and the borderless nature of its effects prompted the rallying of states under international organisations and multilateral cooperation to enhance its vitality

(Mussington, 2019). IR scholars have thus argued for cooperation in addressing the apparent challenges in the space, such as free riding and norms non-compliance by states (Luiijf et al., 2013). IR scholars have also made significant contributions in defining the essential elements of national cybersecurity strategies. This is borne from the concern that though the transboundary and near-universal nature of cyber threat/challenges influence similarities in states' cyber strategies, countries unique domestic situations portends consequential impact on their strategies in dealing with such concerns (Luiijf et al., 2013, pp.4-6). Despite these varied understandings, Sabillon et al. (2016) identified key pillars that influence states' actions and set pertinent international strategies, alliances, and cooperation. IR scholars have, against this perspective, also appraised corporate efforts by states in cyber management, which begins with the individual states' management approaches.

IR scholars have attended to states cybersecurity capabilities assessment. Studies such as Calderaro and Craig (2020) and Craig (2020) have offered valuable insights into states' cybersecurity framework design and cooperation for effective cybersecurity management. Upon their analyses of a number of states and multilateral organisations cybersecurity strategies, the authors identified both domestic and external factors as defining cyber capabilities. They noted that cyber literacy, institutional development, and collaboration (both internal and external) were key to securing states' cyberspace. Drawing from this understanding, the authors cautioned developing states in particular from limiting energies for securing their cyber ecosystems to single efforts or spaces. This body of studies has also argued for developing states' to attempt manoeuvring the consequential security challenges in the international system by leveraging cybersecurity in their international politics.

To establish a firm demonstration of cyberspace as a conduit for power balance in international politics, Crandall and Allan (2015) and Burton (2013) considered Estonia and New Zealand's utilisation of cyberspace, respectively. The two studies concluded that these two relatively small states have creatively used cyberspace to advance their influence and bargaining position in international politics. While, the role played by their advanced technological innovations, which most developing African states lack, is worth acknowledging, it is apparent that the space offers opportunity to less powerful states to make a case for themselves in international politics. The resolve to seize such an opportunity, which would require deliberate policies and investments, now lies in the bosom of such states.

From the above, it is evident that IR scholars have shown significant interest in cybersecurity studies, which is not surprising, owing to the influence the space wields on states' power dynamics. The possibility of states deploying cyber terrorism and espionage or protecting themselves from the same makes it worthy of study among IR scholars. The transboundary nature of cyberspace activities has hence triggered the need for international cooperation in handling all the fallouts, which further buttressing IR's place in cybersecurity. The understanding that a proper balance in cyberspace management hinges on better state-level management through the design and deployment of adequate strategies is also established and affirmed the significance of the central objective of this study.

2.5 DESIGNING STATES CYBERSECURITY STRATEGIES

States in the contemporary world are expected to set cyber threat management goals and strategies in response to their cyber threats and advance the maximisation of the opportunities offered by cyber technology. Those decisions portend considerable implications for government activities, the private community, civil society, and individuals' contributions (Azmi, Tibben & Win, 2016).

States response strategies are expected to fit into the general standard practice and also reflect the domestic peculiarities of the state or organisation. In other words, the need for global harmonisation and cooperation to effectively tackle transnational threats, the commonality in the technology (Broadhurst, 2006), and the peculiarities of the domestic realities in states, are the defining factors for states' cyber-security response design. Therefore, the considerations in cybersecurity strategies design involve the transboundary nature of the cyber threat phenomenon, the implications of those policies and strategies for other states' or entities' interests and the domestic capabilities of the state. The decisions and conclusions that states arrive at in line with the above perimeters explains the possible differences in their strategies. The subsequent paragraphs examines further some factors that influence states' cybersecurity strategies.

2.5.1 The Determinants of National Cyber Security Strategies

The preference for cybersecurity strategies as an effective tool for managing risks and responding to states' Information and Communications Technology (ICT) infrastructure threats (Giri, 2019), has elevated it to national policy priority in states (Lebogang et al., 2022). This observation has empirical affirmation in a survey of ten (10) OECD countries, which found that many states incorporate cybersecurity policymaking into their national policy priority realms (OECD, 2012).

As a policy framework with visions and articulated priorities, states' governance principles, national interest, and the manifesting cyber threats influence national cyber-security strategies (NCSS). This scope of the NCSS design informs the adoption of holistic approaches that border on socioeconomic, educational, legal and diplomatic sectors (Senol & Karacuha, 2020). Various sector players' efforts are thus required to design well encompassing and robust cyber-security strategies (OECD, 2012). Like many other policy decisions or strategies, diverse interests come into play in NCSS design and create the need for prioritization and trade-offs.

Differences in country-level approaches to cyber-safety have been established, with peculiarities in states' vulnerabilities and dominant cybersecurity threats featuring as key reasons (OECD, 2012; Azmi et al., 2016). States have different levels of internet penetration, practice different economic models and have different security orientations and needs. This results in differences in vulnerabilities and the consequential strategies required to address them. Therefore, while states generally attempt to adopt cyber strategies to enhance cyber benefits or mitigate their downsides, their conclusions on what constitutes significant threats and requires attention, influence their approach and the content of their cybersecurity strategies.

Another reason closely related to the above, which Luiijf, Besseling and de Graaf (2013, p.6) identified as influencing variation in states' cyber-security strategies, is their conception of cybersecurity. The authors opine that how states conceptualize, describe, or define cybersecurity influences their strategies for its redress. Differences in conceptualization would reflect differences in strategies and vice versa. For instance, the Australian government, for instance, defines the concept as relating to the measures towards attaining the confidentiality, integrity, and availability of the information that is processed, stored, and communicated by electronic or similar means. To the Canadians, it concerns the "appropriate level of response or mitigation to cyberattacks (the intentional or unauthorized access, use, manipulation, interruption or destruction (via electronic means) of electronic information and or the electronic and physical infrastructure used to process, communicate and or store that information" (Canadian Center for Cyber Security: glossary). On her part, the UK decided to embrace both the protection of national interests in cyberspace and the pursuit of a wider national security policy by exploiting the many opportunities the space affords (Luiijf et al., 2013, p.6).

The three states' conceptions present evident variations in terms of cyber orientation. For instance, while Australia's security/protection is limited to only data, Canada's expand it to cover data and infrastructure, and the UK further extends it to the protection of both the security space and national interest. Again, the definitions also show that while some countries focus on critical cyber infrastructure protection against risks, others are concerned with intellectual property data protection, cybersecurity awareness improvement or even both (Al-Ghamdi, 2021). This understanding is crucial in assessing a state's cybersecurity strategy, such as the current study, through the provision of guiding principles for analytical framework determination.

Through a qualitative review of 54 countries' NCSS in their article "Motives behind cyber security strategy development", Azmi, Tibben, and Win (2016) established a perspective on NCSS which was later built upon by Collier (2017). The authors intimated that three primary motives remained central in the design and implementation of NCSS. According to them, these include National Security, Jurisprudence, and Politics (Azmi et al., 2016, p.7). Concurring with Collier (2017), they maintained that whereas cyber threat management serves a national security objective, states' cybersecurity strategies also serve political and diplomatic relevance. In other words, the objectives of cybersecurity strategies go beyond national security enhancement to providing an avenue for promoting the vision and image of a state within the international community (Azmi et al., 2016, p.7). This indeed comes handy in cyber governance, where collaborative efforts are required to deal with some of the threats to the state's cyber ecosystem. Apart from the clarity provided on the factors that could potentially influence the cyber-security strategies of states including Ghana, which is being considered in this study, the descriptive coding that the authors adopted for the development of themes and the pattern coding aids in-depth appreciation on the motives influencing states' cyber security strategies within methodological construct. This study

thus leaned on such approach in coding the primary data gathered from the field through in-depth interviews.

Another study that sheds light on the determinants of states' cybersecurity strategies is Burton (2013). He underscored that the factors influencing states' cybersecurity strategies could broadly be categorized as internal or external factors (Burton, 2013). Just like the internal, the author indicated that international/external factors played critical roles in strategies for cyber threat management, particularly in smaller or developing states. He argues that the competition between powerful states has rippling effects on the cyber strategies of the less powerful. Citing the example of New Zealand, the author intimates that the rivalling interests among the United States, Russia and China have significantly influenced New Zealand's cyber-security strategies. He explains that the power-seeking agenda by these states has influenced their resolve to cooperate with New Zealand and other states of their ilk on cyber-security matters. Such a tactical move aims at bolstering their wealth of influence against their perceived rivals. These corporations, which involve monetary and technological support, have a significant impact on the design and implementation of cybersecurity strategies. Thus, apart from succumbing to the dictates of the donors due to their support, beneficiary countries also require technical assistance on the received cyber technology to aid its proper installations and operation. Developing African states such as Ghana, will predictably therefore have traces of cyber-matured states' cybersecurity strategies in theirs. While this does not amount to a totally objectionable phenomenon, the state's domestic peculiarities needs to significantly reflect must in such a cybersecurity strategy mix. This study's framework, fashioned on structuration and leveraging on both structures and agents in knowledge construction and neo-institutionalism, which argues for the consideration of informal institutions

in state governance, provides a proper and better grounds for determining the appropriateness or otherwise of the Ghanaian cybersecurity strategy.

In his book chapter on cybersecurity, Collier (2017) reasons that despite the variations in states' cyber-security strategies, all strategies revolve around some general elements. Based on an examination of the cyber-security strategic styles of Estonia and the United Kingdom, he upheld that state's history, material resources, political philosophy, digital ownership or dependence, and the nature of the state's cybersecurity threats and adversaries constituted key variables that influenced the nature of cybersecurity strategies across states (Collier, 2017). These determinants enumerated by Collier attest that country-specific experiences and situations significantly impacts their adopted cybersecurity strategies. The policy insight from this understanding suggests that states must take caution in adopting cybersecurity strategies that may have been successful in other jurisdictions. In Ghana's case, the understanding demands that policymakers pay attention to the country's domestic peculiarities in designing and implementing its cybersecurity strategy. Therefore, the presence or otherwise of these indicators in the Ghanaian strategy will be assessed through a neo-institutionalism theory oriented framework in this study.

It is established from the above that domestic and international factors define the cyber management strategies of states. These factors span the country's economic, political, and social lives and security. However, with the ultimate objective of securing cyberspace through enhancing its cyber resilience and robustness, states embark upon the design of response strategies. Nonetheless, to realise an effective response strategy, the views presented above argues for a holistic consideration of domestic and external factors.

2.5.2 Elements of State Cybersecurity Strategies

Policymakers play a crucial role as the architects of strategies that can effectively address the intricate challenges of their state's cyber ecosystem. The complex interplay between cyber technology and governance in cyberspace operations has underscored the magnitude of this daunting task (Azmi et al., 2016, p.1). However, Swinton and Hedges (2019) propose that the cybersecurity design process follows an order with certain indispensable elements serving as guide for states. As outlined by the authors, these elements include clearly defined goals and objectives, prescribed risk management guidelines/policies, an established roadmap for overall maintenance, and a risk management plan (Swinton & Hedges, 2019). This perspective aligns with the Australian Computing Society's view that

> *"Good cybersecurity readiness encompasses an understanding of risks and threats to assets and information relevant to the organisation and its people, monitoring and detecting cybersecurity threats regularly, protecting critical systems and information, ensuring the organisation meets all relevant standards compliance, and having incident response plans in place in the event" (Australian Computing Society, 2016, p.51).*

Understanding a cyber-ecosystem and appreciating the path an organisation or state seeks to chart is critical for designing an effective cyber-response strategy.

In a similar vein, Ajijola and Allen (2022) notes that meeting required standards constitutes a critical step for a national cybersecurity response strategy. To them, strategies adequacy and effectiveness other than mere existence were central to producing effective cybersecurity and safety outcomes. They further posit that the ability of cyber strategies to inspire the attainment of desired outcomes hinges on three critical elements: their design, implementation, nature and possible impact. The authors underscore that for any cybersecurity strategy to be effective, at minimum, it should justify *why* it is necessary, *what* to do, *when* to do it, *who* is responsible, and *how* it is to be funded and implemented. These indicators could also be conceptualised as

(i) threat assessment, (ii) a plan of action, (iii) stipulated timelines, (iv) the assignment of responsibilities across stakeholders, and (v) allocation of resources. For a state to realise an effective cyber-security strategy, its policies, decision-making processes, and programs must reflect these elements.

On their part, Azmi, Tibben and Win (2016 p.1) also suggest that cyber-security strategies must seek a balance between the accepted norms of a country and the opportunities presented by the internet to maintain any possibility of being effective. Achieving such a marriage sometimes appears difficult because the disruptive nature of the internet calls into question many of the accepted norms in critical sectors such as military affairs, public policy, the private sector and civil society (Lyytinen & Rose, 2003). For instance, governments' responsibility in balancing openness and information free flow makes internet governance a tricky puzzle (Arsneault et al., 2005; OECD, 2012). Either way, the phenomenon poses severe consequences because while strict security policy promotes stability, it also reduces the margin of benefits from information technology (Arsneault et al., 2005). In order to salvage the above situation, states need to always understand their specific challenge and where the vulnerabilities lie. Such understanding will help determine suitable solutions in the technical, policy, economic, or social spheres relevant to addressing the challenge (De Guzman, 2014).

Based on the understanding above, it is sound to conclude that states' cyber strategies design targets to produce outcomes that align with general standard practices (NCS-Guide, 2021). However, each state can select and implement practices that align with its strategic objectives and ecosystem priorities (NCS-Guide, 2021, p.34).

The diagram below depicts a flowchart for developing a tailored national cybersecurity strategy to meet countries' unique needs and priorities.

Figure 1 Elements of Cybersecurity Strategy

Source: NCS-Guide, (2021)

2.6 CHALLENGES ASSOCIATED WITH CYBER SECURITY STRATEGIES

Despite the high aspirations that comes with states' cyber-security strategies, their design and implementation could be more challenging. Some notable challenges include balancing cybersecurity and human rights, cybersecurity capabilities, the transboundary nature of cybersecurity threats, implementation financing, and the cybersecurity skills gap. These are expatiated below;

2.6.1 Cyber Security and Human Rights Balance

It is worth noting that although cyber norms and laws differ, they operate alongside each other. Thus, while laws are not entirely autonomous of norms, they help strengthen and refine a given

norm's behavioural expectations (Finnemore, 2017, p.3). Again, laws appear more binding and command compulsory obedience, but norms are broader and thrive on the logic of appropriateness and goodwill (Finnemore, 2017, p.3).

The significance of guiding behaviour on ICT usage and mitigating of harmful activities that threaten domestic and international peace and security remains a critical focus in cybersecurity discourse (Dunn-Cavelty & Wenger, 2020). Cyber norms, or norms of cyber behaviour, have emerged as a powerful tool for fostering positive conduct within the cyberspace. They promote transparency and confidence-building measures and have been at the forefront of cyber related conversations (Hitchens & Gallagher, 2019; Sabbah, 2018; Osula & Rõigas, 2016, p.11). Their role in fostering predictability, trust, and stability in the ICT space (Osula & Rõigas, 2016, p.11) notwithstanding their occasional clashes with other human rights elements (Finnemore & Hollis, 2016; Grisby, 2017), is conspicuous.

Cybersecurity norms, which seeks to regulate the activities of Internet users, are also expected to uphold their rights. Thus, cyber strategies that promote the development of domestic cyber legal frameworks, which criminalize inappropriate actions and empower institutions to sanction appropriate punishment, must not be seen as infringing on other human rights and freedoms. In this respect, adopted strategies are required to promote approaches such as encryption, anonymity, vulnerability disclosure, and ethical hacking, which are consistent with respect for the rights of individuals (NCS Guide, 2021, p.49). It is worth acknowledging the difficulty in attaining this balance, which has manifested in the global decline of internet freedoms (Turianskyi, 2018, p.5; Freedom House, 2016). Thus, a perfect balance of the two looks daunting, but policymakers at both the international and state levels must endeavour to observe it.

2.6.2 National Cyber Security Capability

States appropriate their available assets and resources to advance their strategic interest in cyberspace. Craig (2018) categorizes these capabilities as either latent (societal-based resources) or active (computer network operations). Also, while states' response strategies are defined by the prevailing or dominant threats in their cyber ecosystem (Makridis & Smeets, 2019), the actual implementation of the strategies are based on their response-ability and preparedness.

Like other state capabilities, national cybersecurity capabilities ride on various material and human factors. Borky and Bradley (2018, p.7) identify three of these critical defining elements to include technical measures (public key infrastructure, security testing, Policy servers), physical measures (placing sensitive information or other protected resources behind barriers) and procedural measures (operational and practical procedures for maintaining security controls effectiveness and vulnerabilities elimination). A deficiency in any of these elements has adverse effect on the policy or implementation schemes of cybersecurity in the state.

2.6.3 Trans-boundary nature of cyber threats

The virtual nature of cyberspace makes its activities and effects transboundary. Therefore, managing cyberspace's challenges require a practical cybersecurity approach framed along transnational coherence and coordination among states (Calderaro & Craig, 2020; Craig, 2020). The cyber capabilities of individual states are essential for the collective management of cyber insecurity in a region or globally. But the varied cybersecurity threats and capabilities of individuals states influences their strategies.

Highlighting this variations of threats and the consequential states response, Calderaro and Craig (2020), Craig (2020), and Van der Meulen et al. (2015) indicate that countries of the Global North are much ahead of their Global South counterparts in cybersecurity capabilities. This situation influences the need for variations in their country's cybersecurity management strategies. Even so, the National Cybersecurity Strategy Guide has maintained that although peculiar circumstances and priorities could define states' cybersecurity strategies, such arrangements must reflect an encompassing understanding and dynamics of the overall digital environment (NCS-Guide, 2021, p.28). Admittedly, attaining convergence for these two situations for effective collaboration remains quite challenging in cybersecurity strategy design.

2.6.4 Cybersecurity Skills Gap

The fast rise in cyber innovations, usage and associated cyber threats has created a demand for a large cyberspace management workforce. Unfortunately, the demand dwarfs the available experts globally. For instance, Neto, Obiso, and Baayen (2022) have projected that there will be over 3.5 million unfilled cyber-security jobs by 2025 worldwide. While this remains a global challenge, developing African countries are much affected. In addition to the limited numbers, the developed countries are poaching the existing professionals in the developing countries due to poor working conditions (Neto et al., 2022). Since countries need these professionals to design and implement cybersecurity strategies, the efforts of developing African states in training and retaining these workforce is continually being challenged.

2.7 SCHOLARSHIP ON CYBER SECURITY IN AFRICA

Since the discovery of the internet's enormous opportunities in responding to Africa's nagging development question, the discourse on securing it has become topical among practitioners and scholars. The development constitutes a critical conversation in Africa because, while

cybersecurity concerns remain global, the particular situation of Africa appears more problematic. This phenomenon is because apart from the continent missing out on the benefits the revolution offers, the absence of proper management could also further derail and damage the already dire developmental condition and infamous insecurity reputation of the continent (Kshetri, 2019 & Gady, 2010). This phenomenon traverses the various aspects of the continent's life that cyber ecosystem impacts.

Discussions on the continent's cybersecurity landscape, for instance, have also been advanced in several studies. As part of this body of literature, Kshetri (2019), van Vuuren, Leenen and Pieterse (2020) examined the threats to Africa's cyberspace. They both pointed out cybercrime as a devastating cyber challenge wrecking the African cyber ecosystem. Factors such as weak cyber defence or infrastructure and developmental deficit on the continent have been identified as rendering the continent's cyber ecosystem susceptible to criminal cyber activities (Target, 2010; Calandro & Berglund, 2019) and presented its cyberspace as a launchpad for cybercriminals targeting victims in other continents (Global Cybersecurity Index, 2020).

The above outlook of the continent's cyber landscape offers credence to the property crime and poverty, unemployment and inequality nexus claim established in the extant criminology literature (Jiyong et al., 2019; Raphael & Winter-Ebmer, 2001). In his study on Nigeria, Akinyetun (2021) buttressed this nexus claim within the continent's cyber ecosystem, concluding that poverty and unemployment positively correlate with cybercrime in the West African country. Tying these linkages with the fact that most African workers, particularly the ICT savvy community, who potentially could make much money from the dark web, are placed on meagre salaries, renders the possibility of cybercrime further festering on the continent.

In a similar study on the trends in cybersecurity threats in Botswana, Sarefo, Dawson, and Banyatsang (2023) reports a worrying rise in the manifestation of cyber threats in the southern African state. They found the most manifesting threats to include malware, phishing, unauthorised access, denial of service, and ransomware (p.19). Most of these threats have the actors acting with monetary incentives as the ultimate goal. This understanding confirms Borky's (2019) findings on the nature of the African cybersecurity threat landscape. He explicitly establishes that the African cyber ecosystem threat actors include insiders, hackers, organised criminals, terrorists, and advanced persistent threats (APT) in state-sponsored military or espionage operations. By adopting such strategies as unauthorised access, phishing, and ransomware, these threat actors ultimately scan for money making avenues to fund their personal or groups' activities.

The downsides of cyber technology on the continent have also been discussed by a section of the literature, including Shani (2019), Warren (2015), Muna and Díaz Pabón (2022), and Toussi (2022). With many of these scholars focusing on social media, they argued that cyber technology could pose some adverse impacts if not properly used or managed. Toussi (2022, p.4), for instance, indicated that apart from helping to redefine political discourse, enabling strong public participation, organising, and protests that have led to autocratic leaders' overthrow in countries such as Sudan and Algeria, social media has also become a propaganda tool for states governments, civil society, individuals, organised groups and foreign elements. Alike, Shani (2019) argues that with its incredible reach and self-selection mechanisms, social media's social engineering algorithm allows for deployment in marketing. It also functions as a more effective propaganda tool and can flame hatred and fuel conflict at a fraction (Shani, 2019). These assertions support the findings from a survey in 24 African countries on the relationship between communication technology and political violence (Warren, 2015). The findings established social media expansion

as directly contributing to increased incidences of collective violence (Warren, 2015). Muna and Díaz Pabón (2022) also affirmed this view by establishing that social media proliferation had promoted worrying acts of hate speech and open violence attacks, such as groups' elimination in Ethiopia.

Despite these clear concerns, social media platforms and their platform hosts have continually been challenged with timely identifying and blocking violence-fomenting activities on their platforms (Muna & Díaz Pabón, 2022), before they escalate or degenerate into confrontations. As observed by the Collaboration on International ICT Policy for East and Southern Africa (CIPESA), ensuing happenings and tensions in Cameroon, Ethiopia, Kenya, Nigeria, and Uganda highlight these challenges (Toussi, 2022). Disinformation actors, both citizens and foreigners, leverage the viral power of social media. They find it as a viable conduit for spreading fake news and false allegations. With its devastating effects of eroding trust in the continent's democratic institutions and fueling politically motivated violence and existing ethnic divisions and tensions, it could function as a great destructive tool.

Owing to the conspicuous rise in threats on the continent and their potential effects, studies including Cole et al. (2008), Adomako et al. (2018), and Kshetri (2019) attempted to understand how the continent has fared in their management. Cole et al. (2008) identified some efforts by African states to address the continent's cybersecurity threat issues. They concluded that most of these state's management approaches consider the phenomenon more an economic development issue than a core national security concern. While the authors' conclusion may have reflected the times of their study, during which time most African states had barely integrated cyber technology into their governance and economic space, it sets a perfect benchmark to ascertain whether such observation of cybersecurity being essentially economic other than security concern still pertains.

The authors, therefore, provide a baseline understanding of how African states have progressed in initiatives towards addressing the challenges of their cyber ecosystem, which the current study builds on.

Adomako et al. (2018) also examined six African countries' CERTs and bemoaned African states lacklustre approach in dealing with cyber threats. According to them, the examined CERTs revealed that most African countries operated with imported technologies. Given the absence of a consensus on how cyberspace is regulated, most countries are tempted to adopt the policies and designed management strategies of technologically advanced states or producers of the technology. This situation creates a mismatch in their adopted strategies or policies, yielding less positive or counter-productive impact in addressing the peculiar challenges and helping to maximise the opportunities the space offers (Adomako et al., 2018). The authors' conclusion did not object to states adopting international benchmarks on cyber security strategies design but were against the holistic importation of such practices from another country.

On his part, Kshetri (2019) indicated in his assessment of the cyber response strategies on the continent that most African countries have, in principle, accepted cybersecurity as part of a national security issue. He found much of the attempts by these countries to address the challenges and threats emanating from the space as concentrated on legal measures with little focus on infrastructural and capacity building (ITU, 2021; Kshetri, 2019). He indicated the detachment of this approach from the prevailing realities in the space. The author revealed the issues of weak or non-existing cyberinfrastructure, funding constraints, high cyber illiteracy and skills gaps, and weak cyber legislation and enforcement as contributing to the lax in the continent's cyber-security governance efforts (Kshetri, 2019, pp.78-80). This inadequate resources allocation by African states for cybersecurity management concerns has also been affirmed in Reva (2020), as a major

concern in the continent's cyber governance. Both authors, hence, argue for African states and organisations to increase their investments in cybersecurity technologies and related trainings' for employees and policymakers in the industry. The current study would thus probe the feasibility of this recommendation against the prevailing situation in the continent's cybersecurity ecosystem.

Another set of studies that focused on cybersecurity on the continent, such as Lebogang, Tabona, and Maupong (2022), Amankwa (2021) and Turianskyi (2018; 2020), examined how the adopted cybersecurity strategies align with international cybersecurity standard practices. On their part, Lebogang, Tabona, and Maupong (2022) examined the national cybersecurity strategies of five African countries, including Botswana, Rwanda, Mauritius, Ghana, and Nigeria. Focused on establishing the extent the strategies meet the standardised cybersecurity management strategies indicators proposed by the ITU, the authors established some trend of improvement in these countries experience overtime. The findings indicated improved levels of their cybersecurity readiness, although there were variations across. While confirming Sabillon et al.'s (2016) argument of variations in African states' cyber-security experiences (threats and capabilities), the study also revealed that the countries' existing institutional structures fairly conformed to international standards and qualified the various states to engage in international collaborations and alliances for cybersecurity strategy implementations. The silence of their findings on whether or not those strategies considered the local context issues, which constitute critical cybersecurity management consideration, was however disquieting. Thus, while adopting international standards, such as the ITU's, as the baseline for cybersecurity management by African countries might not be entirely wrong, domestic environmental peculiarities and their impact on the response strategies is worth considering and interrogating. Amankwa (2021) concurs with this position in his argument that domestic elements like literacy rate and technological advancement, have

consequential impact on cybersecurity management. Zua, (2021) and Ebaye, (2009) identification of both indicators being at low levels in many African states further render the phenomenon much concerning. Again, the nagging developmental issues in health, water, and food insecurities, considered more pressing than cybersecurity, fizzle out governments attention for the latter. This situation has manifested in the low budgetary allocations for cybersecurity management activities tagged mostly as "luxury items" (Kshetri, 2019, p.78). These considerations undoubtedly offer the African cybersecurity approaches some dynamism, which this study factors into assessing the adequacy and appropriateness of the Ghanaian cybersecurity management strategy.

The concern of how the rights of cyberspace users align in the cyber-security management processes has also featured in Africa's cybersecurity literature with works such as Hunter & Tilly (2017) and Turianskyi (2018) and (2020). This conversation became much more pronounced when the UN Human Rights Council declared the internet a human rights issue in 2016, citing its close association with rights and freedoms of association, speech and information (UNHRC, 2016). Citing the situations in some African countries, Hunter & Tilly (2017) observed that despite Kenya high internet penetration rate and Access to Information Act, 2016, which upholds citizens' rights in cyberspace, government officials could still use older laws including the Section, 29 of their Information and Communications Act, to silence dissenting voices. Similarly, in the seeming liberal South African society, cyber-security regimes grant a broad mandate to the government, justifying it to clamp down on criminals and spies (Hunter & Tilly, 2017). This censored cyberspace phenomenon is not different, if not worse, in Ethiopia and Eritrea.

In light of the above observations, studies such as Turianskyi (2018 and (2020) advanced assessments of how African states have endeavoured to balance the complexities of their cyber landscape experiences. In his 2018 article, "Balancing Cyber Security and Internet Freedom in

Africa", Turianskyi acknowledged the complexities involved in manoeuvring the issue. He called for a carefully considered middle ground where states do not renege on their duty of securing their cybersecurity space nor infringe on users' rights. To ensure this, he argued for using more measured security policies to safeguard citizens' rights (Turianskyi, 2018, p.6). In a similar view, as forwarded by Turianskyi (2020), a multi-stakeholder approach is recommended that brings together technology firms, civil society, businesses, and policymakers in the cyber governance process to form workable checks and balances. Such an approach, he argued, had delivered much success in Mauritius and could, therefore, be projected to succeed in other states.

Eboibi (2020) and Richards and Eboibi (2021) attempted to appreciate the levels of cyber hygiene within the continent's cyber ecosystem. Eboibi advanced this objective through a comparative study of the USA, the United Kingdom, and Nigeria's cybersecurity landscapes. The findings, unsurprisingly, showed that unlike the US and the UK, Nigeria's cyber ecosystem lacked preventive and enforcement measures capable of curtailing the activities of cybercriminals. According to the author, the few existing institutions lacked adequate capacity building, professional competence, and inter-agency cooperation for effectively policing cyber criminals' activities. Eboibi's revelations on Nigeria affirmed the broader African situation as earlier found by Bada, Von Solms, Agrafiotis (2019) and Signé and Signé (2021). In their collaborative example, Von Solms and Agrafiotis (2019) lamented the worrying incidences of cyber threats and high levels of citizens' lack of cybersecurity awareness on basic cyber-hygiene protocols in Africa. Alike, Signé and Signé (2021) affirmed this bleak picture of the continent's cyber-security landscape. Eboibi, hence called for immediate steps aimed at institutionalising protocols to help address the nagging cyber concerns including the continent-wide high data breaches.

Following African states' resolutions and commitments towards addressing their cybersecurity threats, Richards and Eboibi (2021) assessed the level of improvement in the continent's cybersecurity landscape resilience. They established that various cybersecurity management interventions in African states have begun to yield some results but have not been devoid of setbacks. The particular issue of Insider-Related threats, according to them, has become a crucial consideration in equipping citizens with cybersecurity skills (Richards & Eboibi, 2021). Even though the study appears descriptive and fails to provide alternative approaches and solutions to the cybersecurity management challenges faced by African states, the authors' observation offers a basis for an in-depth analysis of the cybersecurity management efforts by African states with Ghana as a case study.

Another subject matter on Africa's cybersecurity resilience, which has received substantial attention in scholarship, is the level of cybersecurity awareness among both cyber policymakers and users. The basis for these assessments is that even though cyber awareness-raising and education responsibility are shared between the state and other actors within cyberspace (Bada et al., 2019, p.109), the former owns the primary duty. The "Her Majesty's Government" (HMG) Security Policy Framework clarified the significance of this role by asserting that "people and behaviours are fundamental to good security and the right security culture, proper expectations and effective training are essential in security governance. Moreover, these everyday actions and the management of people that contribute to good security are primarily the state's task" (Bada et al., 2018, p.1). The stimulation, motivation, and reminder purposes that awareness serves for the audience in a community or ecology (Peltier, 2005), thus, occupy an important place in cyber-security policy or strategy schemes. Besides enhancing users' knowledge about security, the

practice also changes their attitude towards cybersecurity and general behaviour patterns (Bada et al., 2018).

It is instructive to note that the similar perspective to the above had earlier been forwarded in Gcaza and Von Solms's (2017) assessment of cybersecurity culture's role in cybercrime mitigation. Using the South African experience as a case study, the authors noted the importance the South African government promotion of a cybersecurity culture as provided for in its 2012 National Cybersecurity Policy Framework (NCPF), towards enhancement of its cyber resilience. However, the authors indicated that the South African approach had not delivered the expected results because the NCPF provisions lacked practical and strategic acculturation steps. Other factors, such as poor government accountability mechanisms, poor stakeholder engagement, and the lack of research and skilled human resources, have further deranged the strategy's prospects (Gcaza & Von Solms, 2017, p.15). Despite these implementation challenges, the authors' findings align with Tolnaiova and Galik (2020) and others who suggest that cyberspace is a community with its own culture and that individuals can only live securely within it by getting accustomed to its principles and norms.

Given that the propriety of a cybersecurity strategy is vital for effective programs, the NIST framework provides three alternatives for organisation structuring. These include the centralised, partially decentralised, and fully decentralised. As suggested by the NIST framework, the program design sequence begins with a needs assessment. The process then evolves to strategy development, the design of an awareness training program, and then to program implementation, (NIST, 2018, pp.9-10). All designs and implementations of awareness campaigns are projected to succeed if they assume "learning continuum" posture (NIST, 2018, p.10). The process, therefore,

entails awareness that evolves into training, and subsequently into education (Bada et al., 2018, p.2, 2019).

Against the above background and the bleak picture reported of the cybersecurity situation on the continent, Bada, Von Solms and Agrafiotis, 2018 and 2019 advanced an assessment of six African countries' cybersecurity situation. With twelve experts' sample engaged through focus group interviews in the countries, the authors assessed their cybersecurity capabilities along the Cybersecurity Capacity Maturity Model for Nations (CMM) developed by the Global Cyber Security Capacity Centre (GCSCC). The analysis involved two layers. The first was an analysis of the qualitative data on awareness campaigns and the extended reflections on best practice approaches for national awareness campaign development in 2018. Its findings became the framework for the second, which analysed the qualitative data from focus group interviews on the same project in 2019.

The two studies by Bada et al. generated informed conclusions on cyber-security awareness in Africa. The authors established that despite the significance of cybersecurity awareness in reducing the success rate of cybercriminal activities, all the countries studied recorded very low levels. This unfortunate situation, aggravated by the low ICT literacy rates and policymakers' underestimation of cyber threats, has resulted in lackadaisical attitudes of policymakers towards its redress and further rendered the continent's cyber ecosystem porous (Bada et al., 2019, p.115). To strengthen the country's response strategies, the authors recommended the establishment of regulatory authorities to coordinate the existing ad-hoc awareness campaign efforts and tailor the awareness campaigns towards targeted susceptible groups, such as businesses, mobile phone users and board executives, during these awareness creation campaigns (Bada et al., 2019, p.20). The authors'

findings thus affirmed the possibility of African states shaping their societal norms on cyber security through awareness creation and enhancing their cyber-security resilience.

Despite the rich understanding provided by these studies on Africa's cyber ecosystem, their findings cannot be held as sacrosanct over time because of the continuous evolving character of cyberspace. Therefore, the response and management outlook of these African countries, including Ghana, which have witnessed several developments after these studies may have assumed new characters. In Ghana, for instance, significant developments including the establishment of a cybersecurity regulatory Authority to regulate the space, have occurred within the considered period. In fact, the authors envisaged such developments which formed the basis of their recommendations. A reassessment of the country's response strategies using similar parameters to establish the impact of the undertakings of these countries, therefore, turns up as a worthy course. By examining Ghana's cyber-security management strategy, this study advances this pursuit.

The above studies show that African states have embraced the need to address the challenges that come with the use of cyber technology to maximise the benefits of cyberspace. A chunk of these studies have concentrated on assessing the continental cyber response mechanisms, governance efforts, and how they fared in mitigating the threats and contributing to maximising the shared opportunities provided by the space. However, a significant concern that runs through the findings of these studies relates to the appropriateness of these redress mechanisms, which are widely adopted on the continent for the task. The peculiarity of the continent's cyber ecosystem, mainly defined by the critical role of human security needs in cybercrime and coupled with the technological infrastructural and cyber skills gaps, have been cited as reasons that warrant the response mechanisms by African countries to be circumspect in adopting wholly international

standard practices. The studies, therefore, argue for African states to adopt distinctively nuanced response strategies using international indicators as frameworks.

2.8 CYBER SECURITY STUDIES ON GHANA

Discussions on Ghana's cyberspace have received some attention in academia. A bulk of the studies on this discourse have focused on cyber awareness and perceptions of citizens and organisations assessments (Forson-Adaboh, 2022; Agbeko, 2021; Affum, 2019; Adu & Adjei, 2018; and Botchwey, 2018). Generally, these studies have indicated a relatively low rate of cyber awareness among both literate and illiterate internet users in Ghana. Nevertheless despite their insightful revelations, the studies gave little considerations to understanding the reasons for such a phenomenon or its effect and how to mitigate it. These unconsidered parameters will be delved into in this study to help understand how such issues have influenced the state's cybersecurity strategy and the required mitigation measures for their management.

Another cohort of these studies, such as Baylon and Antwi-Boasiako (2016), Warner (2011), Motiwala (2017), Danquah and Longe (2011), and Akuako (2022) have discussed the nature of the country's cybersecurity threats and response mechanisms. For instance, Warner (2011) and Motiwala (2017) focused on Ghana's cyber threats profile and the government's policy response through its policy and framework design targeting current and future threats. Through a broad overview of cybercrime activities in Ghana, Warner (2011) sought an understanding of the causative factors and strategies of cybercriminal operations in Ghana. With a particular emphasis on local-level realities, the author explained that domestic drivers greatly influenced the cybercrime phenomena in Ghana. He pointed to geopolitics, the techno-spiritual paradigm of "sakawa", and the "social justice" justification philosophies as drivers significantly defining the Ghanaian cybercrime phenomenon (Warner, 2011, pp. 741-45). Indeed, Western cybersecurity

literature has paid little or no attention to these drivers, making their approach and resultant conclusions incomplete and, worse, unrealistic and inapplicable to specific local cybersecurity contexts such as Ghana. Warner's findings, thus, revealed some of the distinctions inherent within the Ghanaian cybercrime landscape, which consequently points to the need for diverse approaches in both assessment and redress. It also affirms the peculiarities of states' cybersecurity challenges and the need to consider the same in their management strategies.

On his part, Motiwala (2017) discussed the gaps that persisted in Ghana's cybersecurity management practice despite the country-level and regional management's efforts. He argued that the country's cybersecurity management practices required comprehensive domestic regulatory instruments and awareness creation among cyberspace users for any significant economic vitality and national security contribution. Instructively, the 2017 Policy Brief of the Media Foundation for West Africa (MFWA) identified the absence of such issues as the cause for the continued manifestation of cyber insecurity in Ghana. In their critical opinion, a lack of cybersecurity culture, low level of cyber literacy, and existing legislation and cybercrimes delink stifled the management processes (MFWA, 2017 pp.15-16). The findings and conclusions of Warner and Motiwala on the Ghanaian cyber landscape are revealing and provide a baseline for a comprehensive assessment of the country's cybersecurity strategy, which is the core objective of this study.

In their study on cybercrime in Ghana, Danquah and Longe (2011), through ethnography and examination of published texts' chronicled the operationalisation of cyber deception in Ghana. Their findings showed that cybercriminals in Ghana typically hardly engage in spoofing, page-jacking, and auction/merchandised fraud. They discovered social engineering in syndicated cyber deception and theft as the dominant technique deployed by cybercriminals to advance their activities in Ghana (Danquah & Longe, 2011, p.169). This revelation provides an understanding

of Ghana's cyber threat landscape and justifications for studies with a methodologically broad scope expanding to the current times for a better appreciation of developments and patterns. By building on their contribution, the current study seeks to establish whether such findings are still valid or whether some threat factors that deserve attention may have emerged.

The authors also made an interesting call for the deployment of internet users as frontlines to soar the potential of achieving effective defence mechanisms (Danquah & Longe, 2011, p.170). As forwarded by the authors for cyber-security management, this argument warrants further consideration and serves as a template for assessing Ghana's cyber threat strategy.

Akuako (2022) extended the contours of examining cybercrime governance in Ghana by focusing on "sakawa". In the work *"The Sakawa Boys: A Critique of the Policing of Cybercrime in Ghana",* the author attempted to identify the appropriate policing techniques required to manage cybercrime in Ghana. Consenting to previously held views by Warner (2011), Ennin (2015), and scores of extant criminology and cybersecurity literature on the nexus between cybercrime and poverty (Kelly, 2000; Jiyong et al., 2019), Edward Akuako intimated that cybercriminal activities in Ghana were economically induced. This prompted his resistance against the adoption of repressive policing, which deemed inappropriate approach that would generate little or no positive effects (Akuako, 2022, p.62). A human security approach to policing that prioritises mitigating citizens' economic difficulties and needs is, hence, considered by the author as a better approach for managing Ghana and Africa's cybersecurity ecosystem (Akuako, 2022, p.64). These conclusions and admonishment align with Akinyetun's (2021) findings that poverty constituted a major influencing factor of cybercrime in Nigeria. Therefore, Policymakers on the continent need to consider the prevailing poverty and other human security challenges when designing their cybersecurity management strategies.

Scholars have also looked at Ghana's cyber-security capabilities and strategies. For instance, Apau and Koranteng (2020) assessed Ghana's cyber capabilities in Digital Forensic Investigation (DFI) through the established legal infrastructure, technical mechanisms, capacity-building programs, and organisational infrastructure and cooperation mechanisms among relevant institutions. The authors acknowledged the existence of legislations and mandated institutions and their impact but maintained that the state's progress in attaining DFI had ground rather slowly. They attributed scattered legislation, cumbersome legislation processes, and capacity deficiency of mandated institutions to the ineffectiveness of the state's DFI. Apau and Koranteng's admonition that the availability of legal instruments and infrastructure alone was insufficient for realising robust digital space management in Ghana appears critical to this study. Their findings indicate the need to effectively coordinate these pieces together to produce a robust response mechanism. However, it is essential to note that the study's restricted scope to just DFI did prevent a broader understanding of the country's cybersecurity framework and a deeper assessment of the management process. This gap is addressed by this study through an expanded scope and more nuanced assessment that will consequently help advance the frontiers of Ghana's cybersecurity scholarship.

Ouassini and Amini's work on "*the overview of Ghana's cybersecurity strategy"* in the *"Companion to Global Cyber-Security Strategy"* (2021) is arguably one piece of study that came close to discussing the objective of this current research. The authors discussed the nation's cyberspace legal reforms from the 2008 National Information Technology Agency to the 2018 National Cyber Security Center (Ouassini & Amini, 2021). The methodologically descriptive study chronicled the legal strategies employed by Ghanaian cyber stakeholders to combat the threats in cyberspace. Despite the significant contribution of the studies to understanding Ghana's cyber strategy trajectory, their restricted scope to just legal strategies from 2008 to 2018 resulted

in a limited analysis and appreciation of what inspired such legal provisions and policies. This concern aligns with Doreen Bogdan-Martin, a former Director of ITU Telecommunication Development Bureau's view that digital infrastructure, digital skills, and resources other than mere legislation were more central in cyber capacity gap bridging projects cybersecurity promotion (ITU, 2020, p.iv). Her counsel to developing states to go beyond legal strategies to attain cyber-security robustness is a worthwhile call that deserves consideration in any examination of a state's cyber-security strategy as advanced in this study. This study takes cognisance of this recommendation and would factor it into ensuring a comprehensive appreciation of the country's cybersecurity strategy.

2.9 SUMMARY OF CHAPTER

The chapter conceptualizes the salient terms used in the study and reviews scholarly literature on cyber security. The review spanned general cyber-security literature in IR and established that cyber security has become a topical issue for discourse in international relations scholarship. This development has primarily been due to the significant impact of cyberspace on states' socio-economy and national security and its borderless effect that necessitates collaborative management efforts from states. This collaborative nature of cybersecurity management underscores the urgency and importance of this study in providing an empirical understanding of the adequacy of the Ghanaian cybersecurity management strategy.

Within the cyber-security literature on the African continent and Ghana, the review shows a similar trend of conversation on the subject matter. The nature of Africa and Ghana's cyber security threat landscape, response mechanism, and challenges have featured prominently in the discourse. However, in the particular case of Ghana, the review indicates that despite the substantial analyses of the cyber threats landscape and management, state capability, and associated challenges, a

comprehensive assessment of the adequacy and appropriateness of the adopted strategies and frameworks has yet to be attended. The few studies that came close to advancing such an analysis limited their focus to only the issues of legislation applicability. The review, therefore, establishes the need and relevance of this study in providing an empirical understanding of the adequacy of the Ghanaian cybersecurity management strategy.

.

CHAPTER THREE

METHODOLOGY

3.0 INTRODUCTION

This chapter embodies the research methodology for the study. Its content involves the critical interrogation of the methods employed in the research and explains the abstraction underlying the claims and views used in the study (Hughes & Sharrock, 2007, p.35; Ruane, 2005, p.48). The chapter, hence, provides the study's theoretical orientation or philosophical underpinnings and the justification for the methods and tools for collecting data to address the research questions. It also spells out and justifies the type of research undertaken and the techniques deployed for data collection, validation, and analysis.

3.1 PHILOSOPHICAL PARADIGM

Scientific researchers' actions in generating and interpreting knowledge claims about reality are guided by belief systems (Chua, 1986; Myers, 2009). These belief systems/paradigms are defined by questions on three elements: ontology, epistemology, and methodology (Guba, 1990). While Ontology explicates assumptions about the nature of reality, Epistemology denotes the evidentiary assessment and justification of knowledge claims, and methodology relates to those processes or procedures through which knowledge claims are created (Chua, 1986; Guba, 1990; Orlikowski & Baroudi, 1991 and Wynn & Williams, 2012).

The realm of mainstream IR and Security research has predominantly been explored through the *lenses of Interpretivism* and *Structuralism* philosophical paradigms (Kolasi, 2020, p.3). These paradigms offer contrasting perspectives, with Interpretivism focusing on individualist

explanations of social conduct and Structuralism advocating for collectivist interpretations (Archer, 1995; Mouzelis, 1995). Methodologically, interpretivists argue that actors' preferences, meanings, beliefs, and expectations explain social phenomena. On the other hand, Structuralists, drawing on Emile Durkheim's work, propose a collectivist methodology that views social reality as a product of intervening structures that shape human conduct (Kolasi, 2020 p.3).

Structuralists attempt to remedy Interpretivists' limitation of causation in social phenomena to only the unconstrained actions of individuals, straying them into focusing on only the constraining conditions. Consequently, the impact of an individual's agency and capacity on situations has eluded consideration (Sayer, 2010, p.66). In sum, whereas Structuralism fails to recognise any autonomy in the actions of individuals, Interpretivism also tends to ignore entirely the social context within which the activities of the agents are embedded. The dissatisfaction with the single attributions by these two prominent but opposing traditions led to the emergence of the Structuration Philosophical Paradigm (Kolasi, 2020, p.1).

3.1.1 Structuration

In the realm of social theory, Structuration theory stands as a significant departure from the traditionally non-existent relation between agents and structures. It offers a fresh perspective, drawing on the broad frameworks of renowned social theorists like Anthony Giddens, Pierre Bourdieu, and Roy Bhaskar (Kolasi, 2020, p.2). Admittedly, it was Anthony Giddens whose groundbreaking attempt to reconcile the interpretive and structuralist traditions gave birth to Structuration as a social theory.

Giddens (1993, pp163-164) intimated that interpretive sociologists focus on motivational thoughts as an explanatory variable for all human behaviour and ignoring the causal conditions of action

was problematic. He forwarded that such conception fails to account for power asymmetries and divisions of interest in society (Giddens, 1993, p.164). While consenting to Interpretivists' assertion of the human actors being the centre of meanings and free agent that creates social realities, he also agreed with the structuralist on the restrictiveness of the area of human activity (Layder, 2006, p.164). He believed that though people produce society, they do so as historically positioned actors under conditions not entirely controlled by them. Giddens's attempt to avoid shortcomings in opposing structures as "external" to human action but a mere source of restraint to agents' initiative (Giddens, 2004, p.16) led to the conceptualisation of societies as "social systems" without characteristics that researchers could examine independently of the actors' motives and reasons (Layder, 2006, p.161).

The Structuration theory, therefore, adopts a balance of agency and structures in explaining a social phenomenon, leading to what Giddens terms the "duality of structures". This procedure describes the mutual relationship between human actions and social structures. While the philosophy considers human agency as the central variable, Giddens still recognises the role of social structures in social actions (Wendt & Shapiro, 1997, p.176). The Structuration paradigm, hence, provides that society or social phenomenon is a product of the active constructive skills of its members influenced by circumstances that they are aware of and the resources available to them (Giddens, 1993; Kolasi, 2020, p.2).

Applying the philosophical underpinnings of Structuration theory to this study, which evaluates the adequacy and effectiveness of Ghana's cybersecurity strategy, portends significant insights. This is particularly relevant because it provides the intellectual framework for examining the critical variables of the issue. For instance, the design and implementation of Ghana's

cybersecurity strategy are influenced not only by established structures created by national and international cyber-threat norms and laws but also by the actors' agency in devising innovative solutions to address their unique challenges. This dual structure approach thus offers a comprehensive understanding of Ghana's cybersecurity response strategy, considering international structures and country-specific circumstances.

Again, given that structures in themselves are not self-imposing but require implementation, the philosophical paradigm suggests that to assess the adequacy and effectiveness of Ghana's cybersecurity strategy, the domestic and international structures must be considered by the policymakers alongside the peculiar domestic issues of the state. The strategy's appropriateness, therefore, depends on ticking the boxes of standardised cybersecurity management processes and identifying and responding to cybersecurity threats and related issues in the country. An omission of either would result in a skewed analytical framework and prevent a better and holistic appreciation of the phenomenon. Indeed, while structures are essential in such assessments, they do not constitute sufficient conditions for realising a robust cybersecurity strategy. The consideration of the domestic issues that impact both the threats and implementation processes of structures peculiar to states is thus required. The Structuration paradigm, therefore, provides a methodological framework to respond to or interrogate these variables sufficiently.

3.2 RESEARCH APPROACH

As defined by Creswell (2014 p.1), the research approach involves the research plan and the procedures spanning the "steps from broad assumptions to detailed methods of data collection, analysis, and interpretation." It focuses on identifying the appropriate approaches required for studying a research topic. The researcher's philosophical assumption(s), the nature of the research

problem, and the specific research methods of data collection, analysis, and interpretation deemed appropriate for the study inform such a decision (Creswell, 2014, p.1).

Research approaches come under three main types: qualitative, quantitative, and mixed methods (Creswell, 2014; Williams, 2007, p.65). The preference of a researcher for any of these approaches is based on the sort of anticipated data required to sufficiently respond to the set of research questions under consideration (Williams, 2007, p.65). It is worth acknowledging that each approach has methods of collecting and analysing data on a problem and, as such, wields its distinct strengths and weaknesses. All three approaches have seen wide acceptance and usage by researchers with diverse justifications. Based on the objectives of this study, the qualitative approach is considered appropriate in gathering and analysing the required data to appropriately and satisfactorily address the research questions.

The Qualitative Research Approach aims at "exploring and understanding the meaning individuals or groups [inductively] ascribe to a social or human problem" (Creswell, 2014, p.34). Denzin and Lincoln (1994), cited in Biggam (2012, p.86), also indicated that the qualitative approach comes as an apposite method when a researcher seeks to analyse situations in their "natural settings" and interpret people's meaning of phenomena. In other words, qualitative research prevents respondents' positions from being sullied by the researcher's ideas, offers "systematic empirical enquiry of meanings", and analyses phenomena through verifiable means (Shank, 2002, p.5). These qualities render the qualitative approach the most appropriate for social research that seeks an in-depth understanding of the cybersecurity management strategy of developing African states with Ghana's situation as a case study. Therefore, a qualitative design is appropriate for this study because it helps unpack the elements and provisions of the state's cybersecurity strategy and

measure them against best practices and expert respondents' perspectives on its cybersecurity threats.

A qualitative research approach is also appropriate in this study because of the better and more profound meaning and understanding it provides on social research questions. According to Tewksbury, this understanding stems from the approach's aim at providing a complete understanding of how people "understand, experience and operate within the settings that are dynamic and social in their foundation and structure" (Tewksbury, 2009, p.3). The approach, thus, affords researchers the appropriate research mechanisms for unpacking complex details of phenomena, including thoughts, processes and feelings that are often impossible to measure using a quantitative approach (Strauss & Corbin, 1998). The understanding and guiding principles that drove the construction of Ghana's cybersecurity strategy could thus be appropriately analysed using this approach. The approach, therefore, comes forth as the most suitable means for understanding the rudiments of developing African states' security management practices in general and cybersecurity management in particular.

Furthermore, the qualitative method fits appropriately in realising research objectives that require a deeper understanding of specific state information, beliefs, and opinions within their social contexts and how relationships influence states' decisions. This understanding has been underscored by Creswell (2014) and Mack et al. (2005), who identified qualitative study as the most appropriate approach for beliefs, emotions, opinions and behavioural assessments. The textual description associated with the qualitative approach also constitutes a better means of presenting the experiences, beliefs and influences of the people involved in the drafting and

management processes of Ghana's cyber security strategy. These scientifically viable features of the qualitative approach render it more appropriate for this structuration paradigm-designed study.

Andrew Bennett and Colin Elman argued that the above-enumerated advantages of qualitative research methods, particularly in the study of "complex and relatively unstructured phenomena," have given it the enjoyment of "an almost unprecedented popularity and vitality… in the international relations sub-field" and rendered it "indisputably prominent, if not pre-eminent" (2010, p.171 & 2007, p.499).

Despite the inspirations that the qualitative research approach offers for a deeper understanding of complex issues in social research, its limited sample sizes have often been cited by critics as rendering its results inappropriate for generalisation (Mack et al., 2005). It is important to note that this concern is not limited to qualitative studies but applies to all studies of any approach with a scope that does not cover the entire study population. Again, apart from the fact that the limitation's impact could be minimised through the adoption of appropriate sampling techniques, this study mainly seeks an in-depth understanding of Ghana's cybersecurity framework rather than seeking grounds for generalisation purposes. Moreover, the central objective of this study, which seeks to establish how Ghana has responded to her cybersecurity threats through its cybersecurity strategy, would require the perspectives of cyber experts, policy and technologically savvy people and cybertechnology end users in the country to provide relevant information for meaningful discussion of the issue. A limited sample size, therefore, becomes an insignificant and immaterial consideration and, hence, does not invalidate the preference for a qualitative approach for this study..

3.3 RESEARCH DESIGN

A research design refers to a study plan that provides a data collection and analysis framework for a research work (Leedy & Ormrod, 2001). It involves a detailed data collection and analysis strategy focusing on the research procedure and connecting the research questions and available evidence (Collis & Hussey, 2003, p.113; Yin, 2003, pp.19-21). A research design, therefore, comes as the blueprint for conducting a research study and involves a detailed description of the research approach, study setting, sampling size, sampling technique, tools and methods for data collection and analysis to answer the research questions.

Research designs can be broadly categorized into four main types: experimental, longitudinal, cross-sectional, and case study (de Vaus, 2001). Each type has its unique focus and methodology. The Experimental design, for instance, examines interventions and control; the Longitudinal design studies various units over a period of time; the cross-sectional design analyzes existing differences between different independent variables; and the case study, which is the preference of this study, involves an in-depth examination of a single or group of cases. .

3.3.1 Case Study Method/Strategy

The case study design, as indicated earlier, focuses on an in-depth contextual analysis of a case or series of cases or individuals (Creswell, 2003, p.15). The design, according to Yin (2003), is the most preferred when dealing with issues that border on “when” and “how” questions and where the behaviour of the object of study is not subject to manipulation and contextual condition coverage is required for a better understanding of a phenomenon. Creswell lucidly identifies it as a qualitative design in which the researcher explores in depth a program, event, activity, process, or one or more individuals” (Creswell, 2014, p.241). Similarly, Yin categorises the case study into

three (3) forms: descriptive, explanatory and exploratory. While the descriptive seeks the detailed description of phenomena in their real-world contexts, the explanatory seeks the causal factors to explain a particular phenomenon, and the exploratory seeks fresh research questions which could subsequently be researched in detail (Yin, 2018, p.7). The explanatory form is adopted for this study, which seeks to examine and understand what influenced the cybersecurity strategy adopted by Ghana for managing her cyberspace and whether it fits the purpose.

It is crucial to note that a case study is not just another research strategy but a comprehensive approach that aims to learn "more about little-known or poorly understood situations" (Leedy & Ormrod, 2001, p.149). Its structure encompasses the problem, the context, the issues, and the lessons learned or to be learned (Creswell, 1998). A major feature of this approach is that the case(s) are bound by time and activity, guiding the researcher towards an extensive data collection process. It leverages multiple data collection procedures such as direct or participant observations, interviews, archival records or documents, physical artefacts, and audio-visual materials over a sustained period (Creswell, 2014, p.241). This feature allows case study researchers to harness the strengths of these diverse methods, leading to a rich dataset that facilitates an in-depth analysis of issues.

Additionally, the approach again allows researchers to spend time on-site to interact with the studied people or institutions. This intervention helps realise the issues' patterns and connections with established theories. Given the various factors that influence States' management of cyberspace, a qualitative case study provides an opportunity for an appropriate framework that adequately interrogates the issue. Edgar and Manz (2017, p. 305) affirmed this understanding by indicating that case studies significantly help assess the performance or expected outcome of a specific cybersecurity event or system.

The choice of Ghana, as the case for the study, is a logical decision based on the country's high internet penetration rate, high technological/digital drive, and a demonstrated commitment to governing the state's cyberspace. Ghana has made significant strides in internet penetration and connectivity and has shown a solid determination to digitalise its systems and services across various sectors. This proactive approach has garnered widespread support and participation from its citizens. The country's readiness to address the challenges in cyberspace has led to establishing and institutionalising regulatory and governance structures. These advancements have positioned Ghana as a pacesetter within the African cyber industry, earning it accolades and recommendations for emulation by other countries (Adu-Amanfoh & Allen, 2023, p.1). The country's energy in adopting cyber technology and its management processes, coupled with its high level of internet penetration, make it an ideal candidate for examining the adequacy and appropriateness of its cybersecurity management strategy.

The choice of a single case study in Ghana is also justified because although Africa comprises countries with varied economic and technological development and social constitutions, they are mainly developing economies with similar cybersecurity ecosystems. A common characteristic is their importation of cyber technology, which becomes a significant factor in its management. Thus, they rely on foreign suppliers for critical information infrastructure and data management technologies. This practice limits their sovereign control over the electronic information they produce, rendering it vulnerable (Allen & van der Waag-Cowling, 2021). Although the study does not aim to generalise the findings here, the results on Ghana could be a reflection, to a large extent, of the situation on the continent. It is imperative to clarify that the justifications for a case study strategy were oblivious to the challenges of single case studies, such as the inter-related issues of methodological rigour, researcher's subjectivity, and external validity, as Willis (2014, p.4)

suggested. However, in light of the above justifications, and given that the study is qualitatively designed with the overarching objective of gaining deeper insights rather than grounds for generalisation, the choice of only Ghana as the case for the study remains logical.

3.3.2 The Study Population

A study population is "the entire mass of observations, which is the parent group from which a sample is to be formed" (Singh, 2006, p.82). It shares distinctive features and characteristics that apply to an explanation and describe "all the items under consideration in any field of inquiry." These characteristics then form the base for selecting the sample for a study (Harrison, 2001, p.19; Kothari, 2004, p.14).

The Research Population for this study involves policymakers, implementers and influencers, service providers and end users of cyber technology within the Ghanaian and African cyber ecosystem. The policymakers and implementers section comprises senior officials from the Communication and National Security Ministries, the Attorney General's Department, the Ghana National Cybersecurity Authority and the National Communications Authority. The implementers include the security and defence services, i.e. the Cyber Security Bureau of the Ghana Police Service, the Ghana Armed Forces cyber defence sector, the telecommunication networks, and banking and financial institutions (banks). On the other hand, the cybersecurity policy influencers involve Civil Society Organisations, the Commissions of African Union and ECOWAS, cybersecurity professionals and associations, and cybersecurity service providers. The final section of the population involves organisations and individual end users of cyber products offered by financial institutions, telecommunication networks and other service providers.

The composition of the population was guided by the fact that each of these categories of persons is involved in the chain of cybersecurity policy engineering (policymaking and implementation) and retains rich experiences and knowledge that could contribute to an in-depth understanding of cyber policy life cycle. As regulatory policymakers, the Ministries of Communication and National Security, National Communications and the Cyber Security Authorities offer insights into the processes and principles that influenced the design of the state's cybersecurity threats management strategy. The policy influencers, including CSOs, cyber-security professionals and experts' associations, and international and multinational organisations, such as AU and ECOWAS, are also equipped with information relevant to a deeper understanding of the African and the Ghanaian state's cyber security management strategy.

The cyber policy implementers, comprising state and non-state agencies such as telecommunication network providers and financial and banking institutions, contribute significantly to the functioning and management of the country's cybersecurity ecosystem. These implementation agents' activities allow them to understand the state's cyber security strategy's strengths, challenges, and weaknesses. Their views, therefore, contribute to a better understanding of the adequacy of Ghana's cybersecurity management strategy.

Finally, cyber end users are also a key component of the study population. Their involvement stems from their being beneficiaries and victims of cyber technology and its threats and being directly impacted by the state's management interventions. Therefore, businesses' and individuals' experiences using cyberspace platforms constitute invaluable information for assessing the adequacy or otherwise of employed management strategies.

3.3.3 Sampling Technique

A sampling technique is the method(s) adopted to select a study's sample. Researchers have designed and employed various techniques in this regard. Sampling techniques are grouped broadly under probability and non-probability methods. The probability method is where all respondents have a fair chance of getting selected, rendering the odds measurable. Examples of techniques associated with this method are Simple Random Sampling (SRS), Stratified Sampling (SS), Cluster Sampling (CS), Systematic Sampling (SS), and Multistage Sampling. The non-probability method, on the other hand, involves the discretional imposition of the researcher based on a designed or pre-conceived index. The researcher determines the respondents, and the odds are not measurable. These techniques include Convenience, Haphazard, Purposive, Snowballing, and Heterogeneous samplings.

The purposive and snowballing sampling techniques were triangulated as the sampling methods in this study. The decision for these methods is because the purposive technique permits a researcher to determine what needs to be known and the people capable of providing such information. The decision on whom to include is based on potential participants' considered knowledge and experiences (Bernard, 2002; Lewis & Sheppard, 2006). Therefore, the technique is appropriate for studying issues with some technical character, such as cybersecurity, where in-depth knowledge and experience in space operation and management becomes handy. Respondents' knowledge of the issue enables them to provide relevant data for the study.

This technique was supplemented by snowballing, which picks traces of respondents from individuals interviewed on the subject. The technique thus involves referrals by a respondent to an equally capable person to respond to the study's questions. It comes in handy in studies where the appropriate persons to be interviewed are not readily known either because of the danger or the

peculiarity of the subject matter. In the case of this study, this technique became relevant because of the emerging nature of the cyber-security field, which makes the experts and service providers little visible in the country. Again, because the activities of hackers are sometimes criminal and it is a virtual activity done in seclusion, they could easily not be identified without the help of people within the space. Thus, leads by individuals within these groups became the feasible approach to help reach some of the respondents for the needed information to aid a comprehensive assessment.

It is important to note that this study is not aiming for generalizable findings but rather a deep understanding of the adequacy and appropriateness of Ghana's cybersecurity strategies. In this context, the selection of the purposive sampling and snowballing techniques was not only appropriate but also crucial. They helped generate the necessary data to address the study's objectives rigorously and empirically.

3.3.4 Sampled Population

The impracticality of studying an entire population creates the need for a portion of the research population to be selected to represent the whole (Singh, 2006). The extraction of a sample deemed to possess all the essential characteristics of the entire population is, thus, scientifically well-acknowledged. A research sample, therefore, constitutes a subset of the study population of a research project. Effective conduct of this selection renders the research process economical without compromising the validity and reliability of its findings (Singh, 2006, p.82). The technicalities involved in this process necessitate the identification of observable elements such as the type of universe, sampling unit, sampling size, parameters of interest, and budget for the study (Kothari, 2004).

From the understanding of the research sample above, the composition of the study's sample included officials from the cybersecurity departments and sections of the Ministries of Communications and National Security, security and cybersecurity experts from the Ghana-Indian Kofi Annan Centre of Excellence in ICT (AITI-KACE), senior officials from the National Cybersecurity Authority, the National Communication's Authority and members of the Cybersecurity Experts Association, Ghana. Others are senior officials from the Cyber Bureau of the Police CID of Ghana Police Service, the Economic and Organised Crime Office (EOCO), the Cyber Department of two telecommunication network providers (MTN and Vodafone), and the Cyber Desk of the Civil Society Organisations E-Crime Bureau and the Media Foundation West Africa (MFWA). Officials of the cyber desk at AU and ECOWAS Commissions, cyber officials of the Ghana Commercial Bank, Omni Bank, and GTBank, and individuals and businesses who use cyberspace for business transactions and social communication also form part of the sample.

3.3.5 Sample Size

A study's sample size is a critical consideration in research methodology that attracts researchers and their audience attention. Understandably, readers play a crucial role in this discourse as they seek the assurance that they are not gulping knowledge that does not reflect reality. While the audience would prefer a large population to guarantee representativeness, time and funding often constrain researchers from religiously satisfying that. The scientific resolve has been for researchers to strike a justifiably sound balance in sample size. However, the major challenge associated with this approach is the decision on the thresholds of what is considered "enough" for a large population. Responding to this concern, May (2011) and De Vaus (2002, p.80) intimated that a large population does not necessarily require large samples. They argue that the more significant factors in this case are the needed degree of accuracy and the population's variation

level. In other words, a researcher's ability to provide comprehensively convincing explanations for his choice of size constitutes the logical means of dealing with the sample composing challenge in scientific research (May 2011).

It is imperative to note that, unlike quantitative studies, where numerous models for sample size determination exist, qualitative studies' sample determination rides on logical reasoning on a case-by-case basis. The liberality of this phenomenon influenced De Vaus' (2002) admonishment for qualitative researchers to concern themselves more with constituting samples that generate accurate rather than skewed findings (p. 80). Such composition, he intimates, must also ensure a fair representation of the various interests of the population. Creswell (2013) went further to indicate definiteness in qualitative sample composition by suggesting that any well-framed qualitative research should have a maximum of 11 appropriately sampled sizes. To him, this number is enough to provide the quantity and information depth required for an informed analysis. Creswell's attempt, though, provides some certainty; his justification for the figure appears sweeping and could not apply in all situations. For instance, while such a number might suffice in a mix-method research where qualitative data are required to validate or beef up the quantitative component and a qualitative study that has a relatively small population, it surely will be inappropriate for a purely qualitative study with a large population and bordering on an emerging issue with varied perspectives. On their part, Fridlund and Hildingh (2000) also argued that qualitative studies commonly consider data from between 1 and 30 informants. This figure, according to Krippendorff (2004) and Patton (2002), should, however, not be considered as iron-fixed as the informational need to sufficiently and confidently respond to the research questions constitutes the overarching justification (Krippendorff, 2004; Patton, 2002). In the case of this purely qualitative PhD thesis that discusses the complex issue of cybersecurity with a broad

stakeholder base, the researcher assumed that the sample size of 40 would be sufficient to produce the required data for an in-depth examination.

The study's sample size was 40 individuals. This total included eight (8) policymakers, fourteen (14) policy influencers and pressure groups, eight (8) policy implementers, and ten (10) end users. The policymakers were represented by two (2) senior officials each from the National Cyber Security Authority, cyber departments of the Ministries of National Security and Communications, and the National Communications Authority.

The fourteen (14) respondents constituting the policy influencers also involved five (5) officials from the cyber-inclined CSOs Media Foundation for West Africa and the African Centre for Security Studies (ACSS), cyber service providers E-Crime Bureau and Slamm Technologies Ltd., Four (4) others from the Cyber Security Experts Association of Ghana (CSEAG), three (3) cybersecurity expert academics, and one official each from the AU and ECOWAS Commission desks completed this group.

The composition of the eight (8) policy implementers also comprised two (2) officials from the telecommunication networks (MTN and Vodafone), two (2) senior officials from the Cybercrime Unit of the Criminal Investigation Department of the Ghana Police Service, one each from Economic and Organised Crime Office (EOCO), Ghana Commercial Bank, Omni, Bank and GTBank.

The final group consisted of three (3) hackers and eight (8) users of cyber or e-banking products, digital transaction platforms, and the Internet. The group of 8 was split for separate focus group discussions. The two groups, each consisting of four persons, included students, prison officers, teachers, traders, artisans, and entrepreneurs.

Table 2 Interview Respondents

SAMPLE FIGURES		
NO.	**SAMPLE**	**Number**
1	Ministry of Communication	1
2	Ministry of National Security	2
3	National Communication Authority	2
4	National Cyber Authority	2
5	Cyber Bureau of Police CID	2
6	Economic and Organised Crime Office (EOCO)	1
7	Telecommunication provider(MTN)	1
8	Telecommunication provider(Vodafone)	1
9	CSOs (Media Foundation for West Africa and African Center for Strategic Studies)	2
10	African Union Missions	1
11	Cyber Experts (Ghana-Indian Kofi Annan Centre of Excellence in ICT (GI-KACE)	2
12	Academic Cyber Security Expert (UPSA)	1
13	Banks (Ghana Commercial Bank, GTBank and Omni Bank)	3
14	The Cyber Security Experts Association of Ghana	4
15	Subscribers of banks and Telecommunication networks e-banking products	4
16	Internet end users (businesses and organisations)	4
17	Cyber service Providers (E-Crime Bureau, Slamm Technologies Ltd)	4
18	Hackers	3

3.3.6 Sources of Data

Data for this study were collected from both primary and secondary sources. The primary data comprised Ghana's Cyber Security Act, 2020 (Act 1038), the Ghana Cyber Security Strategy, 2015, and field data from in-depth interviews. The knowledge and experiences of this group, which involved policymakers, policy influencers, pressure groups, policy implementers, and end users, were instrumental in providing the required information for a better appreciation of the issues under consideration. The diversity in the respondents' backgrounds, such as academia, security/cyber experts, and information communication technology, was essential because it offered a blend of academic, cyber expertise, and practical experience perspectives to the discourse.

The primary data was gathered through interview guides with semi-structured open-ended questions. The open-ended questions helped incorporate new perspectives the researcher had yet to consider. Although the questions were generally open-ended, a few close-ended ones were also featured in the guide to help keep the interviewee within the study's scope. The researcher designed the interview guide with the guidance of the supervisory committee, and its face and content validity was measured through pilot testing. The pilot testing identified weaknesses for redress before the large-scale roll-out of the interviews.

The secondary data for the study, on the other hand, were sourced from journal articles, books, and institutional and media reports on cyber security in Ghana and Africa. These documents were accessed from internet websites, journal articles, online data portals (Taylor&Francis, jstor, sciencedirect, etc.), and the University of Ghana and LECIAD libraries.

3.3.7 Data Collection Technique

The study adopted the in-depth interview data collection technique, the most frequently preferred technique in qualitative research endeavours, which involves a verbal interaction between the researcher and respondent, leading to the generation of raw data (Kothari, 2004, p.97; Harrison, 2001, p.90). The appropriateness of this technique for the conduct of a purely qualitative study of this kind stems from its ability to help present opportunities to both the researcher and respondent to interrogate or explain in depth the various aspects of an issue (Kothari, 2004). Though the approach looks expensive and often rigorous, especially when the sample size is large, its opportunity for clarification and specificity renders it worthwhile. These advantages of in-depth interviews constitute the justifications for its preference as the appropriate technique adopted for collecting the required data to respond to the questions posed by this research.

3.3.8 Data Collection Instrument

Following the data collection techniques indicated above, the study used open-ended interview guides with semi-structured questions as instruments for data collection. These instruments were preferred due to their flexibility, non-capping of respondents' contributions, and capability to elicit meaningful responses from respondents (Patton, 1990). The semi-structured questions also helped capture the interviewees' perceptions, emotions, and expectations, which aided in exploring the emerging perspectives during the study. The designed open-ended interview guides with flexible semi-structured questions were tested for validity in a pilot exercise before being deployed for large-scale administration.

3.3.9 Data Gathering Procedures

The researcher followed meticulous data-gathering procedures. The researcher began this process by seeking ethical clearance from the University of Ghana's Ethical Committee. The researcher

made this request by submitting the application and providing all the necessary documents, including a research proposal, ethical consent forms, budget progress timelines, etc., as stipulated in the University of Ghana ethical clearance acquisition form. An introductory letter was subsequently taken by the researcher from LECIAD and sent to the various institutions and individuals earmarked for the interview to inform them of the study and to book appointments after the ethical clearance had been granted by the University of Ghana's Ethical Clearance Committee. The researcher duly observed all protocols at the University of Ghana and the respondents' institutions in a manner that conforms to standard scientific research practice. The researcher ensured that suitable places, with minimal to no obstructions, were organised for the interview sessions.

The interviewer recorded the interviews with an LG v20 voice recorder and transcribed them into text. The transcribed data were subsequently coded into various themes. The coding was done in two different sets. The first was descriptive coding, which allowed for the development of themes from the transcribed data. That was followed by pattern coding, which established a broader appreciation of the interviewees' motives for action(s), as indicated in the data.

3.3.10 Method of Data Analysis

Several analytical methods, such as phenomenology, hermeneutics, grounded theory, ethnography, phenomenography, and content analyses, exist for adoption in qualitative data research analysis (Bengtsson, 2016, p.10). The study relied on the content analysis method.

Content Analysis in research is "a technique for making replicable and valid inferences from texts, or other meaningful matter, to the contexts of their use" (Krippendorff, 2004, p.18). This method seeks to link results to the contexts or environment in which they were produced and, as such,

involves more than just a counting process. From this perspective, Downe-Wamboldt (1992, p.314) defines the method as that which "provides a systematic and objective means to make valid inferences from verbal, visual, or written data to describe and quantify specific phenomena." Mayring (2000, p.2) summed its objective as seeking an "empirical methodically controlled analysis of text within their context of communication, following content analytical rules and step-by-step models…" Like many other qualitative data analysis methods, qualitative Content Analysis employs coding to identify the main categories of issues within a dataset.

It is vital to note that data analysis, both in positivist and naturalist research methods, seeks the organisation and meaning of collected data to draw realistic conclusions (Polit & Beck, 2006). Content Analysis' unique suitability for the above purpose, in both qualitative and quantitative methodology, through inductive and deductive means, increases its relevance for social research conduct (Krippendorff, 2004; Neuendorf, 2017; Berg, 2001; Burnard, 1991; Catanzaro, 1988; Downe-Wamboldt, 1992; Bengtsson, 2016, p.10). The method also has a low risk of confusion on matters of philosophical underpinnings and discussions, and researchers only need to adhere to a qualitative perspective and ensure that rigour and credibility processes that would present the results as trustworthy are followed throughout the process (Bengtsson, 2016, p.11).

In Qualitative Content Analysis (QCA), data are presented in words and themes, which makes it possible to draw interpretations from the data as the results. There are two analytical methods for the conduct of analysis in QCA: manifest and latent. Researchers' choice of the type to deploy is influenced by how deep they want the analysis to reflect the informants' statement on the subject (Burnard, 1991; Polit & Beck, 2006). In essence, the Manifest Analysis sets the researcher to describe what the interviewee says, stay very close to the text, use the interviewee's words, and describe the visible things in the text. The latent, on the other hand, extends to an interpretive level

in which the researcher seeks to find the underlying meaning of the text: "what the text is talking about". To this end, he uses his understanding of the perspective and words to communicate to the audience (Berg, 2001; Catanzaro, 1988; Downe-Wamboldt, 1992). The study adopted the latent approach to move from a shallow probing of the gathered data to establishing the underlying meaning and perspective of the interviewees. This decision was to help create an opportunity for a deeper appreciation of the respondents' perspectives and effectively link them to the research objectives.

Apart from the simplistic but effective and detailed understanding of data that this analytical method offers, its ability to help control the intrusion of the researcher's thoughts into the subject matter (Anderson, 2007, p.1) further justifies its preference in this study. These features of the analytical method helped to conduct an exhaustive discussion of the salient arguments and thoughts on the subjective issues of cyber security and state policy.

In terms of processing, the data gathered through interviews were critically scrutinised. The field data obtained through in-depth interviews were coded and analysed using the manual analytical method, and the final outputs were presented in texts and direct quotes. The internal mechanisms of the approach, as incorporated in the protocols, controlled the possibility of the researcher's bias interference, thereby leaving the views of the respondents unsullied and original.

The research questions covered all the various themes of the topic to ensure that the interviews reflected the main objectives of the study and aid analysis. The respondents' responses were coded after the interviews and discussed based on major themes that had emerged from the data. The major themes include Africa's cybersecurity landscape, contemporary cyber-security threats in Ghana, Ghana's cyber-security strategy, and the effectiveness of cybersecurity strategies.

3.4 RELIABILITY AND VALIDITY

Reliability and validity tests have been debatable research elements in qualitative research (Golafshani, 2003). The major concern borders on whether or not reliability and validity are of any essence in qualitative research and could be measured similarly to quantitative research. One of the popular opinions is that reliability is only applicable in quantitative research, where researchers seek explanations other than understanding (Stenbacka, 2001). However, in disagreeing with this view, Patton (2002) insists that reliability and validity concerns all researchers, irrespective of their approach to a study. Lincoln and Guba (1985, p.290) explain that this is because the principle forms the basis upon which a researcher justifies why the audience should pay attention to their study's findings. Thus, one would live in absurdity if he were to expect audience acceptance of a study's findings without satisfying any reliability and validity test. To realise this, steps including structuring questionnaires to focus on the key areas and conducting the study within the logical theoretical frame, themes, and encompassing questions were ensured. For the appropriate adoption of steps toward preventing biases in the analysis and conclusion, the researcher ensured the realisation of the two important features of reliability and validity.

3.5 ETHICAL ISSUES

Ethical considerations are essential in any research and, more importantly, in PhD studies because of their consequential impact on institutions and individuals' data, reputation, and value. Other effects posed by conclusions and findings of studies on the health, identity, and psychological well-being of a studied people or population have been proved and hence created the need for researchers to observe ethical principles in any research endeavour for their prevention and minimization.

Being aware of the above and the significance the University of Ghana and the research community adduced to it, the researcher paid much attention to it during the research process. In this light, the researcher observed the University's procedure for obtaining ethical clearance, which included an application and submission of a research proposal, the justifications of its possible benefits and possible adverse implications on the participants in the study, the various interventions to mitigate these adverse implications on both the researcher and participant and the communication of these intended processes and interventions to the appropriate committees for approval. Upon satisfying itself of these provisions, the committee issued a certificate to that effect.

During the fieldwork that involved interviews with cybersecurity experts, policymakers, and cyberspace users, the researcher ensured that the interviewees were informed of their rights of voluntary participation and anonymity regarding their responses read out to them before the interview sessions. Given the sensitivity of the issues discussed, the respondents were assured that their responses were solely for academic purposes and would likely come to the attention of only the researcher, his supervisory committee, and his examiners upon request. If any other third party requested any portion of their response, the interviewees were informed that they would be the final determiners on such through written authorization.

Finally, where the process leading to the data gathering occasioned a psychological effect or physical injury on any respondent or a person assisting in the interview process, clear guidelines on seeking counselling or financial support upon hospitalization by the researcher were also clearly indicated.

3.6 LIMITATIONS OF THE RESEARCH

The technical and budding nature of the cybersecurity industry in Ghana resulted in various challenges for the researcher, whose perseverance paid off. The researcher overcame the initial difficulty in finding individuals with the requisite knowledge through an extensive search and the snowballing approach. This effort led to the successful location of experts, industry players, and space users, enabling the gathering of the required information.

Again, given the sensitive nature of the information required for the study and its potential implication on organisations' reputations, public and private institutions were reluctant to give out some data. This reluctance, unfortunately, slowed the data collection process, as the researcher had to go through rigorous bureaucratic processes in signing undertakings before accessing some information. Also, having envisaged this from the onset, the researcher designed an interview guide that allowed for probing and elicited the required information to sufficiently appreciate the issues being interrogated. The follow-up questioning approach helped the researcher deal with the respondents' hesitations and limited its effect on the study's final results. So, while these limitations undoubtedly delayed the progress of the work, its substance was not compromised because the researcher got all the required data provided in the long round. To this end, this limitation did not portend any material effect on the study's outcome.

Another limitation of the study involved the nature of cyberspace. This involved the continual evolving nature of cyber technology and industry, which sees new threats or threat techniques manifest and threatens the long-term validity of findings and recommendations. The researcher acknowledged the relativeness of the study's findings and recommendations as a solution. The researcher also advocated for continual assessment of threats and strategies, recognising the need to identify trends and corresponding management strategies.

Finally, the limited time frame for a PhD thesis at the University of Ghana and the financial burdens constrained the researcher to limit the scope of the study to a single case despite being aware of some of the challenges of the option. For instance, extending the scope to involve more than one country's cybersecurity strategies would have provided a broader and deeper understanding of the dynamics in the African cybersecurity ecosystem. But this notwithstanding, the scientific considerations that underlined the selection of Ghana as the case study and the justifiable selection of respondents and interview techniques helped generate a deeper understanding of Ghana's cybersecurity management practice, which offered some sense of the general African cyber ecosystem.

3.7 CONCLUSION

The Chapter outlined the methodological framework and methods that underpinned the study. The Chapter established that the primary data used for analysis was gathered mainly through in-depth interviews using well-designed semi-structured interview guides. The respondents were also selected using the purposive and snowballing sampling techniques. In-depth interviews were conducted with 40 persons in their personal and institutional capacities. The responses of these respondents were recorded, transcribed, coded and analysed. The assertions from these interviews were subsequently juxtaposed with the content of Ghana's cybersecurity management strategy and international cybersecurity management best practices in the analysis. The researcher then employed content and context analysis techniques to analyse the data.

CHAPTER FOUR

THE CYBER SECURITY THREATS AND RESPONSE STRATEGIES IN AFRICA

4.0 INTRODUCTION

Several cyber-security threats have challenged the African continent over the past decades. This phenomenon has influenced the design and adoption of various cyber-security strategies and policy frameworks by regional organisations and individual states on the continent. Therefore, this chapter looks at the continent's cybersecurity threat landscape and the response mechanisms adopted for their management by state and non-state actors at the national and regional levels. The chapter begins by identifying the cybersecurity threats in the region, maps up the response mechanisms, and concludes with a critical assessment of the appropriateness and challenges of the response mechanisms.

4.1 AFRICA CYBERSECURITY THREAT LANDSCAPE

Generally, undertaking accurate statistical predictions on Africa's economic, political, and security indicators becomes challenging due to the lack of reliable data resulting from weak states' governance machinery data collection and analysis capabilities (van Raemdonck, 2021; Arnould & Strazzari, 2017). Therefore, most African states lack reliable data despite the significance of the same for state governance and development planning. In the unlikely situations where some of these data exist, they are in disjointed and scattered patches (Johns, 2021). Cyberspace is not different in this scheme. However, their systems for carrying out activities within the space provide some opportunity for tracking statistics on its usage and attendant threats across the continent (Mitchell, 2022; El Mehdi, 2020). The situation has wielded state and non-state organisations with

the capacity to generate and process data on variables, such as internet usage, penetration, and threats.

Regarding cyber threats, available figures point to soaring rates and devastating effects on the continent. This situation has triggered substantial interest in understanding their causes, the extent of their impact, and possible solutions (Mitchell, 2022 & van Raemdonck, 2021). With the established conclusion on the adverse effects of cybersecurity threats on the continent and its citizens' well-being, the next important focus of the conversation must be addressing the challenge through effective space governance. This governance objective could be addressed first by understanding the nature of the prevailing threats and the general threat landscape. This is what the study advances in this section. It thus examines the African cybersecurity landscape and then dovetails into the continent's response strategies as contained in the existing policy and academic literature, institutional databases and primary data from the interviews.

4.1.1 The Nature of Cyber-Security Threats in Africa

Cyber-security threats have touched every part of the world that has witnessed internet systems usage. These threats, against which states and other organisations seek security, are similar due to the standard operational principle characterising cyber technology. However, differences in the dominant threats in a country and the assets and persons mostly targeted portend some differences in their manifestations across ecosystems (Tagert, 2010, p. 23). These characteristics of state cyber ecosystems also influence the approaches and management strategies adopted for cyber governance.

Evidence from the field interviews lends much credence to the above proposition. The respondents generally noted that, while it was not always clear what cyber security precisely entails in both policy and academic worlds, the concept broadly concerns the protection of data, data systems or

infrastructure, and users of the space against threats and threat actors' activities (Field Interview, 2023). These threats or threat actors have states' critical infrastructure, individuals, and private organisations as their targets and have varied motives and strategies underpinning their actions. Such features, argued by Mitchell (2022) and Tagert (2010), give cybersecurity elements some distinctions across ecosystems.

According to the respondents, the African cyber ecosystem plays host to a wide range of public, private, individual, and organisational target cyber threats. However, these threats have manifested in varying degrees across states and periods. A respondent from the E-Crime Bureau, highlighting this, intimates

> *"In essence, one cannot say that African cybersecurity is distinct from other continents. This is because cyber technology is one, and Africa imports what is manufactured out there. So, the threats that cyber users in the West face are the same as those faced by users in Africa. The only difference is that some threats fester in some places more than others, so what is considered the dominant threat in different countries could differ." (Field Interview, 2023)*

According to the data, the African cyber ecosystem features all three cybersecurity threat portfolios: disruption, destruction, and exploitation. Specifically, the respondents highlighted five cyber threats dominating the continent's cyber ecosystem. These include organised criminal networks, cyber espionage, mis/disinformation, critical infrastructure sabotage, and innovation related to armed conflict conduct (Field Interview, 2023).

4.1.1.1 Organised Criminal Networks or Cyber Crime

Cybercrime is one of the significant cyber-security threats identified by the respondents as bedevilling the African cybersecurity ecosystem. For instance, the African Centre for Strategic Studies (ACSS) respondent explained that this threat often manifests through networked groups of linked criminals who deploy various means to outwit administrative and computer systems to steal critical information. The common techniques and tools usually deployed by threat actors to advance these threat activities include malware, information stealers, and remote administration

tools (Renals, 2020). The respondent from the African Union Expert Group also contended that the intention of the threat actors engaged in these acts is financial gain from selling the stolen information or siphoning monies electronically from a compromised system (Field Interview, 2023).

The above narrative consents with the 2021 Interpol Report findings that online scams, digital extortion, business email compromise, ransomware, and Botnets' had become prevalent on the continent (Interpol, 2021, pp. 11-22). Per the report, data breaches and phishing that aid threat actors in their criminal activities manifested as the most dominant cyber threats on the continent. It also affirmed Allen's (2021) finding that malicious cyber activities with financial gains as their motives had become the African business community's major concern. In Allen's estimation, the continent lost about 3.5 billion dollars to this threat in the year ending 2017, continually ranked as one of the topmost threats to the continent's business communities' activities.

Among the myriad cyber threats, the Business Email Compromise (BEC) scam is a big issue in Africa. The Silver Terrier group, a well-known perpetrator of BEC scams, operates across Nigeria's major cities with hundreds of members. Renals (2020) and Allen (2021) reported that this group has created over 81,000 pieces of malware and conducted over 2.1 million attacks within and outside Africa. Their activities have resulted in staggering financial losses for individuals and organisations within and outside Africa, amounting to billions of dollars.

4.1.1.2 Critical Infrastructure Sabotage

The critical infrastructure sabotage threat in Africa is one of the continent's concerning cyber threats. It involves deliberately targeting systems to cause substantial and widespread interruption or impairment of accessibility and functioning. A typical manifestation of this threat is the

Distribution Denial of Service (Field Interview, 2023). The respondents in this interview highlighted the potential consequences of this threat, stating that it poses a great danger to the African continent. They further clarified that while Africa may not be heavily reliant on the internet, it also lacks the capacity to promptly restore disrupted services of institutions' computing systems (Field Interview, 2023).

The critical infrastructure sabotage threat in Africa manifested with the August 2012 reported hacking of the personnel records databases of Nigeria's Secret Service by Boko Haram. The hacker indicated the breach was executed in the name of Boko Haram and as a response to Nigeria's handling of interactions with the group (Baken, 2013). Similarly, Johannesburg had its website and billing systems shut down in October 2019 after hackers took over the authority's system and demanded a ransom of 4 Bitcoins worth $30,000 (Henderson & Mackenzie, 2019). Another damaging manifestation of this cyber threat on the continent occurred in Liberia when an overzealous hacker employed by a telecommunications company in 2016 sabotaged the network of a rival company, resulting in the disconnection of half of the country from banking transactions services (Chellel, 2019).

4.1.1.3 Dis/Misinformation

Disinformation or misinformation is another cybersecurity threat that resonated among the respondents as dominant within the African cyber ecosystem. This threat, conducted mainly through social media, involves circulating unverified or malicious information, pictures, videos, and news articles to consciously or unconsciously misinform the audience. According to the MFWA respondent, the originators of such content prey on people's gullibility in information sharing (Field Interview, 2023). The acceptance of social media as an authentic source of

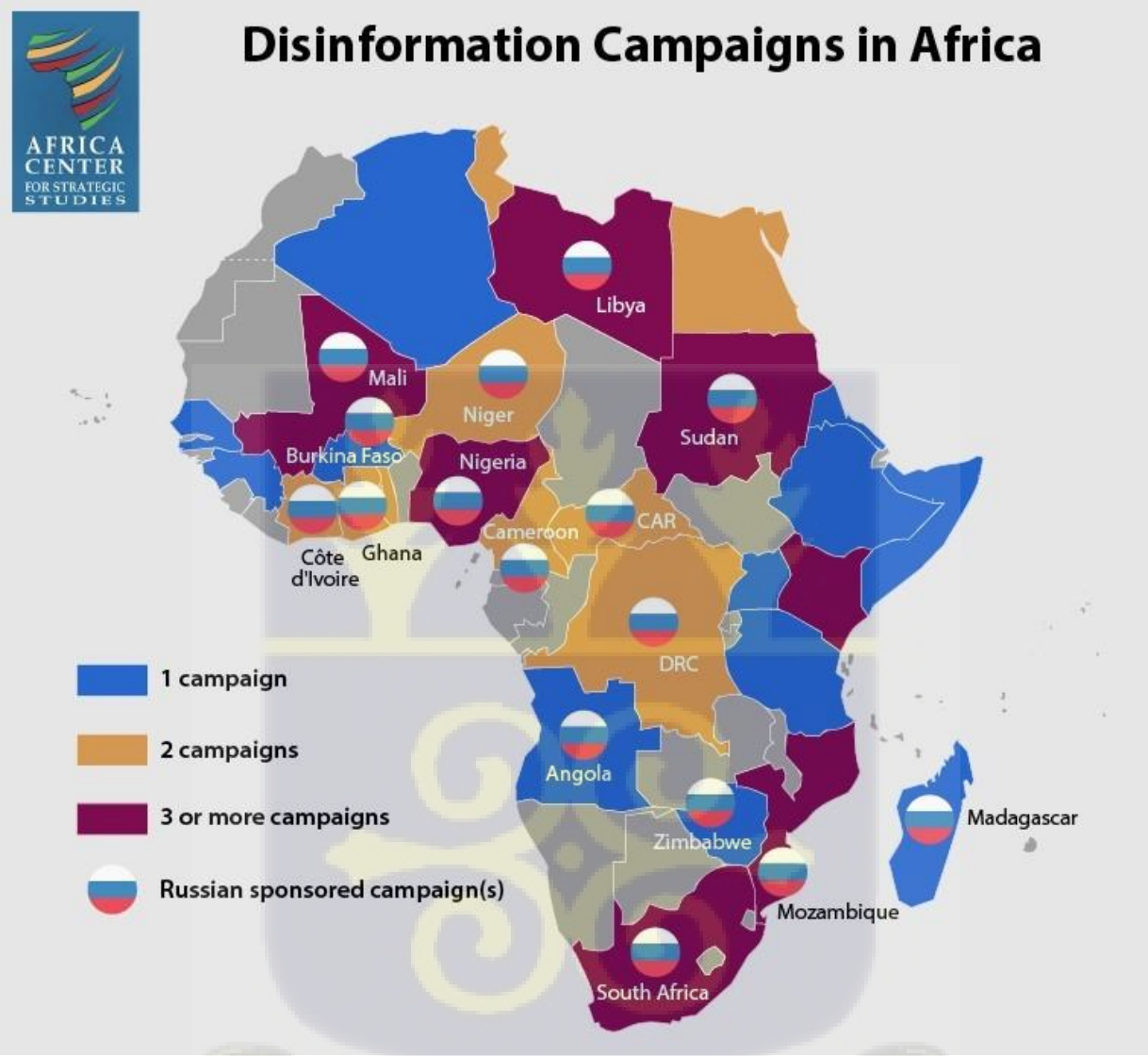
information in Africa, which has led most users to accept its contents and even share them without questioning its authenticity, has contributed immensely to this phenomenon.

The respondents affirmed that the mis/disinformation phenomenon has festered on the continent and affected persons and institutions in all facets of life. The energetic use of the internet by Africa's young social media-hungry demographic population has also seen a significant push in digital campaigning on the continent. State governments, opposition parties, corporate business entities and private individuals have variously deployed the mechanism to advance their interests and policies. In proceeding with such agenda, old, fake or distorted videos or speeches are circulated by creators for business or political capital. In the lead-up to Uganda's 2021 elections, for instance, the state's Ministry of Information, Communication Technology and National Guidance, General Muhhoozi Kainerugaba's spokesperson and some media firms' public relations officials embarked on a widespread disinformation attempt to defame Muhhoozi's opponents and disrupt the sharing of accurate elections' information, particularly on social media (ACSS, 2021 p.4). Similar observations have been made in South Africa with anonymous Twitter handles promoting xenophobic sentiments, and in Ethiopia's Tigra region, where Diaspora supporters of Tigrayan have intentionally attempted to shape the narrative of the Tigray conflict (Knight & le Roux, 2023; ACSS, 2022).

As noted earlier, foreign elements have also been at the forefront of promoting misinformation and disinformation in Africa. A pro-Russian network propagating anti-democratic, EU and UN narratives using African voices has also been cited as a key source of mis/dis information in Africa. The manifestation of this agenda in Mali, Central African Republic, South Africa and Mozambique has seen the recruitment and instruction of the recruits to spread content directly authored by

Russian state media outlets such as RT and Sputnik on social media (Knight & le Roux, 2023; ACSS, 2022).

Figure 2 Disinformation Campaigns in Africa



Source: Africa Centre for Strategic Studies (2022)

Unfortunately, states and cyber technology platforms' difficulty in preventing the use of conflict-fueling content such as fake reports, radicalization, terrorists resource mobilization and recruitment, and violent incitements on their virtual platforms, has continuously threatened the already precarious peace of the continent.

4.1.1.4 Emerging Cyber Technologies Reshaping African Conflicts and Battlefields

The respondents again identified that cyber technologies aid the conduct of conflicts and pose a significant threat to national security in Africa. Being a fragile continent with several conflict hotspots, any situation that contributes to intelligence gathering and the conduct of offensive and defensive actions is of significant consideration. Information Communication Technology (ICT) and related technologies have increasingly become pivotal in military defence and peace operations. It has substantially influenced military operations and battlefield tactics, including air combat and ground warfare.

The respondents indicated that the consequences of this development have been felt within the African conflict space as cyber technology has been deployed in recent years by both state and non-state groups in battle combat. They clarified that although computer-programmed bombings are yet to become widespread on the continent, the deployment of automated systems, such as drones, by both states and rebel groups is becoming a common feature in Africa's battle operations (Field Interview, 2023). The AU respondent added that one disturbing manifestation is that some of these cyber-assisted intelligence gathering and offensive conduct tools by separatist and rebel groups are more sophisticated than those of the target states.

Battles grounds on the continent are witnessing a gradual shift from entirely brute tactics to unmanned or artificial intelligence-programmed information gathering and attacks (Field Interview, 2023).

The above narrative by the respondents consents with Allen's (2021) postulation that even though cyber-related technologies such as drones, artificial intelligence, and 5G network expansion are yet to see much integration into African battlefield operations, they have made significant inroads already. The deployment of drones as a substitute or aid to traditional aircraft in intelligence gathering and for the precision of attack or defence has seen wide display on the continent. The autonomous nature, loitering ability, and low cost of drones have enhanced this development. The drone data on Africa affirms this by indicating that 14 African Countries and militant groups had 2021 acquired and used drones for intelligence gathering and combat purposes (Gettinger, 2020; Allen, 2021). The successful execution of several of Nigeria's deadly extremist groups, Boko Haram attacks, is attributed to its deployment of such sophisticated information gathering and offensive attack drones (Dionne, 2019; Allen, 2021).

4.1.1.5 Cyber Espionage

Another prevalent and alarming threat in African cyberspace, as identified by the respondents, is cyber espionage. This form of cyber threat, characterised by malicious intentions and attacks by hackers on private businesses or government entities, has become frequent globally. The respondent from the National Security Ministry emphasised that Africa's vulnerability to this threat is exacerbated by the widespread use of outdated, pirated, or substandard computer or cyber-security systems by governments, organisations, and individuals (Field Interview, 2023). This practice compromises data systems and grants hackers access to critical institutions and state data, which can be monitored, posing a significant risk.

It is important to note that much of the reporting on cyber espionage in Africa has been centred on accusations, often lacking concrete incrimination or admission of offence. A notable example is the case of employees from the Chinese telecommunications giant Huawei, who are reported to have been spying on the opponents of China-allied governments in Uganda and Zambia (Allen 2021, Parkinson, Bariyo, and Chin 2019). Similarly, Africa has been at the centre of an alleged Chinese hacking of the African Union headquarters, which it built (Abegunrin & Manyeruke, 2020; Satter, 2020). The lack of definiteness in these claims, though unfortunate, is unsurprising because the detection of cyber espionage activities is by the targeted states, which African states are limited in doing because of their low cyber maturity capabilities. Thus, the phenomenon underscores African states' need for more investments to enhance their cyber maturity capabilities and reduce their susceptibility through outdated and pirated computer or cybersecurity systems.

The findings of this chapter, which place organised cybercrimes, espionage, critical infrastructure sabotage, and combat innovation as dominant African cyber threats, are revealing and align with the concluding assertions of the 2022 ACCS report, which identified organised crime, misinformation and critical infrastructure sabotage as disturbing cybersecurity threats in Africa (ACSS, 2022). They also echo an earlier report by the ITU, which highlighted the surge in public cyber infrastructure sabotaging, digital fraud, illicit financial flows, and national security breaches in espionage and intelligence theft by militant groups as the key concerns in the continent's cybersecurity ecosystem (ITU, 2021). These findings underscore the fact that cyber threats in Africa originate from both domestic and external sources, necessitating comprehensive strategies that consider not only external structures and norms but also internal ones. This understanding is in line with the neo-institutionalist theory's norms and structures interplay in governance and

structuration paradigm's argument of an existing mutual relationship between human actions and social structures in knowledge construction (Wendt & Shapiro, 1997, p.176).

4.2 THE AFRICAN CYBER SECURITY THREATS RESPONSE

A popular view from the field interviews is that cyber security involves attaining three main objectives: ensuring the confidentiality, integrity, and availability of data and computer systems (Field Interview, 2023). With its susceptibility to cyber threats, as enumerated earlier, and its resolve to harness the benefits of cyber technology, the African continent has advanced several efforts towards addressing the emerging challenges associated with its deployment. Also, given the prioritisation of cyber diplomacy against states relying exclusively on their cyber defence capabilities in contemporary international politics, various initiatives, including bilateral and multilateral collaboration and cooperation, have been advanced in Africa. This section looks at the response mechanisms that Africa has advanced to address the threats to its cyber ecosystem.

To begin with, the spread of ICTs, Internet penetration in African states, and concerns over the security of the space, which transcends national borders, brought to focus the need for harmonisation in responding to the threats. Consequently, efforts by regional organisations, sub-regional organisations, states, and private sector non-governmental organisations to provide frameworks and collaborative efforts to address cyber threats on the continent have manifested. The following paragraphs detail these response mechanisms.

4.2.1 The AU Convention on Cyber Security and Personal Data Protection

The African Union has functioned as the most prominent regional intergovernmental organisation uniting the 55 African countries. Its core aim is to "accelerate the African continent's political and socio-economic integration" and to coordinate and harmonise the policies between the existing

and future Regional Economic Communities (Constitutive Act, article 3). Alongside this mandate, the AU established a Cybersecurity Convention, which was adopted during the 23rd Ordinary Session of the AU Assembly in Malabo on the 27th of June 2014 by the AU Heads of State and Government (Malabo Convention, 2014).

The Convention thus emerged as a significant continental effort towards responding to cybersecurity threats. According to the respondents, the Convention consolidated all the initial regulatory mechanisms on the continent (Field Interview, 2023). The cyber-related response schemes, which metamorphosed into the Convention, began with activating the AU's institutional bodies responsible for superintending over telecommunications and cyber-security issues. These institutions included the Specialized Technical Committee on Communication and Information Communications Technology (STC-CICT), the AU Commission Information Society Division (ISD), and the AU Cyber-Security Expert Group (AUCSEG). In addition to the AU Commission's Peace and Security oversight responsibility, this activation constituted a response towards addressing the emerging threats from the deployment of ICT (Sulieman, 2020; African Union, 2019; African Union, 2012:Article 16:1(a). The AU instituted a regulatory legal Cybersecurity instrument with a continental scope to achieve a coordinated response. This endeavour resulted in the drafting and ratifying the 2014 Convention on Cybersecurity and Personal Data Protection (AU Commission, 2008; African Union, 2014; Article 36), hereafter referred to as the Malabo Convention or Convention.

The Convention recognises cybercrime as a significant threat to the security of computer networks and the development of Africa's information society (Malabo Convention, 2014 preamble). Member states are mandated under the Convention to establish policy, legal, and institutional governance mechanisms to promote cybersecurity. Such provisions include developing national

cybersecurity frameworks and incorporating national cybersecurity policies, strategies, and governance structures (Malabo Convention, 2014 Articles 24&25). Additionally, the Convention mandates member states to enact laws that criminalise offences such as attacks against computer systems and data, as well as online child pornography (Malabo Convention, 2014; Article 29). It equally demands the establishment of procedural measures to control cybercrime and legal provisions for international cooperation on cybersecurity.

The framers of the Convention sought to encourage the exchange of information on cyber threats and vulnerability assessment among member states through the establishment of institutions such as Computer Emergency Response Teams (CERTS) or Computer Security Incident Response Teams (CSIRTS) (Malabo Convention, 2014; Article 28). It also implores member states to utilise existing international cooperation channels at the state, organisational, public and private levels to promote cybersecurity and tackle cyber threats. The Convention takes a comprehensive cybersecurity governance approach beyond the Council of Europe Convention Cybercrime criminalisation model to institute procedural mechanisms for law enforcement and international cooperation.

With the primary focus on harmonising cybersecurity legislation, regulations, and governance strategies across the continent, the Convention advocated for enhanced collaboration among states and the private sector (van Raemonck, 2021). Member states and the various RECs identified with this provision

On the part of the RECs, various efforts are made to initiate and promote good cybersecurity governance practices through collaboration (Tamarkin, 2015). In this respect, the Economic Community of West African States (ECOWAS), Economic Community of Central African States (ECCAS), and Southern African Development Community (SADC) all sought collaborative

assistance from the ITU through the 2018 AU Reference Framework for the Harmonization of Telecommunication and ICT Policies and Regulation (AU Commission, 2008, p.75). The ECOWAS Commission also partnered with the European Union (EU) in the development of its cybercrime policy and strategy: the Organised Crime: West African Response on Cybersecurity and Fight Against Cybercrime (OCWAR-C) and Regional Cybersecurity and Cybercrime Strategy, in 2019 (Ajijola & Allen, 2022, ECOWAS Development Partners' Coordination Cell, 2022).

Other coordinated efforts in cybersecurity management at the regional level inspired by the collaboration agenda espoused in the Malabo convention include the AU's Mechanism for Police Cooperation (AFRIPOL) and the African Computer Emergency Response Team (AfricanCERT). The respondents affirmed these provisions in their observations of the various levels in which African states have cooperated to respond to their cybersecurity threats. An understanding that emerged, however, was that while such commitments sound encouraging, their effectiveness and the guarantee that they will yield the expected objectives depended on the effectiveness of the individual member states' cybersecurity management systems (Field Interview, 2023). This observation, which concurs with Mitchelle's (2022) and Ajijola and Allen's (2022) bottom-up approach, suggests that while the Convention's objective of promoting cooperation and collaboration among African states in addressing cyber threats remains commendable, it is crucial to ensure that member states response strategies are appropriate and adequately respond to their threats. These cumulative strengths would form the basis of a robust regional response.

Indeed, the Convention's framers appeared aware of this reality in cybersecurity management and attempted to draw on it in dealing with the cross-border element of cybercrimes (Malabo Convention, 2014, Article 28). Here, the Convention demanded express provisions from states on

cooperation in cross-border cybercrime prosecution. Nevertheless, it is worth clarifying that despite such attempts, the provisions do not appear robust enough for the task. Thus, while Article 28 of the Convention provides for international cooperation on cyber security and mandates AU member states to use existing cooperation channels, it does not promote comprehensive mutual assistance. The principle of double criminality that borders on states' assistance on cross-border cybersecurity issues has no established mechanisms for extradition and mutual assistance requests if the parties involved have no existing extradition treaty or mutual assistance on dual criminality arrangement. Article 28(1) of the Convention provides that.

> *"State parties shall ensure that the legislative measures and/or regulations adopted to fight against cybercrime will strengthen the possibility of regional harmonisation of these measures and respect the principle of double criminal liability."*

The application of the double criminality principle is further highlighted in Article 28(2) of the Convention, where it states that:

> *"State parties that do not have agreements on mutual assistance in cybercrime shall undertake to encourage the signing of agreements on mutual legal assistance in conformity with the principle of double criminal liability while promoting the exchange of information as well as the efficient sharing of data between the organisations of State Parties on a bilateral and multilateral basis".*

The Convention, thus, establishes a blanket requirement for member states' application of the double criminality principle.

As Orji (2015) had asserted earlier, the challenge of explicit provisions on cooperation, such as extradition, has created the need to reflect on the Convention provisions in light of the current cybersecurity and legal challenges. This is required to clear the impediments against the Convention's receiving the needed support to be acknowledged as a relevant continental treaty. Notwithstanding these observations, the Convention is the building block for constructing a resilient African cybersecurity response mechanism.

4.2.2 African Sub-Regional Cybersecurity Governance Response

At the sub-regional level, the respondents also indicated some significant efforts by the Regional Economic Communities ECOWAS, COMESA, EAC and SADC towards promoting cyber safety on the continent. The various sub-regional economic communities have designed regulatory instruments for cybersecurity promotion within their jurisdictions.

4.2.2.1 The ECOWAS Directive on Fighting Cybercrime

81

ECOWAS was established by the Treaty of Lagos on May 28, 1975, to foster regional co-operation and integration in West Africa. One of its core objectives is to harmonise and coordinate national policies in different areas such as communication, technology, and legal to promote economic stability and good relations among member states (ECOWAS, 1993 Article 3(2)). In August 2011, the ECOWAS Council of Ministers adopted Directive C/DIR.1/08/11 on Fighting Cybercrime in response to the rising waves of cybercrimes within the region. Email scams, commonly called the *"West African letter scam or 419"*, had gained notoriety in many member states, prompting the adoption of a comprehensive management response framework (Orji, 2019, p. 41).

The ECOWAS Cybercrime Directive, among its various provisions, mandated member states to criminalise cybercrimes and establish a framework for international cybersecurity cooperation. To ensure the effective implementation of the Directive, Article 35 required member states to adopt the necessary legislative, regulatory, and administrative measures by January 2014 (ECOWAS, 2011).

The Cybercrime Directive provisions show several similarities with the principles of the Budapest Convention, even though some fall short of the Convention's principles. It is imperative to note that after over ten years of the Cybercrime Directive's adoption, not all Member States have

established cybercrime laws and other regulatory and administrative measures per their obligations under the Directive (Orji, 2019, p. 52). This development indicates the non-realisation of the Directive's objectives within the stated timeframe. Notwithstanding this unfortunate state of affairs, there is no doubt that the ECOWAS region has shown awareness of tackling cybercrime and promoting cybersecurity within the territory with the adoption of the Directive. Therefore, despite the implementation drawbacks, the adoption of the Directive shows the collective interest of ECOWAS Member States to tackle cybercrime and promote the development of a secure information society (Orji, 2016, p. 214), with the harmonisation of cybercrime control regimes within the region. This spirit of co-operation has influenced ECOWAS' engagement with other international organisations, such as ITU, to support member states in cybersecurity capacity building and expert advice.

4.2.2.2 The COMESA Model Cybercrime Bill

The Common Market for Eastern and Southern Africa (COMESA) aims to enhance regional integration by reducing barriers to cross-border trade among its Member States (COMESA, 1994; Articles 3&6). To achieve this objective, COMESA developed a Model Cybercrime Bill in 2011 to provide a uniform framework for promulgating cybersecurity laws in member states.

The Bill outlines what constitutes offences against computer systems and data. These include unauthorized access, data interference, data interception and misuse of digital devices, digital forgery and fraud, and cyber extortion (COMESA, 2011). It's crucial to note that the Bill lacks binding obligations on Member States to criminalize cyber offences. As of November 2023, some Member States, such as Eritrea, Libya, Comoros, Swaziland, Democratic Republic of Congo, and South Sudan, had no cybercrime laws despite being enjoined by the Bill to have such to ensure the safety and security of their digital environments.

The Bill essentially adopts the language and model of legal instruments such as the Council of Europe Convention on Cybercrime and the ITU Toolkit for Cybercrime Legislation. It also establishes an elaborate guide for developing a general framework to facilitate international cooperation, extradition, and mutual assistance. It provides for establishing 24/7 national points of contact (COMESA, 2011, Articles 56-59). Despite its framework on international cooperation, the Bill only serves as a guide or model for developing national cyber security laws in Member States. Thus, the Bill does not establish any international cooperation obligations on Member States, nor can it be used as a legal instrument for cooperation among Member States. Also, unlike the ECOWAS, the COMESA has no existing legal frameworks to facilitate mutual assistance and extradition among Members. As such, COMESA Member States that have developed national laws from the Bill must enter into separate bilateral arrangements with other Member States to ensure any form of international cooperation or mutual assistance (Orji, 2019).

4.2.2.3 The EAC Model ICT Policy Framework

The East African Community (EAC) is a seven-member state regional intergovernmental organisation established in 1999. The members are Burundi, the Democratic Republic of the Congo, Kenya, Rwanda, South Sudan, Uganda, and Tanzania. The core objective of the EAC is to create a prosperous, competitive, secure, stable East Africa. This objective has influenced the organisation in the provision of general guidance on issues of security and development with ICT at the centre.

Recognising the rapid evolution of information technology and the increasing threat of cybercrimes, the EAC, like other subregional bodies in Africa, has taken the initiative to provide a model framework for member states' legislation. This initiative is crucial as the existing laws on

criminal offences in the EAC member states are outdated and ill-equipped to address these emerging cyber technology challenges.

The objective was to achieve a harmonised operation of its member states' activities in cyberspace in 2015. The Policy framework outlined ways of promoting cyber security, data protection, and e-transaction. It also mandates member states to enact laws on cyber-security, data protection, and other emerging issues (East African Communications Organisation 2017, p.16). States' research capacity promotion, prompt response to legal and regulatory principles, and public consultation towards legal and regulatory framework development have also been highlighted in the framework (EACO 2017, p.16).

4.2.2.4 The SADC Model Law on Computer Crime and Cybercrime

The Southern Africa Development Community (SADC) was founded in 1980 to promote economic integration and cooperation among its member states. Following the increasing use of ICT and the growing rates of ICT crime at both the regional and country levels, the Community resolved to offer a regional response, the result of which is the SADC Model Law (Bande, 2018, p.9; SADC, 2012).

The SADC model laws involved three key elements: Data Protection, Electronic Transactions and Electronic Commerce, and Computer Crime and Cybercrime. The Model Law on Cybercrime, launched in 2012, seeks to guide and facilitate the harmonisation of domestic laws on cybercrime. It was part of the adopted guides for the Harmonisation of the ICT Policies in Sub-Saharan Africa (HIPSSA) project. The Model Law on Computer Crime and Cybercrime aims to offer guidance on how cybercrime and cybersecurity can be regulated by the SADC member states (MISA & KAS, 2021). Unlike the ECOWAS Directive, the SADC Model law does not impose binding

obligations on Member states to enact cybercrime laws. It mainly seeks to influence the incorporation of its provisions into the content of member states cybercrime legislation, as has been the case of Botswana, Tanzania, Mozambique and Malawi, who enacted their cybercrime laws after the adoption of the Model Law (MISA & KAS, 2021, p. 20).

The SADC Model Law identifies the offences member states are to incorporate into their national laws, including illegal access, interception, data interference, espionage, forgery, fraud, pornography, xenophobic material and disclosure of details of an investigation. While the domestication of these provisions by member-states has received criticism for being quite intrusive, the need for cooperation and harmonisation of cybercrime legislation by the regional body is telling. Thus, such provisions are helping to lessen the difficulty of partnering to prosecute crimes across states.

Another contribution of the Community is the support in building members' states' cyber capabilities through workshops. For instance, the Community organised a capacity-building workshop in Ebene, Mauritius, in 2018 for state officials managing cyberspace, and participants from 14 out of the 15 member states attended this workshop (SADC, 2018). The impact was well-informed state officials to contribute to policy-making in their countries.

4.2.3 States level Cybersecurity Response Mechanisms

The respondents also identified some state-level cybersecurity response management mechanisms in Africa. They noted various steps undertaken by states to curtail the threats associated with cyberspace operations. These responses have involved the designing and implementation of regulatory instruments suggested by the various international, regional and sub-regional cybersecurity conventions, treaties, and protocols (Field Interview, 2023).

Though many AU member states have yet to ratify the regional Malabo Convention, most now have national cybersecurity governance frameworks. The November 2016 AU Commission and Symantec corporation's cybersecurity report puts the initial figure of states with laws and provisions on cybercrime and electronic evidence in their national laws at eleven (11) (African Union & Symantec Corporation, 2016). A few of these also submitted bills on cybersecurity legislation to their parliaments for approval, leading to a significant rise in the numbers. For instance, the 2021 United Nations Conference on Trade and Development report recorded thirty-nine (39) countries with dedicated cybercrime laws (UNCTAD, 2021).

It is worth noting, however, that this energy on the enactment of cybersecurity laws and policy adoption has yet to be replicated in the area of technical and organisational capacities development and user education (Orji, 2021 pp.79-80). The significance of these observations lies in the fact that technical capabilities are a significant component of state cybersecurity management. Thus, cybersecurity threats are addressed not only by laws. The availability of the right technology, infrastructure, and citizen awareness are also vital components of cybersecurity management. This observation agrees with the neo-institutionalist assumption that the combined effect of both institutional structures presents a better understanding of state governance or management affairs.

Table 3 Cybercrime legislation in Africa

Have Cybercrime Legislation	Have Draft Legislation	Have No Cybercrime Legislation	No Data
Algeria	Eswatini	Central African Republic	Tunisia
Angola	Congo DR	Chad	
Benin		Comoros	
Botswana		Democratic Republic of Congo	

Burkina Faso		Equatorial Guinea	
Burundi		Eritrea	
Cabo Verde		Gambia	
Cameroon		Guinea Bissau	
Cote d'Ivoire		Liberia	
Djibouti		Libya	
Egypt		Namibia	
Ethiopia		Somalia	
Gambia			
Ghana			
Guinea			
Kenya			
Lesotho			
Madagascar			
Malawi			
Mali			
Mauritania			
Mauritius			
Morocco			
Mozambique			
Niger			
Nigeria			
Rwanda			
Sao Tome & Principe			
Senegal			
Seychelles			
Sierra Leone			
South Africa			
South Sudan			
Sudan			
Tanzania			
Togo			
Uganda			
Zambia			
Zimbabwe			

Source: UNCTAD, (2021)

4.2.4 International Multilateral Cooperation

Another significant effort towards managing cybersecurity threats in Africa is international multilateral cooperation. Most of the country-level cybersecurity legislation recognises the

invaluable role of international co-operation, which constitutes the fifth pillar identified by the ITU's Global Cybersecurity Agenda (Acayo, 2017, Slide. 5), in combating cybersecurity threats. The national cybersecurity strategies of Côte d'Ivoire, Senegal, and Rwanda all acknowledge and provide for the operationalisation of multilateral co-operation in their cybersecurity management responses. For the realisation of these objectives, the Cybersecurity Strategy framework of Côte d'Ivoire provides that the state should continue to engage in international and regional initiatives, ratify and observe the provisions of international cybercrime conventions, such as the Budapest and Malabo conventions (Côte d'Ivoire, 2021, p.24).

Many African countries have since partnered with international institutions such as the European Union and ITU to improve cybersecurity resilience, build capacity and promote responsible state behaviour in cyberspace. The ECOWAS, for instance, sought the assistance of the European Union in drafting and implementing its Regional Cybersecurity and Cybercrime Strategy (Ajijola & Allen, 2022, ECOWAS Development Partners Coordination Cell, 2022). Strengthening cybersecurity co-operation is one crucial element of the 2030 Joint Vision set by the sixth European Union-African Union Summit (European Council & Council of the European Union, 202). Through the AU-EU partnership programs such as the Policy and Regulation Initiative for Digital Africa (PRIDA), the Global Action on Cybercrime (GLACY), the Global Action on Cybercrime Extended (GLACY+) and the EU-Africa track 1.5, the European Union Council has partnered with the African Union Commission and African states to build states policy capacity needed for enhanced cybersecurity (EU Cyber Direct, 2021, European Council & Council of the European Union, 2022). Ghana has participated in all these partnership projects, which has undoubtedly contributed to the country's appreciable ranking in the recent global cybersecurity index ratings (Global Cybersecurity Index, 2020, p.25).

4.2.5 Private Sector and Non-State Actors Partnerships

The private sector, individuals, and CSOs have partnered with African states to promote cybersecurity. These partnerships have proved pivotal in cybersecurity management in Africa. Many Kenyans, for instance, have benefited from the tech firm Serianu's establishment of a Cyber Immersion Centre in Nairobi. The Centre serves as a testing or experimental space for firms' cybersecurity capabilities and for offering cybersecurity professionals training (Consultancy Africa, 2018; Republic of Kenya, 2022).

The respondents identified the contribution of CSOs to cyber policymaking, awareness raising and capacity building on related issues, such as cybercrime, child online protection, and online safety, in many African states. An example in this respect is the activities of the Africa Cybersecurity and Digital Rights Organisation and the African Civil Society on Information Society (ACSIS). The two organisations have been involved in cyber education, advocacy, and capacity building on the continent (Teleanu & Kurbalija, 2022). For instance, the ACSIS has undertaken several partnership projects such as the establishment of a Cybersecurity Operation Centre for the Uganda Bankers Association, provision for the deployment of the Capacity Maturity Modeling (CMM) in Rwanda and cybercrime awareness, skills for South African law enforcement agencies in cybercrime investigations and judicial cybercrime training and training material to improve cybercrime prosecution in Nigeria. The organisation also partnered in training for incidents response Teams in South Africa, developing the National Cyber Security Strategy and Action Plan for Sao Tome and Principe and the digital forensic and operationalisation of national public critical infrastructure in Kenya to create trust in the government's e-services, enhancing cyber diplomacy capabilities and coordination in ECOWAS region (Cyber Capacity Knowledge Portal, 2024)

Foreign multilateral corporations have partnered with African states and institutions to design cyber strategies, embark on cyber awareness campaigns and capacity building, and develop ethical standards. For instance, Microsoft partnered with Paradigm Initiative Nigeria (PIN) to educate Nigerians on cybercrimes and create economic opportunities. The country's Economic and Financial Crimes Commission (EFCC) again announced in October 2009 that its success in shutting down over 800 websites used for cybercrimes and arresting 18 cybercrime gangs was through the help of a "smart technology" provided by Microsoft (Kshetri, 2019 p.80).

As illustrated above, African states' efforts towards addressing cybersecurity challenges have involved various strategies. These efforts have ranged from national and international multilateral cooperation to partnerships with state and non-state institutions, CSOs, and the private sector. The focus of these initiatives have been infrastructural improvement, laws, cybersecurity awareness creation, education, and capacity building. This approach, of infrastructural improvement and norms and norms creation, is in sync with the neo-institutionalist management orientation. It also consents with the structuration paradigm's orientation that both structures and agency are pivotal in understanding the actions and inactions of states. Through these provisions, African states have created space for the deployment of both formal and informal cyber management strategies, which has, in turn, afforded them a broad and holistic framework to deal with the cybersecurity concerns that confront them.

4.3 CHALLENGES TO CYBER-SECURITY GOVERNANCE IN AFRICA

It is apparent from the above that African states have made significant efforts and progress in cybersecurity promotion over the past years. Substantial investments in legislation and infrastructural development have resulted in impressive gains in some member states' cybersecurity performance. Recent ITU reports, including the 2020 Global Security Index,

consequently indicated a significant appreciation in the performance of several African states. Tanzania, Mauritius, and Ghana achieved remarkable performance scores, inspiring others to improve (Global Cybersecurity Index, 2020, p.25).

Amid these efforts by African states and regional organisations, the respondents indicated the many challenges confronting them. At the heart of these concerns is the approach adopted in managing their cybersecurity ecosystems (Field Interview, 2023). Given that the continent is not an originator of cyber technology and its management demands some financial commitments, support-seeking becomes inevitable. But while all the respondents appreciated this reality, a section suggested that while seeking this support from cyber-advanced countries in their drive to promote cyber safety, these states must sail with caution. They believe that even though the African cyber ecosystem shares similarities with general cyberspace, some thin dynamics, rising from the domestic situations, need to be observed (Field Interview, 2023). Commenting on this, the respondent from Slamm Technologies noted that

> *"...threats came with cyber technologies and manifest similarly across all states. So, states, especially cyber-infant ones, do not need to reinvent the wheels of their management than adopt what has worked elsewhere. However, in such adoption, domestic factors in the state should be factored in the implementation process." (Field Interview, 2023)*

This viewpoint concurs with Ajijola and Allen's (2022) caution to African states against the wholesale adoption of cybersecurity strategies recommended or designed by international cybersecurity institutions such as the ITU and cyber-advanced countries. It also suggests that in states' response to cyber threats, some basic questions, as proposed by Ajijola and Allen (2022), need to be answered by the state involved based on its peculiarities. The questions include why the cyber strategy is necessary, what to do and when, who is responsible, and how to fund and implement it. The responses to these questions are to be informed by the peculiarities of the state under consideration.

While the above has remained a general challenge for African states in their cybersecurity promotion efforts, the respondents also identified some specifics as noteworthy. These issues span internal, external, social, and technical spheres. The subsequent paragraphs detail these views.

4.3.1.1 Low Levels of Cyber Literacy

One major challenge identified by most respondents as contributing to the flourishing of cyber threats in Africa and stagnating the management of the same is the region's lag in cyber literacy. A respondent from the Ghana National Security Ministry noted that the African continent has unfortunately lagged in many of the world's revolutions, and the story does not differ from the cyber revolution (Field Interview, 2023). He lamented thus

> *"…. a major hindrance to improving security in this space is the lack of cyber literacy among the population. So you realise that every country is digitalizing to enhance service delivery in both the private and public sectors. But we all would admit that our population, even the educated ones, is not well-informed about it. So, end users of these services are exploited by cyber criminals because they lack knowledge of how they work. (Field Interview, 2023)*

On his part, as one of the 20 who commented on this, the respondent from ACSS retorted that Africa's cyber literacy has not seen much progress despite its intense digitalization drive (Field Interview, 2023). The field data, thus, indicate that despite African states' resolve to embrace digitalization, their awareness of proper cyber hygiene practices remains limited. This low literacy and awareness phenomenon on the continent has impacted the management of the space, limited the utilization of the opportunities provided therein and exposed citizens to cybercriminals' exploitation. Bada, Von Solms, and Agrafiotis's (2018) assertion that many African states are still stuck at the start-up stage of cyber maturity and lack cyber awareness-raising programs has not only been confirmed but shows no progress six years on. Therefore, the need for the continent's member states, stakeholders, and development partners to work towards improving citizens' cybersecurity awareness has become apparent.

4.3.1.2 Policy Coordination and Implementation Challenges

Most respondents also identified policy coordination and implementation challenges in Africa's cybersecurity management efforts. They argued that cybercrimes thrive under collaborated efforts among threat actors. Thus, for any organisation or state's response to be effective, they must follow a similar approach. Expounding on this, a respondent from the Cyber Security Experts Association, Ghana (CSEAG) retorted

> *"…cyber threats do not have any borders. A crime can be staged in one country from another. So if there is no collaboration amongst those states, information sharing, which is critical for tackling such issues becomes difficult to achieve" (Field Interview, 2023).*

The significance of such approaches has been acknowledged in many African states' country-level cybersecurity strategies and the Malabo Convention. Despite these acknowledgements, the respondents lamented that African states were faced with the challenge of meaningfully implementing them. A section of the respondents identified the differences in domestic laws and programs on cybersecurity, the varying levels of cyber liberty across countries and language barriers that contributed to the challenges of implementing the collaborative provisions (Field Interview, 2023).

Regarding language, the respondents explained that collaboration in cyberspace requires swift correspondence, which makes language a critical factor in the scheme. Unfortunately, many African states have adopted foreign languages such as French, English, Portuguese, and Arabic for official communications. Moreover, neighbouring states have adopted different languages among these. The situation creates difficulty in communication, especially if officials in one country are to liaise with their counterparts in other states to deal with an issue collaboratively. For instance, officials from English-speaking Ghana, which shares borders with French-speaking Togo, Côte d'Ivoire, and Burkina Faso, would have a torrid time sharing information, especially if the officials at both ends are not multilingual. Communication among officials attempting to collaborate and

swiftly deal with an issue would become challenging. Commenting on this, a respondent from the National Signal's Bureau explained that:

> *"... It is so unfortunate that we have adopted a foreign language as our official language. So, if, for instance, there is a cybersecurity issue in Ivory Coast, the gentleman or lady in charge of cybersecurity in Ghana has to communicate to the person in French or English and vice versa. If one of them is good in the other one's language, we thank God. If not, translators would have to come in, and this slows down the processes" (Field Interview, 2023).*

A respondent from CSEAG corroborated this assertion by averring that the rate at which things move in the cyber world does not give room for a third-person interpretation when responding to issues. African states' use of different languages significantly limits the continent's cybersecurity collaboration enterprise.

Regarding domestic politics, legislation and programs on cyber security, the respondents argued that African states have different governance systems and legal orientations. This situation informs or affects the nature of laws and programs designed to promote cybersecurity (Field Interview, 2023). The challenge arises, therefore, when countries with conflicting cyber regimes must collaborate. For instance, while countries such as Ghana, Nigeria, and South Africa have a liberal orientation towards the operation of cyberspace and have provisions of their cybersecurity strategies recognising and promoting human rights, others such as Eritrea, Kenya, Ethiopia, Guinea, Mauritania, Senegal, Sudan and Tanzania are much restrictive in their cyber governance (Yusuf, 2023). These varied perspectives have been cited by Hunter and Tilly (2017) as a source of concern in Kenya, Ethiopia, and Eritrea, challenging collaborative efforts.

Again, most African states have signed on to several cybersecurity projects to draw support and help enhance their cybersecurity. This multiple membership has, unfortunately, given rise to the issue of duplication of projects, rendering coordination difficult. Van Raemdonck's (2021) and Gautier and Ridde's (2017 p.2) observations that the littering of several uncoordinated projects in Africa has created unparalleled conflicting interests and has been counterproductive has found

itself manifesting in cyberspace. This challenge, which has also been highlighted in the 2024 World Economic Forum Cyber Security Outlook Report on executives' (businesses and states) challenge for effective cyberspace regulation (World Economic Forum, 2024 p32), has indeed manifested as a significant challenge for African states in their cybersecurity management collaborative efforts.

Figure 3 Challenges in Cybersecurity Management

Source: *World Economic Forum (2024)*

4.3.1.3 Non-Ownership of Web Hosting Sites

Another factor the respondents identified as hampering the cybersecurity management efforts is the status of African states as non-owners of their data hosting sites. Explaining the effects of this on cybersecurity management, the respondents reasoned that confidentiality remains a critical ingredient in cybersecurity. At any moment when someone other than those who owe allegiance to a nation gets the opportunity to see, manipulate or access a state's critical data, the confidentiality of such data is threatened and breached. Notwithstanding such dangers, that is,

unfortunately, the situation of many African countries that do not own the sites that manage their critical data.

The respondents again argued that the location of most hosting sites on which crimes are perpetrated against Africans is mostly outside of Africa. This thrusts the continent's cybersecurity management into the hands of other sovereign states (Field Interview, 2023). Expressing this concern, a respondent from the AU Commission explained that

> *"…because the platforms used in Africa are owned by non-African states, it takes the most needed partners and collaborators outside the continent. For example, when crimes perpetrated through platforms such as WhatsApp or Facebook against African states' citizens occur, little can be done by the said state without the tacit support of the state hosting the platform's servers. Thus, even if the attacker were in Nigeria and used WhatsApp to dupe somebody in Ghana, the Nigerian authorities would not be able to help. Those who can help are the US authorities because that is where the WhatsApp platform is hosted" (Field Interview, 2023).*

Respondents from EOCO and Slamm Technology Solutions shared this position, arguing strongly that non-hosting web platforms are deficient in dealing with cyber threats within the African cyber ecosystem (Field Interview, 2023). These conclusions by the respondents concur with Calandro, Chavula, and Phokeer's (2019, p.5) geolocation analysis on website hosting in Africa. The authors established that over 85% of the websites on the continent are remotely hosted outside its jurisdiction, with the majority in the USA and Europe. According to their findings, the United States of America hosts over 58% of the sites. South Africa is mentioned as the only African country with appreciable inroads into website hosting but controls only a paltry 14% (Calandro, Chavula, & Phokeer, 2019, p.6). This unfortunate reality has called for urgent collaborative and concerted efforts among African states in cybercrime investigation, hosting platform establishments, and cloud infrastructure use.

4.3.1.4 Technology Importation

The importation of cyber equipment and technology, as identified by the respondents, is a significant issue that leaves African states vulnerable in their cybersecurity management strategies.

According to the respondents, most African states are mere end users of cyber technology, lacking the capacity to build their own cybersecurity technology or equipment (Field Interview, 2023). As explained by the respondent from the ACSS, this situation has left the states exposed to numerous cyber threats. The respondent from National Security further elaborated on this, stating:

> *"…. if Ghana is supposed to protect itself against the US government, for instance, and our equipment is produced by the US [or US company], its efforts could go back to ground zero. You are not really in charge. Because they developed it, they know how it works and can bug them (Field Interview, 2023).*

While admitting that meticulous scanning could help remove hidden bugs in procured cyber systems from another state or company, a respondent from CSEAG asserted that the difficulty in fully understanding IT systems in record time worsens the situation (Field Interview, 2023). Lapses could also lead to irreparable damage before possible solutions are found. The apprehension in getting decisions, approaches, and strategies right has been the primary concern, prompting African states' adoption of existing cybersecurity strategies of other states. This is manifestly depicted in African countries' lack of original positions in cyber policies and diplomacy and always aligning with Russia and China or the West (America and Europe). It also explains Ifeanyi-Ajufo's (n.d) doubts about whether the sprouting data centres on the African continent would guarantee any data security. Indeed, most of the cybersecurity policies of African states are adopted from foreign countries. Ifeanyi-Ajufo (n.d) affirms this in her observation: "… I recall in 2018 one example when I picked up a data protection bill of one African country, which turned out to be a verbatim copy of the UK Data Protection Act" (Ifeanyi-Ajufo, nd; p.3)

This import dependence poses severe consequences for the continent's cyber-security management, a view shared by Adomako et al. (2018). Therefore, it is not surprising that the respondent from ACSS echoed the familiar African renaissance chorus of "African Solutions for African Problems". In light of this, the respondents advocated for urgent collaborative efforts

among African and developing states to pool resources and design technologies that effectively respond to their threats and allow for greater control (Field Interview, 2023).

4.3.1.5 Resource Scarce (financial, infrastructural deficit)

The respondents again contended that financial constraints, which translate into infrastructural deficits, constitute one of the continent's principal challenges in cybersecurity management. Explicating the phenomenon, the respondents lamented Africa's lagging in the various revolutions, including the cyber technology revolution. Being non-originators of cyber technology, many African states who opt to use it resort to importation. The required resources for infrastructural development, coupled with the already dire financial constraints of most African states, have resulted in cyber infrastructural deficits (Field Interview, 2023). Most respondents thus identified that the lack of such infrastructure has negatively affected many African states' cybersecurity management.

The lack of financial aptitude to invest in response mechanisms and capability development among African states is at the core of these infrastructural deficits. The respondent from the E-Crime Bureau professed that

> *"... to learn and better appreciate cybersecurity issues, one must mostly be online. But the question is, how many people even have internet access or faster internet access on the continent? So, there is an infrastructural deficit, which is directly hampering our ability to promote cybersecurity" (Field Interview, 2023).*

He emphasized that most internet users in Africa prefer to save money and compromise their gadgets rather than vice versa. This challenge has contributed to the misery of African states' fight against cybersecurity threats. However, in his admission to this reality, the respondent from ACSS suggested that African states should turn to cost-effective techniques, tools, and software and adopt targeted frameworks that could be smartly and effectively deployed (Field Interview, 2023). This

highlights the potential for growth and improvement in African states' cybersecurity management, inspiring hope in the users.

The respondents' statements echo Target's (2010) conclusion that Africa's developmental challenges and scarce resources have significantly impacted its cybersecurity management. This understanding aligns with Raemdonck's (2021) and the World Economic Forum's (2024) insight report, highlighting financial challenges as a significant hurdle in African states' responses to cybersecurity threats. It further supports Orji's (2016) argument that African policymakers have mostly favoured non-binding model law approaches that tie project execution to resource availability. In light of these challenges, adopting cost-effective and efficient measures, such as targeting prevalent threats and deploying free but effective tools, becomes necessary for African states' cybersecurity management efforts.

4.3.1.6 Cyber skills gap

A cybersecurity skills gap has also been identified as one of the manifest challenges affecting cybersecurity management in African states. The respondents argued that all states require better implementation systems to experience the maximum impact of their management strategies. This necessity bills skilled cyber persons or experts as cybersecurity management lifestring. The respondent lamented that Africa had a massive deficit in trained professionals despite the importance of an expert workforce in cyberspace management and effective combat of cyber threats. While admitting that the cyber skills gap appeared to be a global challenge, the respondent from Vodafone Ghana quickly added that Africa's situation was dire and alarming (Field interview, 2023).

The respondents' assertions align with the findings of ISC2 (2022, p.7) and Adomako, Mohamed, Garba and Saint's (2018, p.1), which underscore the cyber skills deficits and their impact. These

studies reveal a global cyber skills deficit of around 3.4 million. Africa is, however, quoted to be facing a much more severe situation with a certified cyber expert to population ratio of 1:177,000. This disparity is particularly alarming as cybersecurity threats, including the rapid spreading of ransomware in the region (World Economic Forum, 2023). It is unfortunate to see Africa suffer a siege by cyber threats, but lacking the foundational elements necessary for effectively managing the situation.

4.4 Conclusion

In conclusion, this chapter addresses the first research objective: to provide an understanding of Africa's cybersecurity ecosystem. To address the objective, the chapter specifically delves into the cybersecurity landscape. This involves the cybersecurity threats manifesting on the continent and how the states, regional organisations, and developing partners and institutions on the continent have helped manage them.

The chapter reveals the continent's unique disposition regarding dominant threats and peculiar cyber management challenges. Thus, while depicting the nature of the general cyber ecosystem, this disposition has warranted country-level-tailored approaches in cybersecurity management. Therefore, they argue against wholesomely adopting international cybersecurity standards for domestic implementation. The findings reveal that while international frameworks and international best practices or strategies are indispensable in cybersecurity management, they should, at best, serve as guides. African states have hence been admonished to resist relying on cybersecurity strategies inspired by external practices or consultants but do not necessarily conform to or reflect their local realities. African states must, therefore, collaborate to build a safe and robust cyber ecosystem that reflects their systems and capacity.

CHAPTER FIVE

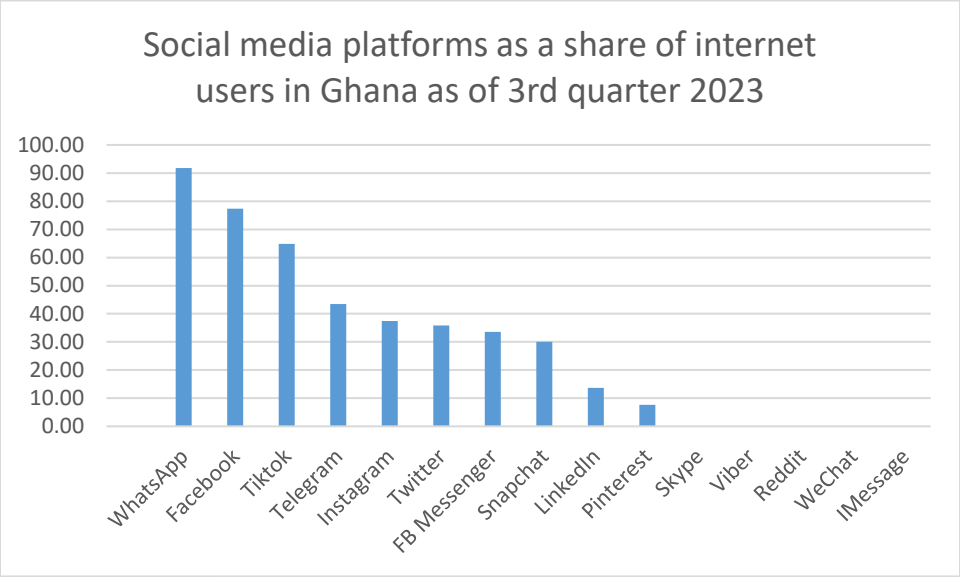
GHANA'S CYBERSECURITY THREAT LANDSCAPE

5.0 Introduction

Ghana's cyberspace landscape has witnessed significant growth over the past decade. The 2018 and 2020 United Nations E-Government Development Index Surveys (UN EGDIS) and other available statistics attest to this tremendous development in the country's cyber ecosystem, particularly in ICT infrastructure, internet speed and accessibility (Alhassan, 2020; UN EGDIS, 2018; 2020). Indexes in E-participation, telecommunication infrastructure, online service, and E-Government Development have all witnessed positive improvements (Kpessa-Whyte & Dzisah, 2022, p. 17). At the heart of these advancements is the widespread use of mobile and smartphones, a development that has significantly bridged the country's digital gap. This has not only opened up new opportunities for businesses and institutions but has also empowered individuals, leading to a surge in digital financial services and promoting financial inclusion (Siaw et al., 2020; Mattern & McKay, 2018). The development has also spurred the Bank of Ghana's policy of building a digital and cashless economy and positioned the country to seamlessly enrol in the Pan-African Payment and Settlement System (PAPSS) (Afreximbank, 2022).

The growth of Ghana's cyber ecosystem has not only been theoretical but has also translated into tangible benefits for businesses and individuals. The rise of digital economic and social services platforms has been significant, with e-commerce outlets like online shopping and e-government service platforms becoming integral to the Ghanaian economy. The internet penetration rate, estimated at 68.2% with a subscription base of 23.05 million (Datareportal, 2023), has also sparked a revolution in social media usage in the country.

Figure 4 Social Media Usage in Ghana



Source: *DataReportal, (2024)*

The growth of Ghana's ICT and cyber ecosystem, while promising, has also brought about a new set of challenges. Despite the opportunities for state and cyber users to leverage cyber technology, this development has also exposed them to the criminal exploits of threat actors. This chapter delves into this dichotomy by examining the prevalent threats in the country's cyber ecosystem, which is the second objective of the study. It specifically analyzes the threats that dominate the Ghanaian cybersecurity ecosystem, their impact, and whether the country's situation differs from the African or global cybersecurity experience.

5.1 THE DOMINANT CYBER SECURITY THREATS IN GHANA

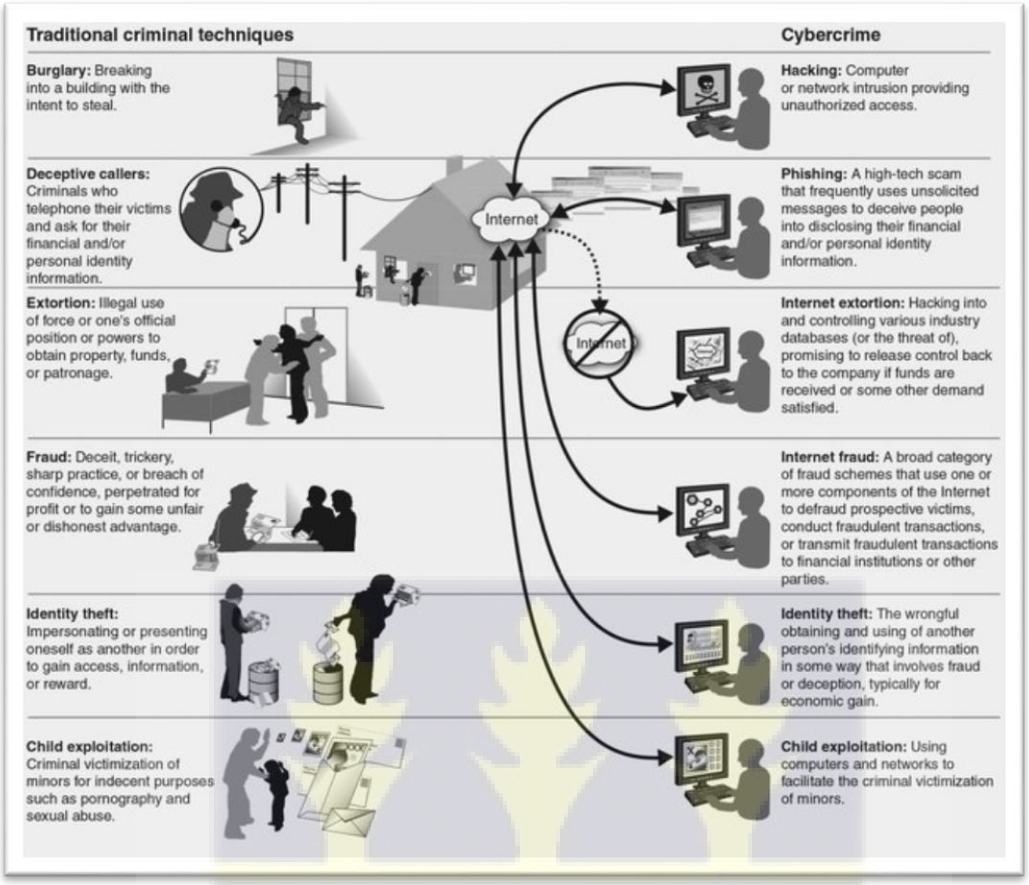
This section discusses Ghana's cybersecurity threats by juxtaposing the respondents' views on the dominant cyber threats in Ghana and the findings in the empirical literature. Such an understanding was to establish the basis for examining the appropriateness of the cyber-security strategies adopted for managing the Ghanaian cyber ecosystem. Upon an in-depth interrogation along this

objective, the respondents identified the Ghanaian cyber ecosystem as sharing threats similar to those of other African states. The Ghanaian space replicates many developing African states' cyber ecosystems with disruptive, destructive, and exploitative threats. Among the many threats identified by the respondents are cyber fraud, insider-related attacks, social engineering (phishing attack or identity theft), denial/distributed denial of service, ransom wares, disinformation, data breaches, and malware.

5.1.1 Cyber Crime/ Fraud

The respondents identified cyber fraud as the most dominant cyber-security threat within the Ghanaian cyber ecosystem. Fraud, explained to involve the "malicious or deceptive means of swindling people of their money or valuables," is an age-long phenomenon that has lurked around for decades. The virtual nature of cyberspace has only come to transform and give it a more sophisticated form (Field Interview, 2023). All the respondents consented to the prevalence of this threat within the Ghanaian cyber ecosystem. Commenting on its widespread, the respondents from CSA placed it atop all other threats based on their institution's Established Point of Contact data since 2019 (Field Interview, 2023).

Figure 5 Cyber Transformation of Crime



Source: Ghana Police service, (2023)

The respondent from the Ghana Armed Forces also indicated the possibility of even a higher prevalence than is reported. He remarked such possible under-reporting was due to the likely reputational damage its knowledge would have on the companies, institutions or individuals involved. He further observed that the widespread adoption of online financial transaction portals has increased the potentials of cyber fraud. He retorted that

> *"…. most of our companies do not talk a lot about it [cyber fraud], but it is our major threat. This situation is so because we have mobile money and other platforms where many transactions are carried out. So, cybercriminals try to take advantage of the innocent and ill-informed persons on the operations of the system to defraud them" (Field Interview, 2023).*

Despite this worrisome development, the respondent expressed scepticism about any solution at sight. The NCA and Slamm Technologies respondents expressed similar sentiments, indicating

further that apart from institutional damage control, the faint confidence of cybercrime victims' in state's institutions to deal with the situation also feeds into non-reporting decisions (Field Interview, 2023). Providing a divergent narrative on the underreporting of cybercrimes, respondents from the banks (GCB and GTBank) and telecommunication networks called for circumspection in outright ascribing the phenomenon to deliberate institutional underreporting. Instead, they argued that victims' lack of confidence in any possible corrective measures and the mostly tiring process they would likely endure was more central to the underreporting phenomenon (Field Interview, 2023). Notwithstanding these varied perspective, the respondents appeared consensual on the widespread nature of the cyber fraud/crime phenomenon, presenting it as a significantly dominant threat within Ghanaian cyberspace.

The above views align with the 2019 Established Point of Contact Data report, identifying cybercrime as Ghana's most prevalent cybersecurity threat. This disturbing but unsurprising revelation is validated by the quantum of money lost by individuals and corporate bodies to the threat over the past years. Its manifestation has witnessed a continual rise without any signs of slowing (Mensah et al., 2023, p. 14). The recent Cyber Security Authority's (CSA) report revealed the state's loss of over GHS49.5 million to the menace between January and June 2023 (Aklama, 2023). Threat actors, such as the cyber gang uncovered in Assin Fosu by EOCO, have been cited as adopting such sophisticated equipment and strategies in their escapades (Mustapha & Boateng, 2024). This development has further fueled the crime in Ghana.

The non-reporting of crimes, resulting from the quest for institutional damage control, lack of trust in investigation and prosecutorial institutions, and cumbersome reporting process, as argued by the respondents' are, thus, revealing. These factors are also in sync with Korsell (2020, p.286), who identified the same as hindering factors in crime reporting. The above narrative reveals that

cyber fraud/crime is much more ingrained in the country and requires urgent attention. Its impact derails citizens' acceptance, and the success of the digital economy drive being championed by Ghana is palpable. It is not surprising, therefore, that a considerable number of the cyber security literature on Ghana, such as Akuako (2022), Baylon and Antwi-Boasiako (2016), Motiwala (2017), Danquah and Longe (2011) and Warner (2011), all focused on assessing the manifestations and management of cyber fraud/crime in the country. Given the effect of this threat and the scope of its victims, an appropriate solution to its manifestation will be a significant leap in Ghana's cyber-safety net.

5.1.2 Insider-Related Threats (IRTs)

Another cybersecurity threat identified by the respondents as manifesting in the Ghanaian cyber ecosystem is Insider-Related Threat (IRT), which constitutes a major attack on system and information integrity. The respondents explained that IRT, which refers to the compromising of data or data systems by an insider, either deliberately for personal gains or accidentally, to grant access to an outsider, has seen a rise within the Ghanaian cyber ecosystem. On identifying this threat as a significant concern in Ghana, twenty-five (25) respondents considered it a primary concern within the country's banking industry. In his narrative, the president of CSEAG indicated that "the reality of IRT as a major threat is glaring and has severally been affirmed by the Bank of Ghana's fraud data, which has consistently recorded its rising spate and effects year-on-year" (Field Interview, 2023). His assertion finds validation by the 2023 Bank of Ghana which indicated a 46% increment of 188 staff-related cases in 2022 within the country's banks and specialized deposit-taking institutions (SDIs). It further indicated spikes in insiders facilitated cyber fraud contributing to losses in excess of about GH¢10.5 million (Sackitey, 2024).

Remarking on why the threat has flourished within the country's cyberspace, the respondent from GTBank stressed that cybercriminals now sit within organisations. He quipped, "…they get themselves employed in the organisations. This is because they know attacking beyond the wall is easier than from behind. So sometimes you (organisation) may put control, but because there is an insider, it is easily compromised" (Field Interview, 2023). A fight against this threat is hence compromised from the onset because the threat actor or an accomplice is also part of those charged to defend the organisation.

The findings from the field interviews also shed light on the factors influencing cybersecurity IRT incidences. It further indicates that of the IRT causative factors identified by the Ponemon Institute's (2022) report, criminals/malicious insiders and employee/contractor negligence have been at the core of the Ghanaian phenomenon. The respondents also suggest that most cybercrimes that have involved data breaches and eventual financial thefts in the country had IRT schemes embedded (Field Interview, 2023). The economic inducement of IRT is a significant concern, with individuals getting compromised on the job due to either a preconceived agenda or monetary enticement from accomplices because of poor working conditions. This economic aspect of IRT underscores the need for a comprehensive approach to cybersecurity in Ghana (Field Interview, 2023).

From the above expositions, it is evident that the property crime and poverty/inequality nexus argument advanced in criminology literature, has gained prominence in Ghana (Jiyong et al., 2019; Raphael & Winter-Ebmer, 2001). The findings align with Akinyetun's (2021) suggestion that cybercrime in Africa is strongly linked to poverty and the search for survival. It also confirms Kaiako's (2022) conclusion that cybercriminal activities in Ghana were economically induced. These findings underscore the crucial role that human nature plays in cyber threats and cybercrime

manifestation, necessitating a theoretical approach that addresses this aspect. For instance, it supports Jaishankar (2007) theoretical postulation that the behaviors or expectations of people could change upon transitioning from one space (physical space) into a new one (virtual space). It also indicates that vulnerabilities in the cyber ecosystem are not exclusive to systems but also involve human elements. Therefore, any attempt to examine or improve the cybersecurity systems of organisations or states must go beyond structural improvements to address human security needs. The findings also echo neo-institutionalism's tenet that people do not turn up an expected good behaviour when left to their own whims (Peters, 2005, p. 26). This underscores the need to establish regulatory norms that spell out punishments and rewards for conduct in communities to complement physical infrastructure.

5.1.3 Social Engineering (Phishing attack or Identity Theft)

The respondents also identified social engineering, which constitutes confidentiality attack where the attacker uses psychological tricks to persuade an employee to divulge sensitive information or access to internal systems, as one cyber security threat in the Ghanaian cyber ecosystem. Thirty-five (35) respondents who identified this as an endemic threat in the Ghanaian cyber ecosystem also named phishing-mails and identity theft as their major manifesting forms. The respondents from GTBank, GAF, and the CSEAG President identified this threat technique as the most commonly deployed by cybercriminals in the country (Field Interview, 2023).

Phishing attacks which involve the conning of unsuspecting victims into disclosing their organisations or personal critical information through deceptive means are identified as widespread in Ghana (Field Interview, 2023). The respondent from GAF recounted that the

> *"…social engineering techniques have been deployed mostly in the Momo pin access, WhatsApp and Facebook compromise schemes. Unsuspecting victims whose credentials are compromised risk the withdrawal of their money in the case of a mobile money wallet or bank*

> *card. When it involves hacking WhatsApp and Facebook accounts, the criminals set out to extort monies or send messages in soliciting for money" (Field Interview, 2023).*

The phishing form of social engineering has manifested along with identity theft, where threat actors illegally intrude on people's privacy and use the victims' credentials to transact businesses, operate, or enter contractual agreements without their knowledge. A respondent from Slamm Technologies cited credit card fraud as one of the primary threats related to this form of threat in Ghana (Field Interview, 2023). OTP disclosures through phishing and identity theft techniques such as phishing emails or messages are another of these threats in Ghana.

From the above stipulations, social engineering is the principal tool widely adopted by cyber threat actors in the financial sector and in crimes such as mobile money fraud. The majority of the respondents agreed that cybercriminals consider the mobile money platform a fertile ground for their activities because it is a widely accepted and easy-to-use banking option for everybody, and most users lack in-depth knowledge of the technology's operation. The vulnerability of users on this score has handed cybercriminals an opportunity to execute their fraudulent activities with little effort. Two hackers confirmed this narrative when they indicated how easily a cyber-naïve individual could be defrauded by a cyber-savvy person (Field Interview, 2023).

These findings affirm Danquah and Longe's (2011, p.169) study, which identified social engineering as the most commonly deployed medium for cybercrime perpetration in Ghana. It also reveals that cybercrimes in Ghana have witnessed little change over the past decades, even though the deployed techniques have seen some modifications. By identifying the naivety of popular cyber platform users in Ghana as influencing the success of threat actors' activities, this study has extended Danquah and Longe's study contours. Thus, it has provided an understanding of factors influencing the prevailing social engineering threat identified by the actors as a dominant threat in Ghana. The study has further identified the vulnerabilities associated with social media usage, its

dangers to user identity in the ever-growing Ghanaian social media space, and the need for proper management.

5.1.4 Denial of Service/Distributed Denial of Service

The Denial of Service (DOS) attack, which is an availability attack, is another cyber threat identified by the respondents as a featuring cyber threat in Ghana's cyber ecosystem. As explained by the CSEAG president, this threat concerns threat actors (black hat hackers) deliberately generating traffic to deny system owners and users access. The respondents from the E-Crime Bureau, CSA, and other institutions collaborated in their submissions on the manifestation of DOS/DDOS in Ghana and the intended rationale behind such acts. They indicated that both fun and monetary gains underlie the motives behind such acts, but the latter dominated the intentions of most of the hackers in Ghana. The CSEAG president, for instance, intimated that.

> *"…it is common for cybercriminals to be paid by a country or institution to overwhelm the websites of Ghana or any other organisation with traffic to deny access, thereby grounding the services offered via those sites. This could lead to huge revenue loss and create disaffection or reputational damage against affected institutions or states" (Field Interview, 2023).*

After gaining control of victims' accounts, some actors may upload inappropriate content on the domains. The respondents indicated that even though the DDOS threat seems not to manifest in Ghana in the same magnitude as in other jurisdictions, it is witnessing a steady rise. The SonicWall, for instance, indicated an estimated 90% rise in the threat in 2022. The recent victims of these attacks are the Electricity Company of Ghana (ECG) and the Ga North Metropolitan Assembly, whose websites were compromised in 2022 and 2023, respectively (Dzidzoamenu, 2022 & Ghanaweb, 2023). There had also been an earlier attack on four (4) major electronic media websites, Ghanaweb, peacefmonline, myjoyonline and adomonline, in the heat of the campaign against illegal mining, popularly termed "galamsey" in Ghana in 2017 (Frimpong & Baneseh,

2017). The attacks denied legitimate users access to the sites' contents in all instances and prevented the media stations from reaching their audience.

5.1.5 Malware

Malwares is another closely related threat identified by the respondent. This threat involves deploying malicious or intrusive software developed by threat actors to steal data, damage, or destroy computer systems. The respondents argued that state and private threat actors have used malware in committing various cyber-related crimes in Ghana. The respondent from Slamm Technologies established that the prominence of the threat in Ghana has mainly been due to the widespread use of outdated technology platforms, sub-standard tools, and weak computer systems (Field Interview, 2023). He explained that most computers in Ghana are infested with malware, and black hat hackers use them for their nefarious activities on the dark web (Field Interview, 2023). The respondent from the E-Crime bureau corroborated that the malware has turned many computer systems in Ghana into bots (Field Interview, 2023).

The respondents further identified that adware and pop-up SMS on job recruitment, lottery and travel opportunities have manifested as the main baits by the threat actors in luring their targets. By accepting conversations or clicking on such links, the malware is introduced into the computer system, giving the threat actor access to the victim's system. This assertion of malware prevalence within the Ghanaian cybersecurity ecosystem affirms Baylon and Antwi-Boasiako's (2016. p7) report, which pointed to an increasing spate of its manifestation within the country.

5.1.6 Ransomware

The respondents underscored the severity of ransomware as a cyber threat that has infiltrated the Ghanaian cyber ecosystem. This threat, which materializes when malicious actors block or encrypt

crucial information of individuals, institutions, or states using software and demand a ransom for its release or unlocking, has been identified as a significant issue in Ghanaian cyberspace (Field Interview, 2023). The respondent from CSA emphasized that ransomware is not just a local issue but a growing global cyber threat, with Ghana no exception. The President of CSEAG, in his account, highlighted the recurring instances of institutions seeking his company's assistance to combat such issues and the substantial ransoms paid in some cases (Field Interview, 2023).

The respondents generally concurred that the stakeholders of industries and institutions operating with computer systems and the internet in the country are weary of this threat. The respondents stated that Ransomware attacks occur in Ghana, even though they may not have received as much media attention as the Colonial Pipeline Attack in the USA. These attacks result in significant financial losses for individuals, institutions, and the state. (Field Interview, 2023). They further indicated that many of these threats are not reported, particularly by banks and financial institutions, which are the most targeted victims, because of reputational damage concerns (Field interview, 2023). The hacking respondents corroborated this by indicating that many companies and institutions in the country run on old technology platforms and sub-standard tools with lots of vulnerabilities. This, they revealed, has made Ghana a favourable target for hackers within and outside the country. These threat actors use most of the country's computer systems as bots or agents for such attacks (Field Interview, 2023).

The respondent from MFWA corroborated with media reports of a case of this threat against the Electricity Company of Ghana's Systems in 2023, which disrupted its systems and affected customers purchasing energy in about ten distribution areas (Field Interview, 2023). Despite the ECG being mute on any breach, energy experts, including a former sector minister, hinted at the possible hacking and the likelihood of a ransom payment (Dzidzoamenu, 2022). The serving

Energy Minister seemingly confirmed this narrative in a press address on November 9, 2023. He stated, "...whether it was internal or external, it was hacked. And then there were a lot of losses that came out of the hack" (Ghanaweb, 2023, no page). Although the minister did not disclose whether the company paid a ransom, which not surprising is given the ECG's reputation, his testimony supports the respondents' assertion of a growing ransomware manifestation within the country's cyberspace. Other incidents, such as the attacks on Ghanaian companies Surfline Communications and Tema Oil Refinery in 2018, which caused significant damage to their institutional operations, underscore the manifestation of the threat and the need for immediate action in Ghana.

5.1.7 Mis/Disinformation

Most respondents also pointed to disinformation/misinformation as a significant cyber security threat element in the Ghanaian cyberspace. Defined as the unconscious or conscious intent to misinform or deceive or forward unverified messages that misinform, cyber disinformation/misinformation has also been cited as a widespread threat within Ghana's cyberspace. The high mobile phone penetration rate in Ghana and the current generation's use of social media for entertainment and information dissemination, have subjected the space to dis/misinformation (Field Interview, 2023). The respondent from the GAF explained that:

> *"...most people are using technology now and find it easy to circulate information on social media platforms, but as to the authenticity of the message they are sending, they do not care. We all then end up serving as post offices; you receive and forward without doing any background checks." (Field Interview, 2023)*

He argued, therefore, that social media has influenced much misinformation and disinformation within the Ghanaian cybersecurity ecosystem. The respondents further noted that such social media platforms as Facebook, writing blogs, WhatsApp, Messenger, Twitter (now X) and TikTok, have provided avenues for disseminating propaganda content in videos, audio, news articles,

pictures, and fake news. The dangers of this development to the peace and security of the country have prompted various stakeholder engagements. One of such engagements organised by the Media Foundation for West Africa (MFWA) in collaboration with the National Peace Council (NPC) and the National Commission for Civic Education (NCCE) ahead of the 2024 General elections discussed how the effects of the phenomenon could be mitigated (NPC, 2024).

It is crucial to stress that amidst the apparent challenges imbedded in this manifesting development, the lack of any significant progress by the social media platform hosts in curbing it further compounds the situation. False or violence-inciting statements through these mediums have, at numerous times, pushed several communities and groups to the brink of violent clashes. Morales et al. (2020) have observed the widespread manifestation of this phenomenon of dis/misinformation in several African countries, including Ghana. This disturbing situation justifies Muna, and Díaz Pabón's (2022) call for systematic checks of ultra-actions of violent incitement on social media. Such steps is required for the promotion of decorous engagements, reduced violence-inciting and hate speech, which he observes prevalent in the current social media space in Ghana.

Given the difficulty platform hosts have faced in dealing with the situation and the potential dangers of its continuous manifestation, states require country-level norms, laws and programs to deal with the phenomenon. Such interventions are, however, expected to also deal with the delicate issue of users' rights in cyberspace. The findings give credence to neo-institutionalism's assumption of the possibility of people breaching order in society and the potential of norms and institutional designs that stipulate guiding principles and sanctions, addressing the situation (March & Olsen, 2005, p. 5).

5.1.8 Data Breaches

The respondents also mentioned data breaches as a notable cybersecurity threat within the Ghanaian cyber ecosystem. Twenty (20) respondents identified this concern in their submissions. They lamented how people's confidential data appear to be accessed easily by people without authority and due process. The respondents maintained that enacting the Data Protection Act and its implementing Commission constituted the Ghanaian state's acknowledgement and resolved to protect state and citizens' critical data, but that has not helped much (Field Interview, 2023).

The respondent from the MFWA averred that the question of the safety or security of information with state institutions, such as the Electoral Commission or the National Identification Authority, begs for answers. In exemplifying the claim, she asserted

> *"... People complain about being contacted by people they never gave their phone numbers to. You receive phone calls or text messages from strange people, mostly members of the mobile money scams. During the 2020 and 2016 elections, we received phone calls from political parties. These are political parties we did not give our phone numbers to. So how did they get them?" (Field Interview, 2023).*

She maintained, therefore, that much of the data gathered on Ghanaians often gets into the hands of third parties without the people's knowledge or consent. Thus, data security and safety have continued to be a cause for concern among Ghanaians, with institutions and organisations in banking and finance, political space, general service providers, and lottery agencies pointed out as major culprits.

Two central and somewhat contrasting explanations have emerged regarding how such sensitive information gets into unauthorised persons' hands. Some respondents blamed the phenomenon on institutions, such as telecommunication companies, hospitals, banks and schools, which are privileged to collect such information as permitted by law. They explained that state institutions and agencies such as the National Identification Authority, NCA, the Electoral Commission, the Birth and Death Registry and the Passport Office can legally extract and preserve citizens' data.

Therefore, these institutions stand accused if the data in their possession gets into a third party's hands.

Another group of respondents, mainly from the telecommunication and banking sectors, rebuffed this narrative even though they admitted such institutional breaches could occur. They argued that the data breaches in Ghana are primarily the result of genius methods deployed by threat actors. The respondent from MTN commenting on this averred that.

> *"...people are wrong to always think that because telecommunication networks have information on their SIM, any time someone other than a person they have provided such information gets it, then the network provider's system has been breached, or an insider leaked them. Nevertheless, the truth is far from that. Most of the threat actors out there are smart people. They deploy various genius ways, or sometimes guess, to obtain people's telephone numbers and names." (Field Interview, 2023)*

A hacker somewhat affirmed both contrasting assertions by the respondents. He noted that threat actors could obtain information on victims or targets from several places. While maintaining genius means could be used to get information, he also did not rule out the possibility of a threat actor getting information from repository institutions. In his explanation, he averred that people within some institutions were always ready to trade confidential information (Field interview, 2023). A respondent who had fallen victim to mobile money fraud corroborated this assertion of operatives acting as information agents from within institutions. Relating this to her experience and the operation of the mobile money system, she asserted,

"Some of these scammers are friends to the Momo vendors. When I completed my transaction, the agent exposed my number and name, which was on the ID card I gave out for verification. So when he called me, he knew my full name, the amount I sent, and the time and sounded convincing" (Field Interview, 2023).

It is clear from the findings that data breaches have become a prevalent issue in Ghana, with various points of compromise. The intentions behind these breaches, whether to gain advantages over rivals or financial rewards, pose a significant threat that will escalate if not effectively

addressed. While commendable, the steps taken by the state do not seem sufficient or comprehensive enough to tackle the issue. The solution, therefore, lies in the need to define regulatory tasks, punishments, and rewards for stakeholders and users of systems to ensure accountability. The audience must be aware of these measures and strictly implement them to motivate or deter potential offenders. Therefore, achieving a safer cyber ecosystem in Ghana necessitates both institutional structures and strict compliance with norms born out of rigorous enforcement and vigilance on the part of cyberspace users.

5.2 Conclusion

The chapter examined the predominant cybersecurity threats within the Ghanaian cybersecurity ecosystem. As evidenced by the discussions, the cybersecurity threats inherent in Ghanaian cyberspace do not differ from those of the broader African cybersecurity landscape. The chapter revealed that Ghana's cyberspace has registered various cyber threats ranging from disruption to destruction and exploitation. Cyber fraud, insider-related threats, social engineering, DDOS/DOS, ransomware, malware, mis/disinformation, and data breaches constitute the dominant cyber threats in the country. Financial benefits have also emerged as the primary factor driving these threats in the country. These findings are significant and provide appropriate information for framing the required framework for assessing the country's cybersecurity response strategy, which is the preceding chapter.

CHAPTER SIX

GHANA'S CYBERSECURITY RESPONSE AND ITS ADEQUACY

6.0 Introduction

This chapter addresses the question of Ghana's cybersecurity response strategies adequacy. The objective is to examine the respondents' views on how the Ghanaian state has addressed its cybersecurity threats as revealed in the previous chapter and to establish how adequate such efforts have addressed them. To achieve this objective, the first section of the chapter demonstrates the state's role in cybersecurity management and analyses Ghana's efforts. An evaluation of the adequacy or otherwise of these efforts then follows.

Regarding the responsibility of promoting cybersecurity, the respondents were interrogated on who was responsible for promoting cyber safety and whether or not the state played any such role. In unison, the respondents consented that the charge towards cyberspace's security promotion is shared among the state, the private sector, and individual private citizens. They also added that notwithstanding the corporate responsibility, the state wielded the primary responsibility in cyber-safety promotion within its jurisdiction (Field Interview, 2023). Justifying this assertion, a respondent from the National Security Ministry reasoned, "States are in charge of security in all spheres. In the past, it had been land, border, sea, and internal security. But now, we are in the era of cyber, and so the responsibility extends there" (Field Interview, 2023). This understanding was corroborated by the respondents from CSA and MFWA, who reiterated the state's place in promoting cyber safety within its jurisdiction. The MFWA respondent notably claimed

> *"….the ultimate responsibility in cyber security lies with the state. The state has to put in place measures in terms of policies and practices to ensure that people are protected online, information people share online is safe, and information and data collected and gathered from individuals and state operations are safely guarded." (Field Interview, 2023).*

The respondent from the AU Commission similarly indicated that the government (state) is not just a passive observer but an active actor in the cyber-safety management processes. He highlighted that the state, in addition to its direct interventions towards cyber safety promotion, also plays a crucial role in coordinating the cyber threat mitigation and management efforts of non-governmental agencies, civil society organisations, research bodies, and private individuals (Field Interview, 2023). These encompassing duties make the government the central figure in cyber infrastructural establishment, norms and regulations enactments, and activities coordination for cybersecurity enhancement.

6.1 GHANA'S CYBER SECURITY MANAGEMENT RESPONSE

Having established that the state plays a central role in cyber security management and governance and proceeding to identify some of these roles, the researcher sought the respondents' views on how Ghana has fared in that respect. The results indicated that the respondents were aware of the developments within the Ghanaian cyber ecosystem and how the state has responded to its threat challenges. All the respondents could identify some of the steps the Ghanaian state had undertaken in response to its cybersecurity threat challenges. A popular view flowing through their submissions was that the Ghanaian state was committed to responding to cyber security threats. The ensuing paragraphs provide a detailed analysis of the various engagements undertaken in the country to address threat concerns.

6.1.1 The Establishment of Cybersecurity Management Strategy

The consensus among the respondents was clear: state governments, fully aware of the benefits and challenges of cyberspace, have taken up the crucial role of its management. This unanimous view echoed in all 40 responses, underscores the state being the bearer of the topmost responsibility in cybersecurity management (Field Interview, 2023). In his observation, a respondent from the

CSEAG emphasised that "cyber-security strategies or policies development constituted the foremost responsibility of the state in the promotion of cyber safety" (Field Interview, 2023). This understanding was further buttressed by a respondent from the National Security Ministry, who noted that such strategies by the state were critical in articulating its vision and priorities for the space. He elaborated

> *".... State governments are required to give direction in the form of strategies for managing their cyberspace. Such strategies provide a clear vision of the future and the state's priorities. It [the cyber security strategy] defines who will bear responsibility for what, who will be the leading and supporting agencies, and the relationship between all these kinds of bodies" (Field Interview, 2023).*

Therefore, the state takes the initiative in defining its cybersecurity strategy through its vision for cybersecurity management. The respondents suggested that the state provides governance direction or framework through well-designed governance and management strategies.

To this end, the respondents from CSA and Police CID referred to the state as the path determiner in cyber-safety promotion (Field Interview, 2023). Through the strategy, it conveys the broader vision of cyberspace and the calculated steps towards realising the desired outcomes. This proposition by the respondents aligns with neo-institutionalism's assumption that institutional frameworks and strategies, which defines roles, identities, and vision formulation on issues of national interest, including cybersecurity, are undertaken by states (March & Olsen, 2005, p.5). These management strategies become the guiding principles for attaining efficiency and effectiveness in areas of interest to the state. This constitutes a significant element because all organisations, including states, have visions and interests that constitutes their guiding compass. But given the constellation of interests from groups and individual interests therein, the state is required to carefully outline them and provide a clear path towards their realisation. Developing strategies and allocating roles and responsibilities for all stakeholders, therefore, create well

established paths towards achieving set goals and interests and promoting accountability and proper channeling of energy.

The respondents identified the National Cyber Security Policy and Strategy of Ghana as playing this critical role in the Ghanaian cybersecurity industry. This policy document, spanning five years (2016-2020) and published in 2015 after extensive considerations and engagements, was the first official articulation of Ghana's vision and expectations of cyber technology and space and its implementation. Its core provisions include the establishment of Critical National Information Infrastructure (CNII) designations, stakeholder identification, child online protection, international cooperation, education research and development, and the building of cybersecurity culture and capacity (NSCPS, 2015, pp.30-33). It also outlines the timelines for implementing and revising these policies and strategies. The respondent revealed that, upon the expiration of the policy strategy's timeframe in 2020, the CSA has initiated drafting a revised policy and strategy document. A respondent from the CSA affirmed the assertion by indicating that a new strategy document was under consideration by the Cabinet at the time of this study (Field Interview, 2023). The policy prescriptions and approaches adopted in this strategy affirm Ghana's resolve to tackle its cybersecurity threat concerns and maximise the benefits of the space. The provisions also align with arguments advanced in cyber security literature, including Azmi, Tibben, and Win (2016, p.1) and Ajijola and Allen (2022) on the relevance of states' cybersecurity strategies. These authors argue that a well-crafted cybersecurity strategy is necessary to cater for states' national interests, cybersecurity capability, and the management of threats to cyberspace. The strategy, therefore, serves as the condensation of the various steps required to manage the country's cyberspace.

The findings of this study align with international standard cybersecurity management practices set by institutions such as the ITU and cyber-advanced countries. They also underscore the

significance of regulatory principles in state governance, as neo-institutionalism theorists' advocate, and, by extension, cybersecurity management. The presence of conflicting interests within a state, as posited by neo-institutionalism, necessitates the establishment of regulatory rules that define the boundaries of actions (March & Olsen 1989, 2006). Applying this to the cyber-security ecosystems, which feature conflicting interests from states and individual users, underscores the need for a legal framework that defines responsibility, crime, and related punishments. This promotes accountability, direction, and focus in cyberspace management, aligning with Willett et al.'s (2019) assertion on the relevance of laws in state affairs.

While acknowledging the relevance of these developments in law and policy documents, which, by extension, indicate the state's commitment to duty, it is imperative also to mention that the appropriateness and applicability of such provisions are vital. The appropriateness of the response provisions is, therefore, of much critical than just their existence.

6.1.2 Promulgation of Cyber Security Legislative Instruments

Another crucial role the respondents identified as required of the state in cyberspace governance is the drafting/promulgation/institution of legislation or legal frameworks. One respondent from the National Security Ministry aptly stated, "Nothing is criminal if you do not criminalise it, and nothing is an offence until such is stated and the penalty thereof provided in a written law" (Field Interview, 2023). This underscores the significance of the state, through its law-making organs, such as parliament, passing laws that criminalise actions that can lead to criminal infractions or jeopardise the state's security (Field Interview, 2023).

The above assertion concurs with Jean Jacques Roseau's Social Contract Theory, which presents the state as the custodian of citizens' rights and the entity contractually bound to protect the same

(Bluhm, 1984). The state is, hence, obligated to enact laws through its law-making institutions, such as the parliament, for this cause (Paleri, 2022). This understanding affirms neo-institutionalism's assumption that the state is an institutional umbrella that bonds citizens despite their diverse interests and perspectives. It prevents a one-sided pursuit of self-interests or drives through its laws (March & Olsen, 2005, pp.5-8).

The respondents highlighted the role of legal instruments in guiding and protecting people, data, and infrastructure within the cybersecurity ecosystem of Ghana. These instruments, both sectoral and general, play a significant role in maintaining the security and integrity of the ecosystem. Notable among the identified instruments are the Data Protection Act, 2012 (Act 843), the Bank of Ghana Cyber and Information Security Directive (Oct 2018), the Cyber Security Act, 2020 (Act, 1038), and NCA LI (1992) (Field Interview, 2023).

The respondents subsequently revealed that following the provisions of the cybersecurity strategy and in conformity with international cybersecurity standard practices, as well as earlier cyber-related legal instruments in Ghana, Ghana passed a Cyber Security Act (1038) in 2020. The Act's core objective is to serve as a regulatory instrument for the country's cyberspace management. The Act's major provisions include institutionalising a governance authority, a critical information infrastructure, cyber security incident reporting teams, and licensing accreditation and certification. It also provides for online protection, investigatory powers on cybercrime, industry forums, engagements and penalties for non-compliance (Cyber Security Act, 2020, pp1-87).

It is worth noting that unlike the National Cyber Security Policy and Strategy, majority of the respondents demonstrated awareness of the Act's existence, its provisions, and relevance. Commenting on its content, the respondent from GAF noted, "the Cyber Security Act (Act, 1038)

spells out what every stakeholder within the state's cyber ecosystem is expected to do" (Field Interview, 2023). A cyber security expert and academic concurring with this assertion intimated that "…the Act presents the state with a robust framework for managing its space. Therefore, with a proper implementation mechanism, Ghana is assured of a serene cyber ecosystem" (Field Interview, 2023). The NCA and CSA respondents agreed with the shared views on the benefits of the Act, such as offering clarity and definiteness on the state's cybersecurity management process. However, they also highlighted that the Act's provisions would need periodic reviews and updates due to the constantly changing nature of cyberspace (Field Interview, 2023). The respondents explained that the fluidity of cyberspace, coupled with the emergence of new threats (techniques and forms) resulting from technological advancements, necessitates the implementation of modifications in existing approaches for effective redress.

The findings from the above assertions align with the provisions of international standard practice on cyber security governance outlined by institutions such as ITU and NIST (ITU, 2021 and NIST, 2018). It also affirms the significance of regulatory norms in state governance, as suggested by neo-institutionalism theorists. Per the theory's assumption, conflicting interests within a state create the need for laws to define actions' boundaries (March and Olsen 1989, 2006). With the cybersecurity ecosystems featuring diverse users (states, organisations and individuals) who habours varied and largely conflicting interests (e.g. white hat and black hat hackers), defining the proper rules of conduct constitutes a necessity for better management. This understanding also affirms Willett et al. (2019, p. 478) suggestion that harmonious engagements in human society could be realised only when responsibility, crime, and related punishments are clearly stipulated and appropriate compensations and punishments outlined. The structuration paradigm's central tenet's insistence against the absolute reliance on only structures for understanding of societal

situations further lends credence to these standpoints. Rules of engagement, as provided in the regulatory instruments, are thus, central in guiding the direction of life in a society, and therefore critical in a society's cybersecurity experience.

6.1.3 Establishment of Cyber Security Regulatory Institutions

A significant proportion of the respondents also indicated that the Ghanaian state had institutionalised management bodies, as advocated for in the Cyber Security Act and international cybersecurity professional bodies and organisations (Field Interview, 2023). The respondents explained that these established institutions have the Cyber Security Authority as the overarching body. The Authority's mandate, as contained in Section 4 of Act 1038 and alluded to by the respondents, appears comprehensive and robust. It includes advising government and other public institutions on cybersecurity, registering cyber security products and service providers, assessing, testing and evaluating the cyber vulnerabilities in cyberinfrastructure and systems, and conducting thorough examinations on computer systems for cyber security threats or incidents.

A significant element in the management processes of this institution is its stakeholder composition. The stakeholders that comprise the forum for any discourse on space issues include representatives from various governmental institutions and agencies. The respondents lauded such an expanded, multi-stakeholder approach in the governance of the space (Field Interview, 2023). Highlighting the aptness of the approach, a respondent from the CSA forwarded that cybersecurity concerns every sector of society. This makes each sector susceptible to cyber threats, but they also have unique contributions to mitigate them (Field Interview, 2023). In an attempt to exemplify this assertion, a respondent from NCA narrated how a church's computer system got hacked and obscene pictures of a respectable church member were displayed on the screens during a live

service. He explained the phenomenon to mean that sectors ordinarily considered less involved in cyberspace have all attained greater heights in cyber vulnerability (Field Interview, 2023).

The respondents maintained, therefore, that deploying an expansive composition or the Joint Cybersecurity Committee module, which has the various key stakeholders in the Cybersecurity sector sitting on one table, grants the Authority a robust decision-making structure (Field Interview, 2023). The representative from GAF observed that

> *"…the various stakeholders, ministries, and agencies whose mandate touches on cyber security or defence are all represented on the Authority. This expansive composition feature distinguishes the Authority. The situation where almost all top-ranking decision-making stakeholders in the sector are represented is in working Authority is rare." (Field Interview, 2023)*

The Authority's compositions undoubtedly affords it a better spectacle to discuss critical issues in the space at all times, as key decision-making institutions' representatives are always present on its decision-making table. A respondent from the National Security summed this up in the following words.

> *"We have a governing board for cyber security encompassing top ministers; we have Ministers of Communications, National Security, Finance, Attorney General, etc. The presence of all these ministers on a governing board rarely happens. It simply shows how serious we consider it. We have a committee and a joint committee of almost 20 Director Generals or Executive Directors of institutions that come together to plan how to secure our cyberspace. All these people's involvement is an indication of how serious we are as a country when it comes to cyber security" (Field Interview, 2023).*

As indicated by the respondents, the organisational framework established for the Authority demonstrates the state's resolve to enhance its cyber security resilience. It again illustrates the state's conviction in the need for urgent attention and quick action on cybersecurity issues. Thus, the arrangement ensures that the Cyber Security Authority always has the people needed to make conclusive decisions on issues that require urgent redress in the space.

The deductions presented here provide reasons for endorsing multi-stakeholder approaches in public administration, particularly in dynamic areas like cybersecurity. These findings align with the prevailing opinion in cybersecurity literature that suggests the need for governance frameworks

to address the wide range of cyber threats and the sectors they impact (Li et al., 2020). The results also demonstrate Ghanaian policymaker's association with ITU (2021), Bada et al. (2018; 2019), and Turianskyi's (2020) suggestions that admonish states to construct their cybersecurity governance structure along a multi-stakeholder framework, which offers them the space to respond to a wide range of concerns.

However, while the state's adherence to this standard practice has resulted in exemplary performance in the 2022 cybersecurity index performance by the ITU, securing robust cybersecurity for a cyber-ecosystem goes beyond having adequate structures. The appropriateness of the strategy and the state's implementation capacity are equally crucial factors.

6.1.4 Establishment and Protection of Cyber Security Infrastructure

As highlighted by the respondents, a key element of cybersecurity promotion by the state is the establishment and protection of critical national cyberinfrastructure and data (Field Interview, 2023). They underscored that for a state to realise its cyber vision effectively, it needs a robust infrastructure and institutional establishments as a conduit. This infrastructural development in cyberspace is a collaborative endeavour between the state and private sector actors (Field Interview, 2023). While the private sector actors engage in such ventures with profit motives, the state assumes it as the primary responsibility. The classified nature of some data further emphasises the state's role in cyberinfrastructure establishment and management. Only the state is authorised to generate, store, or define the terms for generating and storing some critical data in the country. This view aligns with the provisions of Article 35(2) of the 1992 Constitution of Ghana, which entrusts the state with both the authority and duty to protect its citizen's interests everywhere. However, the state's limited capacity influences the private sector's involvement in providing such services under the direct guidelines of the state.

Regarding implementing these practices in Ghana, the respondents revealed that the country has proactively enacted provisions for establishing and protecting critical cybersecurity infrastructure, as provided in the NCSPS and Act 1038. For instance, the NCSPS (2015, pp. 19-21) outlines modalities for establishing and safeguarding cybersecurity infrastructure for the pursuit of cybersecurity promotion. The Cybersecurity Act, Act 1038 in Section 35 and the NCSPS have both, for instance, sought the designation of CNII in specific sectors considered as critical for cybersafety and national security and sectoral CERTs established for them (NCSPS, 2015, pp.19-21; Cybersecurity Act, 2020(35)). The respondents also highlighted the state's establishment of various organisational structures such as NCA, Data Protection Agency (DPA), and National Data Centre, each with mandates and infrastructure that feeds into the national critical cyber infrastructure (Field Interview, 2023). The NCA respondents, for instance, shared their experience of creating and regulating the telecom sector and the various infrastructures, including sectoral CERTs, they have put in place to manage the state's cyberspace. They also mentioned setting up an Incident-Reponse Team that coordinates and receives reports/complaints from clients on the efficiencies or deficiencies in the sectors (Field Interview, 2023).

The CSA respondents equally confirmed the designation of some sectors as critical national information infrastructure and a national CERT. Other institutions, such as the Data Protection Agency, National Identification Authority (NIA), and National Information Technology Agency (NITA), have been mentioned as part of those institutions and infrastructure established by the state in support of its cybersecurity governance agenda (Field Interview, 2023). These findings in the National Cyber Security Act (Act 1038) and National Cyber Security Policy and Strategy (2015) provisions, with the same alluded to by the respondents, indicate the Ghanaian state's acceptance of a duty to set up strategies for its cyberspace management and implement them. These

findings also affirm the aptness of the argument for a targeted governance approach in cybersecurity management, especially for cyber-infant states such as Ghana (Bada et al., 2019, p.20).

6.1.5 The Licensing of Cyber Security Service Providers and Professionals

The licensing of cyber practitioners and institutions offering cyber security services was also identified as the Ghanaian state's effort to promote the security of its cyber ecosystem. As provided for in Section 49 of Act 1038, the Ghanaian state is obliged to regulate the usage of the cyber skillset within the country. Commenting on the essence of the licensing, a respondent from CSEAG explained that it seeks "to ensure that the cybersecurity professionals we have in the country, at least, have some level of knowledge, skills, and expertise to help organisations, individuals and the state combat cybercrimes" (Field Interview, 2023). A respondent from the Cyber Bureau of the Police CID added that such registration is required and constitutes an effective measure in helping to bring credibility and formality to the reports produced by the registered bodies and individuals engaged. According to him, this intervention offers those reports credibility for acceptance as evidence in competent courts of jurisdiction for prosecutions (Field Interview, 2023).

While acknowledging the legality of the exercise, a section of the respondents dissented over its timing and modalities. Three respondents and members of CSEAG raised concerns over the charges that practitioners and organisations were to pay. One of the respondents averred

> *"…you want me to license my organisation at a fee. But then, even before I started the business, I was already doing freelance work, and most of our contracts didn't even come from Ghana. So if my contracts are not from Ghana and you want me to pay a licensing fee, you know it becomes a problem (Field Interview, 2023).*

They projected that the policy had negative repercussions, the major of which was the high propensity of practitioners and service providers, who consider such conditions unbearable, to exit

the jurisdiction or move to operate behind the scenes. However, in sharp contrast to this assertion, the GAF respondent maintained that the exercise attempts to harmonise the country's cyber workforce for strength capability assessment, which the service providers themselves stand to benefit from in times of collaboration. He continued that

> *"…if we have identified that workforce development in cyber security is a challenge, but there are people already working in the space, it is proper that we know that population. These statistics will be empirical proof of the percentage of cyber professionals and what percentage or numbers we need to add. We can also tell which of the professionals we have and which are lacking. This information is key for policy-making and direction" (Field Interview, 2023).*

The respondent indicated that people would typically object to regulatory policies because of the operational restrictions and economic burden they generate for them. However, the benefits of such initiatives to the public and their contributions to building a more resilient cyber ecosystem outweigh those personal considerations. A respondent from CSA agreed with the above position, indicating that the initiative would benefit all the stakeholders in the space. Apart from affording state authorities a clear overview of the space, the exercise is also considered helpful to professionals and service providers in the country. He explained that those professionals and service providers could enjoy immunity from unnecessary competition as the CSA is keen on barring all unregistered professionals or service providers from operating within the country.

The above assertions indicate the need for continuous engagement and vigilance over persons' and organisations' conduct within cyberspace as their interests and drives are subject to change. Although the policy of registering and monitoring the activities of cyber professionals seems promising, there are concerns about its implications that need attention. For example, the policy may lead to attrition in cyber professionals and force some to operate behind the scenes. Additionally, the policy may create opportunities for space hijacking. This happens when individuals and organisations close to the corridors of power, regardless of their knowledge and expertise, can easily obtain licenses and win contracts to provide critical services.

6.1.6 Ratification of International Protocols

According to the respondents, one significant step the Ghanaian government has taken to enhance the security of its cyber ecosystem is ratifying international treaties. The government has been actively participating in international conferences and has signed various treaties and conventions as part of its cybersecurity promotion effort.

Most respondents alluded to the importance of international cooperation in cybersecurity management. They submitted that Ghana's cyber security ecosystem management could not be administered exclusively by Ghana alone. This conviction influenced the provisions on collaboration in the NCSPS (NSCPS, 2015, p.33). The respondents believe unilateral cyber response attempts, especially by developing states, are ineffective against borderless cybercrimes (Field Interview, 2023). These reasons, hence, underscored the need for Ghana to enter bilateral and multilateral treaties with other states and organisations at both the regional and international levels. After taking this path, Ghana has joined and ratified all the major international cybersecurity treaties and conventions it is qualified to join (Field Interview, 2023). Key among these are the Malabo and Budapest Conventions spearheaded by the AU and UN, respectively, and the ECOWAS Regional Cybersecurity and Cybercrime Strategy by ECOWAS.

The respondent from the MFWA signalled that the Ghanaian remarkable feats in cybersecurity management cannot be distanced from its engagements with the international community at these levels. She remarked that

> *"…Ghana is making strides internationally and regionally by ratifying the Budapest and Malabo Conventions. This step helps us learn from and pick strategies for implementation in our ecosystem. For example, the Cyber Security Act has elements or discussions or things mentioned in the Budapest Convention, and the convention also admonishes and obliges the state to do them" (Field Interview, 2023).*

The respondents from EOCO and the National Security Ministry agreed by adding that the Ghanaian state has strived to refrain from going against the provisions of the conventions it is a signatory of. The obligation to observe cybersecurity management standards placed on Ghana by international protocols has shaped its governance strategies and responsibility towards other states and vice versa. Commenting on this, the respondent from EOCO averred, "...because of the pacts, we (Ghana) can liaise with other countries like the USA, to shut down or track sites and individuals suspected to be engaging in criminal activities in cyberspace." (Field Interview, 2023). The respondents from National Security, reflecting on this, maintained that the country had showcased its conviction in the relevance and commitment to this approach of cyber security management by being among the first group of countries to ratify the Second Pact of the Budapest Convention in 2023 (Field Interview, 2023).

The revelations in the above paragraphs have further affirmed the relevance of institutions and norms in cybersecurity management, suggested by the neo-institutionalism theory, which underpins this study (March & Olsen, 2005). Thus, the treaties signed by Ghana now afford her the support of other states and oblige her to offer other states the needed support in addressing cyber threat challenges. Therefore, Ghana's cybersecurity strategy's provisions are expected to consider the provisions of these international treaties and conventions. The findings confirm the importance of corporate governance in managing cyberspace, and Ghana is ready to embrace this approach. This aligns with the recommendations put forward by Luiijf, Besseling, and de Graaf (2013) and Mussington (2019) for effective cyberspace management.

6.1.7 Promotion of Collaborative Efforts

The respondents also highlighted collaborative initiatives as a significant measure through which the state bolsters the security of its cyber ecosystem. According to the respondents, the necessity of cooperative efforts in cybersecurity promotion stems from the transboundary, intricate, and dynamic nature of activities in cyberspace (Field Interview, 2023). Investigators would need to access the systems and crime scene for tangible evidence when a crime is perpetrated against a victim in one country, but the evidence is located in another. Given the security implications of such processes, investigators would necessitate the express permission and support of the sister state for a meaningful investigation.

To reinforce this point, the respondent from the E-Crime Bureau stated, "Cybercrimes are different from traditional (physical) crimes on many fronts. They (cybercrimes) characteristically involve crimes that can be committed from outside a country, creating the need for collaborative efforts among targeted or affected countries" (Field Interview, 2023). Criminal syndicate members operating beyond states' borders can only be tracked and arrested through collaborative efforts (Field Interview, 2023).

It is crucial to indicate that similar collaboration efforts occur within the state as it pulls together the expertise and energies of various subsectors to propel its cyber security promotion agenda. Cooperative efforts by states in cyber security management are, therefore, indispensable, especially for cyber-infant countries like Ghana that are seeking to tackle complex cybercrime..

6.1.7.1 Forms of cybersecurity Collaborations in Ghana

The respondents clarified that state collaborations in cybersecurity promotion occur at different levels. They involve external (state-to-state) and internal (state-to-private sector industry players, state-to-CSOs, and public institutions) (Field Interview, 2023).

State-to-state collaborations, occurring mainly internationally (Calderaro & Craig, 2020; Craig, 2020), involve two or more states or states and international organisations. The collaboration is conducted through the parties' officials or representatives assigned for such a purpose. Ghana's involvement in this collaboration resulted in her signing the cybersecurity protocols, such as the Budapest and Malabo Conventions (Field Interview, 2023). The provisions of these protocols further oblige the state to collaborate with other member states.

The Budapest Convention, for instance, establishes the obligation for parties to cooperate in Article 23. The Convention, in its general principles relating to international cooperation, provides,

> *The Parties shall cooperate with each other, in accordance with the provisions of this chapter, and through the application of relevant international instruments on international cooperation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence." (Budapest Convention, Article 23)*

Similarly, Article 28 of the Malabo Convention obliges its member states to observe international cooperation in harmonising legal provisions, mutual legal assistance and exchange of information (Malabo Convention, Article 28 (1-3)). It further charges member states to use existing means of cooperation, such as international, intergovernmental or regional, or based on private-public partnerships, to improve cybersecurity and stimulate dialogue among stakeholders (Malabo Convention, Article 28(4)).

Based on the above provisions, Ghana, a state party to the two Conventions, has cooperated with other member-states in various dimensions. For instance, the country partnered with the USA to build capable and resilient security and justice sector institutions, which had cybersecurity as a critical component (US Embassy in Ghana, 2020). Ghana is also a member of AfricanCERT, a group coordinating cooperation among African Computer Security Incidence Response Teams (CSIRTS).

The other forms of cybersecurity collaboration witnessed in the country are internal ones. The first in this line is the state (public)-to-private sector collaborations. Here, the collaboration is between the state and other non-state entities or parties (Field interview, 2023). The state's partners in these categories include industry players and CSOs. This collaboration has manifested in Ghana through dialogues, public lectures, and awareness creation organised by the CSA, CSOs, the mass media, and other state institutions. For example, in a groundbreaking initiative, Slamm Foundation, a Corporate Social Responsibility arm of Slamm Technologies, in collaboration with the International Information System Security Certification Consortium (ISC2), provided free training to over 400 participants during the 2023 Cybersecurity Month Celebration. The training was designed to empower individuals with essential cybersecurity skills towards a safer online environment and digital inclusivity (Citi Newsroom, 2023).

In line with the above, a respondent from the National Security Ministry opined that

> *"... the majority of cyber security infrastructure is outside the government's ambit. Private actors own it. But given that the state would be blamed if citizens suffer damages from these infrastructures, the state is obliged to collaborate with the private sector to ensure their security" (Field Interview, 2023).*

The respondents, thus, identified that the private sector controlled a significant portion of the stakes in cybersecurity infrastructure and installations. In Ghana, for instance, the telecommunication and financial sectors, which are the most targeted by cybercriminals, also have much of their shares in

private ownership. Telecom operators: MTN and Vodafone, who provide internet, call services, and banking and financial products such as mobile money, are all privately controlled (Field Interview, 2023). In addition to this infrastructure, a chunk of skilled cyber professionals are also found in the private sector. Ghana has acknowledged this and, according to the respondent from the E-Crime Bureau, has taken steps to collaborate with these industry players and tap their expertise and infrastructure to promote cyberspace safety. He asserted thus:

> *"…being a private organisation, our role is primarily through partnerships and collaborations under various MOUs with the various government institutions. If a government institution requires investigation, for instance, we can do it entirely by ourselves. We also have specific tooling, analysts, and experts, which the government lacks. So, we work with many state institutions by either training them on cyber awareness, technology or technical expertise" (Field Interview, 2023).*

Therefore, the state can greatly enhance its efforts to safeguard users and systems with the direct support of these stakeholders and partners (Field Interview, 2023). While remaining the primary bearer of the responsibility to safeguard cyberspace systems and users, the support of the private sector players who control cyberinfrastructure and expertise remains indispensable.

Closely related to the above is collaboration between the state, CSOs and the media. The promotion of cybersecurity thrives on information availability, awareness, and advocacy, which constitute the core activities of CSOs and the media. To this end, the private sector, particularly the CSOs, within the cybersecurity space have developed the expertise and knowledge base to offer constructive policy recommendations for policymakers. They also have easy reach for their audience through their established engagement channels. The respondents noted that the private sector contributes to the discourse on policy designing and implementation for the governance of Ghana's cyberspace. The MFWA respondent recounted several times the government sought their input during cyber policy design and implementation. Narrating the role they played during the

preparation of the National Cyber Security Policy and Strategy, the MFWA respondent forwarded that,

> *"... We contribute to some national-level discussions that go into policy. Some of these policies our contributions have shaped in cyber security are used to govern the space and create awareness. We have been involved in the cyber policy discussions at the national level. We are mostly given these drafted policies to study and make our input, and we see that the inputs we make are considered" (Field Interview, 2023).*

Therefore, several engagements by the CSO community and the central government have been advanced for cybersecurity promotion. For instance, in the build-up to the 2024 General elections, the Media Foundation for West Africa (MFWA), in collaboration with the National Peace Council (NPC) and the National Commission for Civic Education (NCCE), organised a public forum on how to dis/misinformation and propaganda narratives (NPC, 2024). Again, Youth Bridge Foundation, in collaboration with Joynews, also organised a national dialogue on "strengthening cybersecurity protocols and safeguarding citizens' vulnerability". The dialogue, which brought together industry players, cybersecurity experts, banks and policymakers, assessed and offered policy recommendations for enhancing the security of the country's cyberspace (Adu-Owusu, 2024). These engagements' impact on the safety of Ghana's cyberspace is enormous.

The final form of internal collaboration is among state institutions. This collaboration effort involves two or more state institutions uniting their energies to promote cyber safety (Field Interview, 2023). These collaborative efforts have manifested in the Ministries of Communication, Interior and National Security joint symposiums to educate citizens on cyber security. The Ministry of Education has also partnered with the CSA to roll out cyber education in schools within the country. The National Communications Authority (NCA) also partnered with CSA to organise a sensitisation workshop on cybercrime and cybersecurity for its staff. The forum highlighted the authority's engagement with Mobile Network Operators (MNO) and Undersee Cable Operators

(UCO) to assess their readiness for cyber challenges as some of the measures it had taken to promote cybersecurity (NCA, 2023).

6.1.7.2 Formal and Informal Cybersecurity Collaborations

The respondents further elucidated that the collaboration employed by the state in cybersecurity promotion assumes both formal and informal natures. Adopting the two collaboration streams results from the fluid and complex nature of events in cyberspace. The Ghanaian state has adopted both collaboration mechanisms in its cybersecurity promotion mechanisms. While the formal has involved the documented formalities of duties of parties in collaborative engagements, the informal does not follow any such order and relies mostly on informal contacts or conversations.

Corroborating this assertion, the EOCO respondents explained that,

> *"... not all that happens is part of what is spelt out in books or working documents. The speed at which cybercrime evidence disappears requires that investigators trigger some informal processes to save pieces of evidence before moving on to formalise the process." (Field Interview, 2023).*

The informal mechanism is even deployed at both the domestic and interstate levels. At the interstate level, partnering investigators usually rely on their contacts for briefings before formal information exchange. A similar situation transpires within the democratic space where state institutions collaborate among themselves or even the ordinary citizens. The National Security Ministry's *"If you see something, say something"* awareness drive underscores the informal collaboration. The drive encourages citizens to report or provide information on any suspected criminal incident or activity to the appropriate authorities for action.

From the above, it is apparent that the two forms of collaboration complement rather than contrast each other. Thus, while the formalised processes with legal backing are recognised and applied,

the bureaucratic process that characterises them slows their implementation. This is the gap the informal processes fill by helping to preserve evidence. Given that such informal processes contravene the established standards, the formal processes followed afterwards to help legitimise the process and make their results admissible as evidence in courts for prosecution, if required.

The findings from the above analysis align with Calderaro and Craig's (2020) and Craig's (2020) suggestions for the need to frame cyber management approaches with transnational coherence and coordination in mind. Such an approach, which Mussington (2019) and Luiijf, Besseling, and de Graaf (2013) corroborate, provides an opportunity to deal with the resultants of the complexities and borderlessness of cyberspace. The findings also strongly advocate for the multi-stakeholder cybersecurity governance model, which has been trumpeted by 2014 NetMundial (WSIS, 2005, 35(a) and gained significant traction and recognition. This model involves governments, private sector players, technical communities, CSOs, and other entities as the critical stakeholders required to promote cyber security collaboratively.

The assertions again affirm neo-institutionalism's assumption of the relevance of informal institutions and processes in state governance. Kshetri's (2019) and Bada, Von Solms, and Agrafiotis's (2019, p.109) arguments that the private sector plays pivotal roles in cybersecurity and hence should be considered a significant stakeholder in any attempt to secure the space has been given much impetus by the findings.

6.1.8 Cyber Security Awareness Creation and Education

The respondents again identified cybersecurity awareness creation and education as other vital efforts the Ghanaian state has attempted in its cybersecurity management process. The thirty-two (32) respondents who mentioned this explained that the responsibility to create cyber awareness

among citizens rests with the state. According to them, such exercise seeks to boost citizens' appreciation of the opportunities and risks involved in using cyber technology (Field Interview, 2023).

The respondents highlighted that the state is responsible for educating citizens on cybersecurity. However, this is done with the support of the private sector, including industry players and Civil Society Organisations (CSOs), who have that duty as a corporate social responsibility. CSO's contributions are essential and enhanced by their synergy with the citizenry. Therefore, while the state is primarily responsible for creating citizens' cybersecurity awareness, the responsibility is shared with industry players and CSOs (Field Interview, 2023).

In addition to creating cyber awareness, the respondents indicated that the state was responsible for promoting cyber education. Unlike the awareness creation, cyber education takes on a more structured and closed instructional mode. Through this model, the state, with the support of other professional bodies, attempts to equip citizens with relevant cybersecurity knowledge and skills. The respondents from CSA and GTBank stressed that it helps shape citizens' attitudes and values towards life in cyberspace, i.e., cyber-culture orientation.

The respondents consented that there have been attempts to promote both cyber awareness creation and cyber education in Ghana. Such efforts are inspired by the state's commitment towards promoting cybersecurity culture and capacity building as stipulated in Section 3(4) of the national cybersecurity strategy (NSCPS, 2015, p.31). Regarding awareness creation, the respondents mentioned the annual Cybersecurity Awareness Campaign Month. This celebration, slated for every October, is aimed at helping to promote, inform, and educate citizens on the space's

opportunities and promote threat hygiene practices towards building a more robust cybersecurity culture (Field Interview, 2023).

Commenting on the cybersecurity awareness month, the respondent from the E-Crime Bureau posited that the observation is gaining traction. According to him, the display and sharing of flyers with cyber hygiene inscriptions characterize this celebration (Field Interview, 2023). While applauding the state's awareness creation month initiative, some respondents expressed dissatisfaction with its programming. The response from the National Security Ministry, GAF, Police CID, UPSA and GI-KACE raised concerns over the initiative and all its related programs being limited to just a month within the year. A respondent from UPSA reasoned

> *"....Cybersecurity awareness should be a continuous process. It shouldn't be something that we talk about and make much noise about once a month in the year and go to sleep. Cyber-attacks do not happen once a month or once a month all year round. So we need to have continuous education and awareness creation." (Field Interview, 2023)*

The respondents thus argued for a continuous campaign instead of a one-time, month-long annual celebration. Their justification is that it was the appropriate approach for dealing with the evolving concerns in the space. Thus, given that cyber security threats and threat actors' activities are continuous rather than periodic, continuous awareness creation is also required (Field Interview, 2023). Against this narrative, the respondent from the E-Crime Bureau proposed the adoption of any available avenues for sustained awareness creation. He advocated using radio and other media channels (both traditional and social) and incorporating heavily patronized government institutions to sustain conversations and broaden the campaign's reach (Field Interview, 2023). He expounded that

> *".... there are areas where government institutions can contribute. If people go to government offices and state-owned enterprises such as DVLA, Hospitals, and Bus terminals like STC, and wherever they pass, they see posters on cyber security practices such as, "Do not pick up a pen drive that you don't know who it is for," pasted, it will imprint it in their mind. (Field Interview, 2023)*

The respondents again mentioned that apart from the Cyber Awareness Month Campaign, the state has also instituted other activities to promote cyber awareness and education. The E-Crime Bureau and CSA respondents mentioned that the Ghanaian state had added engagement at the school level to its cyber awareness and education module. They referenced the high-school cyber drive, which the Cybersecurity Authority's Child Online Protection Unit initiated in 2022 with a National Cybersecurity Challenge. The E-Crime respondent stated that

> *"....It started with six schools and expanded to about 50 this year. These competitions are styled similarly to the national science and math quiz competitions but are solely on cybersecurity issues. You see that these things drive awareness because if you attend the quiz as an audience and the participants have to talk about cybersecurity issues, you will leave there informed" (Field Interview, 2023).*

So, like the famous National Science and Maths quiz, the initiative is anticipated to help develop students' interest in cyber security and draw participants' and audience's attention to the need and means of cyber hygiene maintenance.

The above assertions affirm Peltier (2005), Bada, Von Solms, & Agrafiotis (2019, p.109), and Her UK Majesty's Government (HMG) Security Policy Framework position on the place of cyber security awareness and education in cybersecurity promotion. The literature has argued that these processes stimulate and remind citizens of what is required of them in cyberspace. This consciousness ultimately engenders robust cybersecurity culture construction. Again, the unremitting awareness campaign argument lends credence to the NIST (2018) framework. In the framework, NIST had strongly considered unabated awareness creation processes as non-negotiable for any state desiring to realise a hygienic cyber ecosystem. Similarly, it approves Bada, Von Solms, and Agrafiotis's (2019, p.109) suggestion for adopting multi-varied activities involving various stakeholders for cybersecurity promotion as a worthy approach.

6.2 THE ADEQUACY AND EFFICIENCY OF GHANA'S CYBERSECURITY STRATEGY

As demonstrated earlier, Ghana has undertaken several programs, projects, and policy measures to improve its cyberspace's security and maximise its benefits. These efforts, which have earned commendations from the international community, including organisations and states such as the ITU (2021), were applauded by the respondents. However, some respondents expressed reservations about the state's response approach helping to realise the much desired results. A respondent from the National Security Ministry, along this view, contended that Ghana's cyber security governance approach appears somewhat misguided in maximising the opportunities and addressing the evolving threats in cyberspace (Field Interview, 2023). He reasoned that the Ghanaian strategy overly concentrates on cybercrime and appears mute on evolving cyber concerns such as the weaponisation of the cyberspace. He quipped

> *"....weaponisation of the space has taken centre stage, and countries have started moving along that direction. If you look at the 2014 Quadrennial Defence Review of the United States, it recognises cyber as the next frontier in warfare. Countries have started developing cyber weapons, but Ghana's strategy has not yet envisaged that. It, therefore, does not orient us to be able to face the world, as it will be in a few years to come." (Field Interview, 2023)*

To this end, the respondent maintained that Ghana's cybersecurity strategy provisions do not adequately reflect the times and the higher matters in the cyber industry.

Although firmly argued, the respondent failed to consider the impact of the state's peculiarities on policy and strategy direction in the analysis. It is indeed palpable that states' power, influence, and capacity shape their interest and approaches in politics (both international and domestic). This line of understanding featured in the reasoning of differing respondents who argue that while it appears prudent for states to be forward-looking in cyber security strategies, cyber-infant countries needed to tread cautiously because of the resources and technology required to accomplish such ambitions. Emphasising this, a cybersecurity expert stressed,

> *"…developing countries such as Ghana only need to focus on tackling the manifesting threats rather than scavenging everything that could emerge. This is particularly necessary because of the resources and expertise required to tackle cyber security on several fronts." (Field Interview, 2023).*

Furthering this line of reasoning, the respondent from the AU Commission underscored the need for cyber-immature countries to prioritise and adapt cyber security infrastructure tailored to their country-specific threats rather than throwing resources at addressing all threats. To him, if states prioritize addressing the manifesting threats with the resources and technology within their reach, even a non-wealthy nation could still assemble a solid cyber defence (Field Interview, 2023). So, despite the seeming validity of the concern that Ghana's strategy or approach is not ambitious enough, the state's approach justifiably aligns with its position as a cyber-infant country with limited financial and skilled human resources. This conclusion concurs with Apau and Koranteng's (2020) and Roshanaei's (2021) suggestion that states with limited technology and other resources need a targeted rather than broad focus in their cybersecurity management approach. Therefore, addressing all manifesting and potential cyber threats in Ghana would have been imprudent, given the country's deficiencies in cyber technology, experts, and financial resources.

Despite the debates on the strategy's focus, the respondents unanimously acknowledged Ghana's commitment to promoting cyber safety. They emphasised that cybersecurity promotion goes beyond the mere availability of strategies. This aligns with the World Economic Forum (2022) report, which observes that targeted approaches, such as channelling investments into core fundamentals like asset, vulnerability, and patch management, greatly enhance cybersecurity. They also noted that while the threats in Ghana's cyber ecosystem are not unique to other African or developing countries, the state's social, economic, political, and geographical characteristics offer a unique context for its cyber ecosystem (Field Interview, 2023). This perspective justifies the state's tailored management strategy to address the specific concerns of its cyber ecosystem.

As already established, Ghana has heeded the obligation of cybersecurity promotion. This conviction has resulted in the fashioning of a cybersecurity strategy, a Cyber Security Act, and a regulatory body with its supporting agencies. The developments have put the state in the spotlight and attracted commendations and good ratings from international cybersecurity watchers such as the ITU (ITU, 2021). These exertions of the state, which involved both domestic and international programs, projects, and collaborations, have, however, not gone without challenges, affecting the full realisation of the intended objectives. The identified issues are discussed in the ensuing paragraphs.

6.2.1 Anti-Cyber Security Social Norms/Culture

To begin with, one major issue that emerged as bewildering Ghana's cybersecurity threats management is the manifest dominance of anti-cyber security culture in the country. Anti-cyber social norms or culture here refers to the behavioural patterns or norms considered misfits in cyberspace. Such behaviours contravene cyber hygiene, expose the individual to more cyber threats, and complicate the fight against cyber threats. Among the anti-cyber security cultural or social norms identified are:

- The culture of credulousness or gullibility.
- A lack of security consciousness.
- Aversion to crime reporting.

6.2.1.1 Credulousness or gullibility in information sharing

Credulousness or gullibility within the Ghanaian community is identified as one of the paramount anti-cyber security social norms that militate against cyber security hygiene promotion in Ghana. The respondents argued that the community-based living system among Ghanaians has given community members the duty to support others. This belief has faded the thoughts or reservations

of people harbouring bad intentions (Field Interview, 2023). People are thus assumed to be good, and community members repose high confidence in their engagements with their neighbours. Explaining this, the CSEAG president noted that

> *".... that culture of individuals trusting and being less suspicious of others is ingrained in the Ghanaian. Irrespective of our religious or ethnic backgrounds or anything, we still see ourselves as a family and trust each other. People hardly suspect that a neighbour has the tendency of attacking them in the cyberspace. So if a neighbour comes to say Oh, I'm your neighbour and I just wanted to connect to your Wi-fi to update something right now. The first thought that comes to mind is having gotten an opportunity to help a neighbour rather than getting your password compromised or him intending to use your router to even commit a crime." (Field Interview, 2023)*

Corresponding to this narrative, the respondent from the MFWA opined that mobile money scamming, one of Ghana's most endemic cybercrimes, has thrived behind this culture. She stressed that for someone to entertain a strange caller narrating stories of wrong money transactions and be willing to check their account and return such an amount showed how ingrained the phenomenon was in Ghana. A student also related that the prevalent issues like romance scams and non-consensual distribution of intimate videos and photos (revenge porn) in the country owed their source to this norm (Field Interview. 2023). Corroborating these assertions, a hacker argued that such habit among Ghanaians made it easier to get people to fall to even old tricks and get swindled or serve as a man-in-the-middle for an attack (Field Interview, 2023).

It is imperative to note that these socio-cultural norms contravene acceptable norms in cyberspace. Unlike generally accepting and treating people as innocent norms, cyberspace culture sees everybody as a criminal or at least a potential criminal from the onset. Again, the well-appreciated communalist Ghanaian lifestyle is seen as a dangerous path in cyberspace. Reiterating this point, a National Security respondent explained that people do not behave the same way when they move from one space into another. So, to judge anyone in cyberspace based on who the person is in the physical space would amount to threading a dangerous path (Field Interview, 2023). However,

according to the respondents, this is what Ghana's cultural orientation promotes (Field Interview, 2023).

This revelation agrees with Bada, Von Solms, and Agrafiotis's (2019, p.109) conclusions on cybersecurity maturity in Ghana and five other countries. Ghanaian citizens were found to be gullible in giving information even to strangers. The underlying view of people taking the different characters in cyberspace also affirms Jaishankar's (2007) "Space transition theory". The assertions, therefore, reveal the contrasting relevance of practising customs in the physical and cyber worlds.

6.2.1.2 The Lack of Security Consciousness

Another anti-cyber security social norm found endemic in the Ghanaian community is the lack of security consciousness among the citizenry. The respondents suggested that Ghanaians generally pay less attention to their security and are more inclined to reactive rather than proactive measures in security matters. Despite the severe consciousness it portends for individuals, organisations, and state security, this behaviour has transitioned into cyberspace. It remains endemic among the country's literate and non-literate population, rendering many cyber users susceptible to cyber threats (Field Interview, 2023). Exemplifying this phenomenon with cyber services or product usage, the respondents indicated that most Ghanaians are more interested in the output than in understanding the effects of their systems or products. Arguing along this line, the respondent from Police CID observed that

> *"...the typical Ghanaian is less concerned about the security implications of the apps and websites they subscribe to and visit. All they look out for is to be able to open it and view what is there. People get video links on WhatsApp and other social media platforms and hastily click to see what they contain. These people will accept any pop-up or consent without reading a line for at least a gist of the agreement". (Field Interview, 2023)*

This anti-cybersecurity social norm among Ghanaians manifests in homes and offices. Respondents from CSEAG and a hacker outlined how such actions compromise individuals',

institutions', or states' computer systems. The CSEAG respondent, for instance, narrated, "…people who live a free life and like to post everything about themselves, including pictures taken at their workplaces on social media, become agents for criminals unknowingly." (Field Interview, 2023). This act provides excellent leads for attacks because it gives the attacker much information about the target. A respondent noted

> *Some take pictures and videos of themselves in their offices with their monitors on. That way, you can identify the operational icons and determine the operating system the entire organisation uses. Such information is solid to start with and can make your attack against the organisation easier" (Field Interview, 2023).*

Despite the ethical rules that some organisations institute to reduce such practices, this anti-cyber norm still manifests because of the ingrained security-unconscious attitudes among Ghanaians. This revelation, which concurs with Asamoah's (2019) observation of Ghanaian indifferent attitude towards terrorism, has further been impacted by the general low knowledge of the operations of internet technology among Ghanaians (Chen et al., 2014). Hackers and other threat actors have, thus, continually exploited this trait in luring their targets to pick up strange calls, divulge confidential information, or click phishing links to compromise their credentials.

6.2.1.3 Aversion to Reporting Crime Culture

A third societal norm in Ghana found to be anti-cyber security practice is the aversion to reporting criminals or criminal incidences to law enforcement agencies or authorities. The respondents noted that Ghanaians rarely report incidents to law enforcement agencies. They explained that Ghanaian society is not oriented toward honouring the civic duty of reporting crime and providing information on criminal activities to appropriate authorities (Field Interview, 2023).

Individuals who turn against this status quo are branded traitors and nonconformists in their communities. Remarking on the phenomenon, the CSEAG President indicated that once someone

attempts to inculcate a reporting habit, he or she is nicknamed a ***"chook" or "Babylon"*** (Field Interview, 2023). People would, therefore, conceal information or ignore criminals and criminal activities to maintain an acceptable personality rather than do otherwise. According to the respondents from NCA, the reporting aversion culture in Ghana is endemic and was responsible for low statistics on issues that are known upon victims' reporting. This is the reverse of what exists in countries where citizens highly honour their civic duty of reporting what they should report to the appropriate authorities (Field Interview, 2023). The phenomenon denies authorities valuable data and hampers their decision-making. The role of information in fighting crimes, particularly cybercrime, coupled with the fast pace at which evidence in cyberspace disappears, places the effect of this norm as a critical concern in cybersecurity management.

The impact of these cultural norms on Ghana's cybersecurity management is informative and worrying. The findings on these anti-cybersecurity norms also echo the suggestions of Bada, Von Solms, and Agrafiotis (2019, p.109) and the HMG Security Policy Framework, emphasizing the need for a cultural shift as states adapt to the new cyber world. This shift has become necessary and agrees with the neo-institutionalist's assumption of the protocol for continuity or change in state practices (March & Olsen, 2005, p.5). The assumption is that a system, norm, or practice should be changed when it no longer fits the current time or situation.

6.2.2 Financial Challenges

Financial constraints are a significant hurdle, posing a challenge to cybersecurity governance efforts in Ghana. The respondents emphasized that African states' efforts to address cybersecurity challenges are often caught in a balancing act as they grapple with a multitude of other pressing developmental concerns vying for attention and resources (Field Interview, 2023). This struggle is

further exacerbated by the high capital requirements of cyberinfrastructure and the ever-evolving sophistication of cyber threats.

The Ghanaian cyber ecosystem is said to share the above characteristics. However, while most regulatory agencies in critical and technology-inclined sectors can generate enough resources for their activities, the respondents indicated that the same could be said of CSA and its sister agencies. A respondent from the CSA affirmed this by asserting that although several revenue sources have been provided in the authority's operations support stipulated in Article 23 of Act 1038, government subventions and donor support have been the mainstream sources thus far. The demand for the government to provide several other public and social goods in the health, education, transport, and agriculture sectors has further stifled the scarce resources and slimmed the chance for cybersecurity projects to be considered in the budget (Field Interview, 2023).

The above indicates that a chunk of the support is expected from donors who only get involved when they deem a project appropriate. The development also exposes the country to external controls on the management of its cyberspace. Through their support, donors gain the moral locus to define or influence policy decisions, projects, and even technologies deployed in the country. The respondent from the UPSA explained that the phenomenon often leads to the state embarking on projects that focus on getting it to qualify for donor support rather than addressing nagging cyber challenges faced by the country (Field Interview, 2023).

These findings align with the conclusions drawn by the World Economic Forum (2024), Raemdonck (2021), and Target (2010) on the detrimental effects of financial challenges on the effectiveness of cybersecurity management in developing African countries, including Ghana. The revelations also shed light on why developing states are more susceptible to adopting policy

measures and suggestions from well-meaning but potentially misguided donor partners rather than formulating response strategies tailored to their unique circumstances.

6.2.3 Limited Cybersecurity Awareness and Education

Emphasising the pivotal role of cyber awareness and education in promoting cyber safety, as underscored in Peltier (2005), Bada, Von Solms, and Agrafiotis (2019 p.109) and HMG Security Policy Framework, the respondents expressed deep concern over the alarmingly low levels of its implementation in Ghana. They stressed that regardless of the use of advanced technologies, robust installations, effective management, and governance mechanisms (sound laws), a community of uninformed citizens on cybersecurity practices and hygiene renders the system highly vulnerable.

Justifying the above conclusions, the respondents from GAF, EOCO, and NCA argued that despite Ghana's high mobile phone penetration rate, their handlers demonstrate little to no knowledge of cyber security (Field Interview, 2023). The respondent from GAF identified that the phenomenon has transcended to the younger ones. He explained that because the elderly lack such knowledge, they cannot carry out proper cyber parenting for the younger ones to imbibe a healthy cyber culture (Field Interview, 2023). Many parents in contemporary times have, therefore, introduced their children to the cyber world without corresponding tutorial on its dangers. He postulated that

> *"... how many of us [parents] take time to do digital parenting or coach our kids? We are quick to give them devices to play with so that they will not disturb us, but do we take time to find out where they go while surfing? That compromises their safety because there are lots of predators online that can easily lure them [the kids] off. So, your child who is online and you think is IT Savvy cannot analyse situations because of his/her level. He/she could hence ignorantly therefore been victimised or used as a man-in-the-middle for an attack" (Field Interview, 2023).*

The respondents again noted that the gap in cyber awareness has resulted in less appreciation of safeguarding cyberspace among cyberspace users in Ghana. A cybersecurity professional from

CSEAG, exemplifying this, recounted how an organisation's Head of Operations downplayed the relevance of securing their company's system against attacks. He is reported to have retorted that,

> *".... Excuse me! Our organisation has nothing to hide, so no one can steal information from us. There is no need for an attacker to even encrypt our files" (Field Interview, 2023).*

Recognising that cybersecurity is not just a concern for larger companies, managing critical information is crucial. The above example shows that the lack of awareness in Ghana is pervasive, even among senior institutional officials. This systemic issue directly influences organisational decisions regarding cybersecurity policies. It also highlights the widespread deficit in cyber awareness at private and corporate levels and the need for comprehensive solutions and collective action.

Regarding cybersecurity education, the respondents noted that even though cybersecurity is relatively new, its rays in the educational systems have been overly deeming. They averred that curriculums at the basic and pre-tertiary levels have not conceived of this, even if there has been any discussion about that. At the tertiary level, studying the subject matter as a course is still embryonic (Field Interview, 2023). The respondent from UPSA, in his affirmation of this reality, admitted that even as an academic, he only got introduced to cybersecurity at PhD level (Field Interview, 2023).

It is imperative to indicate that the above development is manifesting against the elaborate cyber awareness and education provisions in the 2015 National Cybersecurity Policy and Strategy. Section 3(4) of the strategy, for instance, mandates the state to promote awareness creation and online skill development among all stakeholders, including children (NSCPS, 2015, p.31). The policy document also recommends offering certification courses on information and cyber security, training law enforcement officers on cyber investigation and effective persecution of

cybercrime offences through universities and other training institutions' collaborative efforts (NSCPS, 2015, p.31). This low level of cyber education constitutes a worrisome development because it is manifesting at a time when cyber threats are rising steeply, and deficits in cybersecurity professionals are widening globally.

The forgone assertions support previous studies and conclusions, including Forson-Adaboh (2022), Agbeko (2021), Affum (2019), Adu & Adjei (2018) and Botchwey (2018), Motiwala (2017) and MFWA, (2017) that have all pointed to low levels of cyber awareness in Ghana. It also reveals that the solution to this persistent and troubling challenge needs to be more comprehensive than just the creation or institutionalisation of regulatory instruments, as suggested by Motiwala (2017). The appropriateness of designed instruments, state actors' commitment to their implementation, and the availability of resources are equally vital for attaining cyber-safety objectives.

Again, the findings reveal that while the regulatory and legal provisions could compel institutions to institute cybersecurity structures, the same process could not be used to get the cooperation of individuals. This brings to the fore the neo-institutionalist's call for deploying non-formal institutions in state governance and, by extension, cyber governance. Its application, hence, proposes the incorporation of non-formal groups and forums, such as youth groups, farmers' forums, market associations, trade unions etc., for awareness creation.

6.2.4 Cyber Security Skills Gap

The critical shortage of cybersecurity professionals in Ghana, a key challenge in cybersecurity promotion, is a grave concern. This cyber skills gap, while a global issue, is particularly acute in

Africa and Ghana. A respondent from the CSA underscored the gravity of the situation, stating that

> *"The lack of these experts in the field is a significant obstacle to Ghana's efforts to build a robust cybersecurity ecosystem. This huge skills gap within the sector is disturbing because if you don't have professionals to help you fight threats and you enact laws, you still will not be doing anything" (Field Interview, 2023).*

The high attrition of the few existing ones compounds this already dire situation of the limited cyber professionals in the country. The respondents revealed that countries, mostly in the West (Europe and America) and other international organisations, have been poaching the few cyber professionals in the country. The respondent from GTBank lamented the country's inability to retain these few critical service providers as the lowest point of the matter. He asserted that

> *"... to worsen it, a lot of them [cyber professionals] are leaving the country, and very soon, there are roles that will be very difficult to get people to fill. Qualified people to fill the roles of Chief Information Security Officers (CISO) and system auditors are all leaving. They are leaving for Canada and the US, where they are in high demand." (Field Interview, 2023).*

According to the respondents, these professionals are in high demand in those jurisdictions, and the countries and organisations needing their skills offer better working conditions to entice them.

While establishing how state and private institutions feel the brunt of the country's widening cyber skills gap, the study equally revealed an insignificant proportion of women in the field. The respondents acknowledged the ratio of men to women in the country's cyber security profession was unmatched (Field Interview, 2023). This situation found expression in the negligible number of females identified in the institutions and professional bodies engaged during the study. Thus, despite the deliberate effort by the researcher to get a significant representation of female respondents, most institutions virtually had no female staff. In the few instances where they were, their designations were the more conventional administrative duties other than the core technical services.

The above findings affirm the World Economic Forum (2024) and ISC2 2022 Cyber Security Workforce Study reports and Adomako et al.'s (2018) observations of a widening skills gap globally and confirm that Ghana is not the exception. The study's revelations also lend credence to the neo-institutionalist and structuration theorists' assumption on the significance of human agency in state management and the study of the same. Developing people is as critical as structures in countries' cybersecurity management. The revelation of the gender dimension of the skills gap and the causative factors for cyber professionals' attrition is equally informative. The sector's minister's lamentation in 2017 on the lack of cybersecurity professionals, constituting the most challenging situation for Ghana's cybersecurity promotion efforts (KAIPTC, 2017), is affirmed and persisting. Concrete efforts towards addressing these issues, whose impact has been pronounced, have been justified.

6.2.5 Limited Cyber Technology and Infrastructure

In addition to the above, the respondents also mentioned limited cyber technology and infrastructure as another challenge Ghana faces in cybersecurity promotion efforts. They contended that amid the enthusiasm and commitment to digitalising its systems across all sectors, the country also needed to ensure it secures its cybersystems. A respondent quipped thus

> *"…while our drive to digitalise is good, we should also be concerned about securing them. The energy that is channelled into the digitalisation drive should be the same in seeking to ensure that those things [infrastructure/technology] are secured" (Field Interview, 2023).*

Robust and reliable cybersecurity infrastructure and technology are required to tackle cyber threats. However, some respondents noted that this is currently lacking in the country. Expanding on this point, a respondent from Slamm Technologies pointed out that the Ghanaian government's ability to proactively manage the various sectors designated as critical infrastructure is questionable. He quizzed how the country intended to protect its data with foreigners managing the process and the logic in hosting its critical data in servers outside its jurisdiction. He concluded

that although the country may have genuine intentions to promote cyber security, it has yet to develop its capacity to match such a dream (Field Interview, 2023).

One of the major concerns is that the country relies heavily on foreign sources for all the services and products required to keep up with technological advancements. It is essential to note that aside from the security implications mentioned above, the country's lack of website content server hosting, email domain systems, data storage, and exchange domains poses a significant challenge to the country's socio-economic life. Using platforms owned by third parties raises critical concerns about the potential for the state to be grounded. This phenomenon could halt businesses and social life and severely affect critical services such as health, education, and transport. These concerns align with Adomako et al.'s (2018, p.3) and Tagert's (2010) assertions regarding the risks faced by the African continent, particularly developing African countries, as importers of cyber products, technologies, and services. Thus, it supports the caution of the Ghanaian state to be measured in its digitalisation agenda and guided by its capacity to protect the established critical services providing infrastructure.

6.2.6 Policy Implementation Challenges

The last of the concerns that featured as a challenge in Ghana's cybersecurity promotion drive is policy implementation. The respondents related that while laws are good, cyber threats are not fought on paper with intentions. The ability and commitment to translate scripted or abstract ideas into tangible projects is vital in cyber governance and cybersecurity promotion (Field Interview, 2023). They further indicated that policymakers could only consider laws and intentions good if they effectively transition into action. According to the respondents, this transition has challenged Ghanaian cyberspace managers, leading to nagging concerns in cybersecurity promotion (Field Interview, 2023).

Along the above tangent, the respondent from the Police CID quipped that the nature of cyberspace has rendered the implementation of cybercrime legal provisions challenging. He explained that cybercrimes could be committed at different locations, leaving the crime's evidence scattered across a space (region or country). The ability and capacity of countries such as Ghana to gather these pieces of evidence in record time without getting them sullied is challenging (Field Interview, 2023). According to the respondents, the differences in states' cyber regimes and provisions have made it harder to resolve cyber issues. Although international protocols and treaties on cyber security have helped with cooperation, the respondents have noticed that the differences in national laws and governance systems create challenges. In his explanation of this scenario, the respondent from the Police CID narrated that

> *"...when a prosecutor is demanding data on a case from another country to press criminal charges against someone, the likelihood of securing it is dependent on the laws and governing system of the other. It mostly becomes a tag if the laws of the country providing the data classify such a case differently. If a country classifies a case as civil, it will be reluctant to give out data for criminal prosecution on the same case against a person in another country" (Field Interview, 2023).*

Prosecutors in Ghana, hence, encounter challenges when dealing with legal cases involving neighbouring countries. These countries are technologically less advanced and have different legal systems. Because of their French colonial background, the legal systems in these countries consider a person guilty until proven innocent, while in Ghana, the accused is presumed innocent until proven guilty. The challenges from these differences have been recognised by various stakeholders, including RECs, who have variously called for harmonising the national cyber laws of their member states.

In another breath, the respondents raised the capacity of prosecutors and judges to handle cyber evidence and professionally prosecute cyber cases as a challenge in Ghanaian cybersecurity promotion. The respondents contended that the distinction between cyber and physical spaces is

not just in name but also in distinct modes of interaction. These interactive modes define the laws required to manage conduct and prosecute the same when breached. Therefore, the laws of one space are not rightly applicable in the other (Field Interview, 2023). Handling cases and interpreting laws in the space by judges, magistrates, lawyers, and prosecutors who received their training along the traditional evidence-gathering and analysis procedures has been problematic. Therefore, cyberspace issues and fledging laws appear novel and challenging for prosecutors and law enforcers in Ghana to handle them. This revelation justifies the call for joint efforts towards capacity building on law interpretation and enforcement for agencies through programs such as the Council of Europe's Project on Cybercrime and the Lisbon Network.

6.2.7 Conclusion

The chapter examined the strategies adopted by Ghana to secure its cyber environment and analysed the process of implementing these strategies. By this, the chapter has responded to the fourth objective of the study, which sought an understanding of the kind of strategy the Ghanaian state had deployed in its cybersecurity and how it could address the country's cyber threats. The chapter reveals that the Ghanaian government is determined to tackle the challenges faced by its cyber ecosystem. It also highlights that the cybersecurity strategy adopted by the country, though appropriate, is faced with several challenges in its implementation that the state needs to address.

CHAPTER SEVEN

SUMMARY OF FINDINGS, CONCLUSION AND RECOMMENDATIONS

7.0 INTRODUCTION

The main objective of this thesis was to investigate the cybersecurity strategies adopted by developing African countries, using Ghana as a case study. The study analysed Ghana's cybersecurity threats and the response strategies employed to manage them. The structuration philosophical paradigm and the neo-institutionalism theoretical lens guided the methodology and discourse of the study. The view of structural duality, which runs through both paradigms, was central to the thesis analysis.

From the broader perspective of managing the cyber ecosystem in developing African countries, the study narrowed to Ghana as a case study. It analysed how Ghana has dealt with the threats in its cyber ecosystem and assessed the effectiveness of the adopted strategy. In this light, the thesis analysed Ghana's cybersecurity landscape, including its policies and regulations, institutional frameworks, and cyber awareness among its citizens. The study used the qualitative research approach that involved interviewing individuals from among industry players, cyber policymakers, academics, organisations, and individual users of cyberspace. The gathered data and the text of the documents used, including the Ghana cybersecurity policy and strategy document, were analysed using the qualitative content analysis approach.

This chapter summarizes the study's key findings based on the above-stated objectives. It then presents the major conclusions drawn from the findings, followed by recommendations for enhancing the cybersecurity experience in Ghana. The chapter also provides the study's

contributions and suggests future policy and academic discussions on cybersecurity in Ghana and Africa.

7.1 SUMMARY OF FINDINGS

The summary of the study's findings is organised around the research objectives, which focused on four key goals. Firstly, an examination of Africa's cybersecurity threat landscape and the associated continental and regional responses. Secondly, an assessment of the specific cybersecurity threats facing Ghana as a developing African country. Thirdly, an evaluation of Ghana's response strategies to cybersecurity threats within the context of the country's cyber ecosystem. Fourthly, an analysis of the adequacy of these strategies in addressing the challenges of Ghana's cybersecurity landscape. The following synopses detail the findings related to each of these objectives.

7.1.1 The Nature of the African Cybersecurity Threat Landscape and the Continental Response Mechanisms

The African cybersecurity threat landscape has been discussed in chapters two and four. First, the study analysed the meaning of cybersecurity by juxtaposing the perspectives presented in the literature with those gathered from the field. The analysis revealed that cybersecurity is conceived differently by people, institutions, and states. While some consider it narrowly as data protection, others expand it to include securing the physical infrastructure that carries or stores the data and the users of the space. The concept is, therefore, said to revolve around three fundamental tenets: ensuring data and data systems' confidentiality, integrity, and availability. The study also established that attaining these objectives was hinged on several other factors, including the sanctity of the computing systems and the physical infrastructure that carries or stores the data. The study, therefore, conceived the concept in alignment with the expanded scope definition as

advanced by Dunn-Cavelty (2010, p.363), Von Solms and Van Niekerk (2013), and the ITU (2021), which stipulates that safety in cyberspace transcends stored data secrecy. Cybersecurity in this study thus encompasses the securing of the infrastructure and systems used for data generation, transmission, and storage chain, as well as the data and users of the space.

Based on the above-established meaning of cybersecurity, the study analysed the views on the nature of the African cybersecurity landscape using the respondents' perspectives. The results indicated that the African cybersecurity ecosystem had no distinct character from the general cybersecurity landscape. This understanding concurred with Wong's (2016, p.14) and ENISA Threat Landscape's (2021) conclusions that the cybersecurity threats manifesting in Africa were similar to those of other continents. However, a few variations in elements, such as the dominant cyber threats, cybersecurity orientation and culture, and state cyber capacities, were reported. In terms of the dominant threats, the study revealed that the continent's cyber ecosystem witnessed disruption, destruction, and exploitation threats and had cyber-organised crimes, disinformation/misinformation, cyberinfrastructure sabotage, and cyber espionage as the most dominant threats.

Against the above cyber threat portfolio, the study also revealed the efforts by Africa's continental and sub-regional bodies to manage them. These efforts comprise governance regimes and advisory institutions establishment, and building synergy and harmonisation among member states' responses. Infrastructural development is left to member states. Some of the identified collaborative regimes, institutions and norms for Africa's cyber governance, include the AU's Malabo Convention, the ECOWAS's Cyber and Data Protection Management Framework and the COMESA's Model Cybercrime Bill. The notable advisory and collaborative institutions identified also include the African Union Mechanism for Police Cooperation (AFRIPOL), the AU Cyber

Security Expert Group (AUCSEG) and African CERT (AfricaCERT). The study further revealed that the provisions of the regulatory norms were largely persuasive and suggestion-oriented rather than placing compelling or binding demands on the states to either criminalise cyber offences or establish cybersecurity infrastructure. Even though such a posture looks upsetting, African states' weak finances and technological capacities, which hinder the delivery of strict mandates, have been identified as the reason.

Amidst these efforts, the study identified several challenges that hinder their maximum impact. These include low cyber literacy, language barriers hampering collaboration, non-ownership of hosting sites, cyber technology importation, financial challenges, and infrastructural deficits. The study also established a basis for advocating concerted efforts by African states to address these challenges, as that was the key to protecting citizens and maximising the opportunities provided by cyberspace. It also highlighted the need for resource-trapped African countries to prioritise cost-effective measures in their management efforts, with targeted focus and less costly application deployment frameworks.

The findings of this study objective show that the African cyber ecosystem, save its dominant cyber threats, resource capacity, and cyberculture, is similar to other cyber ecosystems. It reveals that the continent's cyber-ecosystem threats are greatly influenced by socio-economic factors. This reality suggests that while adopting internationally standardised cybersecurity management practices remains commendable, each state requires a more tailored approach that addresses the peculiarities of its cyber ecosystem dynamics or challenges in its management processes.

7.1.2 Ghana's Cybersecurity Threat Portfolio

According to the study's findings, Ghana is faced with a variety of cybersecurity threats. These threats range from crimes facilitated by the internet, attacks on infrastructure, and data breaches, which threat actors have used in disruptive, destructive, and exploitative attacks. The study identifies the country's most dominant threats including cyber fraud, insider-related threats, social engineering, DDOS attacks, malware/ransomware attacks, data breaches, and dis/disinformation.

First, the study identifies cyber fraud as the most prevalent cybersecurity threat within the Ghanaian cyber ecosystem. Instructively, the threat was revealed as an age-long phenomenon that had lurked around for decades but just seized the virtual nature of cyberspace to assume a new and more sophisticated form. Its manifestation, though disquieting, is unsurprising. Individuals and corporate organisations have lost substantial amounts of money and valuables to the threat over the years. Such occurrence, the study establishes, has yet to show any signs of cessation, with their continual manifestations. A further disturbing observation in the study is that the actual levels of cyber fraud in the country appear underreported due to factors such as:

- reputational damage to the affected institutions or organisations,
- the cumbersome processes involved in reporting such attacks, and
- the lack of trust in the security services to respond adequately to victims reporting crime.

Another threat revealed as besetting Ghanaian cyberspace is social engineering. This threat, which uses phishing and identity theft techniques, has users and operators of financial and quasi-financial sectors as their primary prey. Fraud syndicates in Ghana's mobile money and online banking sectors are primarily conducted using these techniques. The success of the threat actors in these schemes is due to the popularity of the Momo platform against users' lack of knowledge about the

system's operation. This finding by the study aligns with Danquah and Longe's (2011, p.169) establishment of widespread deployment of social engineering for cybercrime perpetration in Ghana.

The study also identified malware and ransomware attacks as significant threats within the Ghanaian cybersecurity ecosystem. These threats that aim at compromising organisations' or individuals' computing systems to either access confidential information or encrypt them for ransom have manifested widely in Ghana. Institutions, both private and public, have been identified to have suffered this threat, with many concealing it due to reputational damage. The prevalent channels and techniques through which the threat actors deploy these threats are adware, compromised emails, pop-up SMS, and social media platforms like WhatsApp, Facebook, and voice calls. The study points to the naivety of internet users in the country as contributing to the success of most of these attacks.

The study again identified insider-related threats (IRT) as another major threat associated with Ghana's cyber ecosystem. The study reveals that this threat has witnessed a continual rise recently. Although disturbing, the findings aptly agree with the Ponemon Institute's (2022) report, which points out malicious insiders and employee negligence as the leading causes of organisations' systems and information breaches. While the threat is not identified as peculiar to a sector or field, the banking and financial sectors were pointed out as places where it appeared more prevalent. The study highlighted that the motives of these compromised insiders, whether premeditated before employment or monetary enticements during their engagement, constituted serious concerns that required urgent redress. The impact of economic factors on cybersecurity threats, as suggested by many studies on Nigeria, including Akinyetun (2021), has also been validated by the study to be true of Ghana through this threat. This relationship between property crime and

poverty/inequality, as articulated and well-established in criminology literature (Jiyong et al., 2019; Raphael & Winter-Ebmer, 2001), has thus been affirmed in this study.

The study further revealed dis/misinformation as another ingrained cybersecurity threat in Ghana's cybersecurity ecosystem. According to the study's findings, cyberspace technology and its information delivery channels have been deployed by individuals and groups as propaganda tools. It has established the manifestation of disinformation and misinformation within the Ghanaian cyber ecosystem. It cites the high mobile phone and internet connectivity levels and the appetite for social media usage among Ghanaians as contributing to the threat's flourishing. It further revealed that although this cyber threat occurs at all times, it becomes more pronounced and intense during electioneering campaigns and ethnic contestations.

Another threat revealed by the study as besetting Ghana's cyber ecosystem is data breaches. The study underscored that data breaches have become a common phenomenon in the country despite the existence of a Regulatory Authority and Act charged with data protection responsibilities. The study highlighted that private and state institutions are involved in this worrying threat trend. In addition to the conventional system weakness and compromised insiders leaking data, the study added that some of the breaches emanated from the pure ingenuity of cybercriminals.

Lastly, the study revealed distributed denial of service or denial of service as the other threats with traces within Ghana's cyber ecosystem. The DDOS/DOS, which manifests as threat actors hacking organisations' websites to restrict access to their use, also manifests in Ghana. The findings indicate that though the levels of this threat manifesting in the country could not be compared to those of Western countries, it still poses a significant concern to the country's cyber ecosystem. The

debilitating effect of its manifestation on the services of ECG systems in 2022 buttresses the concern.

From the above-identified threats of the Ghanaian cyber-ecosystem, the study has established that domestic or human factors rather than just cyber-technology systems failure, contribute to Ghana's proliferation of cybersecurity threats. This situation leads to the utility of Anthony Gidden's "duality of structures" and neo-institutionalist framework. It also establishes that socio-economic elements impact Ghana's cyber threat landscape. In other words, economic inducement plays a critical role in cyber threat actors' activities in Ghana. This highlights the crucial role that human security concerns play in addressing the cyber threats faced by Ghana.

7.1.3 The Ghanaian State's Response to Addressing Its Cybersecurity Threats/Challenges

In response to this objective, the study delved first into identifying the duty bearers in cybersecurity threat management. The findings showed that the responsibility was not reserved for one person or individual but shared among industry players, individuals, CSOs, and the state. However, the study underscored that the state's pivotal role as the custodian and guardian of the peoples' rights, charges it to ensuring the sanctity of the space.

The study identified that the state is mandated to perform several direct and indirect tasks to promote cyber safety. Among the direct roles identified are the design and implementation of cybersecurity frameworks, strategies, and legal and regulatory institutions. It also plays the hybrid or indirect roles of collaborating with the private sector and industry players in intelligence gathering and policing, cybersecurity awareness creation, and education.

The above observations demonstrate that the Ghanaian state has a central responsibility in promoting the robustness of its cybersecurity ecosystem. The study further revealed the proactive measures undertaken by the state, such as the drafting of a cybersecurity management strategy and regulatory mechanisms/instruments, further highlighting its commitment to this crucial task.

Regarding drafting a cybersecurity strategy, the study identified that the Ghanaian state has a National Cyber Security Policy and Strategy in place, drafted in 2015 to guide its cyberspace management. This strategic policy strategy, which was set to provide cyber policy directions and implementation strategies for the state, had a five-year (2016 to 2020) implementation period. With this set objective, the provisions of the strategy outlined the vision, mission, and strategies for their realisation. The study also revealed that upon the expiration of the current policy strategy document, efforts towards drafting and adopting a new one had commenced, and the draft was under Cabinet consideration during this study. The study further revealed the passage of an elaborate cybersecurity legal and regulatory instrument named Act 1038. The Act, also known as the Cyber Security Act, was launched in 2020 as the legal instrument for the governance of the state's cyberspace. With its provisions spanning roles and responsibilities of the state and other stakeholders, clarification on criminality in the space and the penalties thereof, and the operational framework of the cyber regulatory body, the Act had assumed the status of a guiding reference.

The study again identified steps the Ghanaian state took to institutionalise a cybersecurity regulatory body. This body called the Cyber Security Authority, is mandated to regulate and offer advice and direction on all cybersecurity-related activities in the country. The study revealed that the authority comprises the various stakeholders, agencies, and ministries involved in cybersecurity or defence management. The study showed that the state's adoption of this approach is the conviction in its appropriateness for effectively tackling nagging issues in the state's

cyberspace. This step also constituted an acceptance of the justification for such an approach by international institutions and scholars, including the ITU (2021), Bada et al. (2018; 2019), and Turianskyi (2020), which is justified to provide grounds for building synergy of the various stakeholders' energies for effective redress of threats.

The study also confirms the state's classification of some sectors as critical and the designation of their computing systems as critical information infrastructure. National and sectoral Computer Emergency Response Teams have since been designated to manage cybersecurity incidents within those sectors. While these CERTS were expected to be functional, the study revealed that only those of the banking, finance, telecommunication, and security service sectors and the GH-CERT were operational. These efforts signified the country's conviction in a decentralised but tailored approach to cybersecurity management, which is argued to be appropriate for cyber-infant countries' cybersecurity management.

According to the study, the Ghanaian government has taken steps towards licensing cybersecurity professionals and organisations operating in cyberspace. This exercise aims to create a database of practitioners in the field and uphold standards through effective monitoring. While the policy measures appear well-intentioned, the concern that it might force many service providers and professionals out of business and allow those with close ties to political power holders to dominate the space has been expressed.

Regarding collaborative efforts on cyberspace management, the study revealed that Ghana had engaged in international collaborations, which resulted in ratifying some international cybersecurity treaties and protocols. The study indicated that Ghana had signed all the international cybersecurity treaties it is qualified to join and has demonstrated commitment to collaboration and

joint management tasks. Among the international treaties and conventions ratified by the state are the Budapest Convention (first and second pacts), the Malabo Convention and the ECOWAS Protocol on Cybercrime. The provisions of these instruments have obligated the country and rendered it eligible for collaboration and support from other state parties. The study traces the state's commitment to these cooperative efforts to the deficiencies associated with a state unilaterally dealing with borderless cyber threats. The Ghanaian state has also cooperated with the European Union and other states to promote awareness and capacity building.

The study revealed that collaborations are not exclusive to the international arena. Several such efforts have unfolded among state institutions, private sector industry players, and CSOs. The collaboration is warranted due to the significant ownership and control of skilled cyber professionals and cyberinfrastructure by the private sector in the country. This expertise and resources play a crucial role in enhancing overall cybersecurity efforts. Therefore, these non-state domestic actors have greatly supported the state in service provision and policy designs.

Finally, the study revealed that the state had also made conscious efforts to enhance citizens' cybersecurity knowledge through awareness creation and education. This phenomenon has been acknowledged in the National Cyber Security Policy and Strategy and Act 1038. Efforts, including an annual cyber-month celebration, have been instituted for this cause. Other efforts and programs, such as a cyber-security inter-school competition, have also been initiated.

7.1.4 The Adequacy and Efficiency of Ghana's Cybersecurity Strategy

The study's findings have revealed that the Ghanaian state has demonstrated an admirable commitment to addressing its cybersecurity threat challenges. It has successfully incorporated and implemented several internationally recommended policies, programs, and infrastructural

improvements to enhance its cybersecurity robustness. Such initiatives as the 2015 National Cybersecurity Strategy, National Cybersecurity Legislation, and the National Cyber Security Authority have significantly bolstered the country's cybersecurity framework, earning Ghana commendations in the ITU's 2022 cybersecurity performance rankings and many others.

Regarding infrastructure, the state has also designated some sectors as critical information infrastructures and established national and sectoral CERTs for them. It has established collaborative arrangements with international and local organisations and institutions to design and develop cyberinfrastructure, policy, and management systems. The country has also signed onto the major international cybersecurity protocols, such as the Budapest and Malabo Conventions, and committed to creating a hygienic cyberspace through citizens' awareness and education. The state's response has involved a multi-stakeholder approach with all the major cybersecurity stakeholders in its management response.

Indeed, the country's cybersecurity management efforts have been identified as conforming to international standards in cybersecurity management. These efforts have reflected in the country's sterling performance, as reported in the ITU's 2022 cybersecurity performance rankings and many others. Its adoption of the multi-stakeholder and cyber-threat-tailored management approaches has also been commended as a fitting practice for developing cyber-infant states of its status.

Amid these commendations and positive compliments, the study has identified inadequacies and challenges with some provisions, approaches, and programs of the country's cybersecurity strategy. A significant observation in this regard concerns the class of the stakeholders and the focus of the management approach. In cognisance of neo-institutionalism's assumption, which underpinned this study, a better appreciation of society comes by considering both the formal and

informal structures within it. In other words, a society is defined not only by formal structures but also by informal ones. To this end, the state's cyber governance or management strategy must consider formal and informal approaches in its cybersecurity promotion agenda. This is more so because most of the businesses and people in Ghana are within the informal sector. Such understanding, however, is not reflected in the strategy, as many of the provisions in the strategic document are formal-oriented processes targeting formal institutional and infrastructural development and functioning.

Another concern the country's adopted cybersecurity management strategy raises is the implementation process, particularly awareness creation programs. As established earlier, although the strategy recognised the need for cyber awareness raising and acknowledged that safety promotion would only be successful with informed users, periodic approaches, such as Cybersecurity Awareness Month, needed to be revised. The findings, hence, strongly advocate for continuous engagements, sensitisation and education. The urgency of this position is underscored by the continual manifestation of cyber threats. Given the varied nature of the space users, adopting a single-stream format of sensitisation and awareness creation is undoubtedly problematic. A multi-varied activities approach involving diverse stakeholders and users of the space is not just a suggestion but a necessity.

Again, the study revealed that despite the existence of a well-crafted strategy, which has earned the country commendations, some serious issues that could become obstacles to the realisation of the intended objectives of the strategy have yet to be effectively addressed. One such issue is the existing socio-cultural norms regarding anti-cybersecurity in Ghanaian society. These cultural norms, including gullibility in information sharing, the lack of security consciousness, and aversion to crime reporting, have not been addressed. Admittedly, even though the approach

towards addressing them may have been subsumed under awareness creation, the robustness of the processes required for cyber acculturation would require that the strategy itemises it and provide a detailed approach for its realisation. This is a critical issue that demands immediate attention and action, underlining the gravity of the situation.

The study also revealed the country's strategy as witnessing shortfalls or requiring improvement in bridging cyber skills and cybersecurity infrastructural gaps. Despite acknowledging both gaps and conveying the same in the strategy, the country has witnessed a continuous widening. This has primarily been attributed to the slow pace of introducing cybersecurity studies into education curricula, especially by the country's universities. Cyberinfrastructure has also reported a gap, which has yet to witness matching levels with the state's digitalisation pace. The provisions on the state's obligation are also less compelling as they are more suggestive.

In sum, the study's findings indicate that Ghana has an auspicious cybersecurity strategy to manage its challenges in cyberspace. The cybersecurity strategy satisfies most international standards, as provided by international organisations and cyber elite countries. However, it falls short in some provisions and implementation processes. Therefore, to realise the envisioned objective of the country's cybersecurity strategy, there must be a conscious effort to strengthen the various requirements and address the implementation challenges.

7.2 CONCLUSION

The principal question that preoccupied this study was; to what extent does Ghana's cybersecurity response strategy address its cybersecurity threat challenges? The question was addressed through an examination of the state's cybersecurity policy and strategy and its implementation mechanisms in the face of the country's prevailing cybersecurity threats. The cybersecurity and policy strategy

document was synthesised and compared with qualitative data collected from field interviews with cybersecurity stakeholders, national and private industry representatives, civil society organisations, and private users of cyberspace. The understandings from the data set were juxtaposed with general best practices and international cybersecurity management standards and discussed within the framework of the neo-institutionalism theory. Fitting institutional arrangements that involve structures, norms, and laws as posited by the neo-institutional theory as prerequisites for state governance, and a medium for understanding and resolving conflicting interests more cordially guided the discourse. The structuration paradigm served as the philosophical framework for data analysis.

The interviews and documents analysed revealed that the African cyber ecosystems, and by extension Ghana's, shared many commonalities with the broader cyber landscape. These revelations indicate that the cyber threats experienced by African states, including Ghana, were not too distinct from other states. It added, however, that the manifestation of cybercrimes and critical roles by domestic environmental factors (economic insecurity, finance and infrastructural deficits) in African cybersecurity threats manifestation gives its cyber ecosystem some variation. Concerning the continent's cybersecurity threats management mechanism, the study revealed key efforts in cooperation through legal treaties and protocols such as the AU Protocol on data protection and the ECOWAS Critical Infrastructure Protection Policy. While these measures align with internationally recognised cybersecurity threat management practices, the study highlighted the necessity of balancing them in a way that effectively incorporates the domestic factors contributing to cybersecurity threats.

In the case of Ghana's cyber ecosystem, the study revealed that, like the general African cyberspace, the differentiating character that marks it out from others is its dominant threats. The

study identified the country's primary cybersecurity threats as cyber fraud, DDoS attacks, insider threats, social engineering, malware and ransomware, disinformation and misinformation, and data breaches. Threat actors have deployed these threats to perpetrate disruption, destruction, or exploitation attacks. The study established a continuous increase in the number of these threats, with monetary incentives being a major motive behind this trend. In other words, human security needs or human insecurity elements feature as major drivers of the Ghanaian cyber threats manifestation, thereby, affirming Madrid-Morales et al.'s (2020), and Baylon and Antwi-Boasiako's (2016) earlier assertions. The study concludes that threats to the Ghanaian cyber-ecosystem arise from both cyber technology and domestic socio-cultural factors.

In response to the various threats facing Ghana, the study outlines the state's efforts to address these challenges. This commitment has resulted in a national cybersecurity policy and strategy drafting and implementation. A National Cyber Security Act and a National Cybersecurity Authority, subsequently birthed by these initiatives, now serve as the regulatory regime and authority, respectively. The study also revealed that the legislative and regulatory instruments and how they define the roles of the state and other stakeholders, align with international standards. Its provision in favour of a multi-stakeholder approach is also identified as being consistent with international cybersecurity governance standards suggested by cyber-elite countries and international cybersecurity organisations, such as ITU and NIST.

In terms of implementation, the study again revealed that the cybersecurity strategy and the Cybersecurity Act provisions on domestic and international collaborative efforts have been realised. Ghana has engaged in collaborations, internationally with the ITU, AU, and other ECOWAS member states. Locally, collaboration among state agencies, industry players, and CSOs has also been undertaken to promote infrastructure and cyber awareness. It is, therefore,

evident from the above that the Ghanaian state has waded vigorously into building synergy and exploiting the energies of the various stakeholders for the promotion of the sanctity of its cyber ecosystem.

The above observations indicate that the Ghanaian state's relentless efforts toward attaining a robust cybersecurity ecosystem align with the standardised provisions set out by cyberelite countries and international cybersecurity institutions such as the ITU and NIST. While it is admissible that cybersecurity threats cannot be entirely eradicated, effective strategies for their management should result in a reduction of their occurrence. Achieving a secure cyberspace remains an unrealised goal in Ghana, where cyber threats continue to rise and inflict significant damage. The study revealed unaddressed factors in the country's response strategy that has contributed to this phenomenon. In other words, the study identified some challenges that characterise the Ghanain cybersecurity response strategy.

This study concludes that both domestic and international factors, along with technological and socio-economic elements, influence the manifestation of cybersecurity threats. Therefore, it is essential to incorporate these elements into the cybersecurity management strategies of states. Additionally, it established that domestically, the critical elements required in cybersecurity management were not exclusive to formal structures but informal norms and rules that address pertinent cyber threat causative elements. These understandings also indicate that the state's cybersecurity strategy needs to incorporate those informal processes and norms, which are missing in the current strategy. To this end, the study concludes that Ghana's cybersecurity response strategies have an elaborate formal management mechanism largely based on indicators by ICI and cyber-advanced countries but offer little consideration of the informal norms or domestic environmental factors.

On the issue of domestic factors stifling the efficiency of the state in cybersecurity promotion, the study identified anti-cybersecurity social/cultural norms, citizens' gullibility in divulging information, the lack of security consciousness, and the aversion to reporting crime. Others, including funding, a cyber-skills gap, a lack of awareness, insufficient cybersecurity infrastructure, and a general policy implementation gap, have equally been highlighted. For the state to witness meaningful progress in its cybersecurity ecosystem management, these identified cultural orientations and other cybersecurity implementation challenges must be addressed.

In sum, the study underscores that while there is a growing acknowledgement that global harmonisation and cooperation are essential to tackle transnational cybercrime (Broadhurst, 2006) effectively, there is equally a compelling need for countries to ensure that their cybercrime legislations are responsive to their specific realities and needs. This is particularly so for developing countries, whose existing challenges and circumstances are not the basis for the Global North provisions of existing international instruments such as the Budapest Convention (International Telecommunication Union, 2012). A "glocal approach", which argues for countries' adoption of initiatives that balance global standards with local/domestic realities and circumstances, as noted in Chang (2012), is worth considering. The approach addresses the above phenomenon to the extent that it recognises the need for countries to adopt a tailored approach to cybercrime legislation that incorporates their specific needs and global realities and standards. By this, countries can attain effective, relevant, and responsive legislation to the challenges posed by cybercrime.

From the above, it is right to conclude that the Ghanaian cybersecurity strategy is driven by international standardisation rather than its domestic disposition. The study has established that while the state is justified in taking inspiration from international cybersecurity benchmarks and

standards for its cybersecurity management response, critical attention to its particular disposition and domestic environmental factors i.e. dominant threats, resource challenges, and status as a cyber-infant country, should have been observed. The study has indicated that while the state's efforts have undeniably created a formidable base for realising a robust cyber ecosystem, much improvement is still required. It concludes that although the general focus of Ghana's cybersecurity is appropriate for a cybersecurity response of a cyber infant country of its stature, there is a need to address its implementation challenges and realign its provisions to respond to the prevailing domestic environmental threat influencing factors. Addressing these through the *"glocal approach"* remains central if the country is to experience a more hygienic and robust cyber ecosystem.

7.3 RECOMMENDATIONS

The findings and conclusions of the study have influenced several recommendations. The findings and conclusions, as advanced above, indicate that cybersecurity remains a primary concern in developing African states and Ghana at the sub-national level. Response mechanisms at the regional and state levels also exist in legislative and regulatory structures. However, some gaps and inadequacies in the provisions and implementation challenges have been identified as besetting the state's strategy. The recommendations are directed at African states and their regional organisations, the Ghanaian government or policymakers, civil society organisations (CSOs), donor partners, and academia.

7.3.1 African States and Regional Organisations

1. Based on cyberspace's indispensable nature in state management and its susceptibility to threats, the study recommends incorporating cybersecurity and digital resilience into African

states' developmental agendas. The states must harness the opportunities offered by cyber technology through increased investments in its various sectors.

2. Again, given the common feature of African countries as cyber technology importers and the peculiarities of their cybersecurity landscapes, the study recommends collaborative investment projects by African states to develop cybersecurity frameworks and infrastructures that fit their ecosystem.
3. Furthermore, the African regional organisations and their member states must also rise above regulatory guidelines provisions and embrace the provision of intercontinental cyber security management infrastructure. Such infrastructure which would be seen as owned by all partners, will strengthen their collaboration towards managing the ecosystem.

7.3.2 Ghanaian State

1. There is a need for a revision of the National Cybersecurity Policy and Strategy and its resultant Cyber Security Act, Act 1038 provisions. These revisions are required to reflect the local context-specific issues that feed into the country's cybersecurity threats. Central in this respect are provisions addressing the human insecurity needs such as unemployment in the country.

2. The Ghanaian state needs an elaborate policy on cyber-awareness creation among citizens. This policy must focus on re-culturing citizens towards hygienic cyberspace lifestyles. Thus, even though the existence of systems and laws is essential, using human beings as a defence mechanism has proved to be more effective in cybersecurity promotion. And given the pervasive anti-cybersecurity socio-cultural norms in Ghana, policymakers must deliberately drive an agenda targeted at re-culturing citizens for the cyber world.

3. There should be a revision of the cyber awareness creation approach. Ghana's cyber awareness creation programs should be continuous and more targeted. Thus, the institutionalized Cybersecurity Month celebration, which features many awareness creation and cyber hygiene lifestyle, although good is long spaced. A continuous cyber awareness program that adopts varied avenues and strategies should be adopted to curb cyber threats which in itself occur unceasingly. The campaigns which are mostly in English and text form should be revised to include visual and audiovisual content in local languages.

4. The institutional partnership should be encouraged and harnessed. The state should continue to deepen its multi-stakeholder approach in both policymaking and implementation. On the implementation of cyber awareness creation, for instance, highly patronized institutions of the state, such as DVLA, hospitals, airports, and ministries, should be incorporated and their premises and platforms used as mediums to create cyber hygiene practices awareness. Informal and social groups and associations, such as youth and women groups, trade union groups, etc., should also be engaged and equipped to sensitize their members on cybersecurity.

5. The study recommends deliberate steps by the state towards the inclusion of cybersecurity studies into the curriculums of schools from the basic levels and the running of courses on cybersecurity by tertiary institutions. The Education Ministry, the Ghana Education Service, and tertiary institutions should, therefore, restructure their educational curriculums and course structures to incorporate the teaching and learning of cybersecurity. This has become necessary because children's exposure to cybersecurity knowledge in schools amounts to a prudent way of enhancing child online protection and minimizing their

vulnerabilities to cyber criminals. The incorporation of the subject matter into university courses of study would create both awareness and train professionals to reduce, and bridge the widening cyber-skills gap.

6. Given the underrepresentation of women in the cybersecurity profession in Ghana, the study recommends that the state utilize opportunities, such as the ITU initiative "Her CyberTracks", which offers free training for women from developing and middle-income countries. This will significantly enhance women's cybersecurity skills and grant them equal, full, and meaningful representation in the cybersecurity industry, contributing to the total cyber resilience of the country.

7. The study further recommends that state institutions, especially the CSA, should ensure the effective implementation of cybersecurity regulation provisions provided in the regulatory policies. The application of the rule and bringing offenders to book will deter other likely offenders. For instance, in data breaches and accountability mechanisms, the Data Protection Agency should be seen prosecuting offenders and making those cases come to public notice. The CSA must also hasten the processes of the passage of the legislative instrument (LI) on Act 1038 to give legal effect to detailed processes on its implementation.

8. The state must continue to show more commitment to providing more resources towards the improvement of cyberinfrastructure and strengthen its private sector partnership. A deliberate state policy should be pursued to promote collaboration with non-state entities in investing in domestic cybersecurity research to develop homegrown solutions.

7.3.3 Civil Society Organisations

1. CSOs should refrain from reneging their role as watchdogs and agenda setters on cybersecurity-related matters. They should continue to draw the state and other relevant stakeholders' attention to their responsibilities in cybersecurity promotion. They should continue to advocate for citizens' rights in terms of access and protection of their data.

2. The CSOs should continue to partner with the state in its cybersecurity promotion by using their platforms to create cybersecurity threat awareness among the citizenry. The organisations should also continue to counsel and offer policy recommendations to state agencies and policymakers on best cybersecurity practices. Such counsel should focus on the ultimate welfare of the citizenry rather than the organisations' parochial interests.

7.3.4 Donor Partners

1. Donor partners should continue to support the country in its cybersecurity management efforts through funding and technical advice. Supporting state and non-state agencies with funding for cybersecurity research to build homegrown solutions and capacity building is required.
2. Donor partners should also prioritise the peculiar situation of the state in their support scheme designs. Donor-sponsored cybersecurity programs and projects should be well coordinated to eliminate conflicts and redundancies.

7.3.5 Academia

The impact of academic writings on the transformation of societies has been reve. Academics and philosophers influenced their society's paths through their logical arguments and empirical justifications. In this respect and based on the findings, the study recommends more scholarly

enquiry into cybersecurity in Africa and Ghana specifically. Scholarly assessments on the contributions, impact, challenges, and proper management processes of the Ghanaian cyberspace should concern scholars. Such critical scholarly engagements, in partnership with industry players and donor agencies, will help the understanding of the country's cyber ecosystem to influence the design of domestic response schemes to harness the opportunities offered by cyberspace.

A major focus in academia should be given to research partnerships with industry players and donor agencies on cybersecurity to help understand and develop local response schemes to the state's cybersecurity challenges.

7.3.5.1 Future Research Agenda

The study's findings indicate a call for further research on Ghana's cybersecurity industry. Quantitative studies into the levels of cybersecurity awareness in Ghana and how to address the anti-cybersecurity socio-cultural issue in the country need more interrogation. The philosophical underpinnings of Ghana's cybersecurity strategy and cyber-parenting also require further reflection.

7.4 THE CONTRIBUTIONS OF THE STUDY

Based on the foregoing discussions, the study highlights the following five lessons, which have implications for our theoretical, empirical and comparative understanding of cybersecurity in general and the Ghanaian cybersecurity experience in particular.

7.4.1 Contribution to knowledge

The study has clarified that the existence of rules and regulations governing the conduct of persons, institutions and states in cyberspace is a necessary but not a sufficient element for states' cybersecurity robustness. Thus, cyber-security promotion does not thrive exclusively on the

existence of laws. Such provisions must have accompanying infrastructure and effective implementation of its provisions and other acceptable norms.

7.4.2 Funding

Money plays a central role in determining the robustness and security of the cybersecurity ecosystem of states. In this vain, the cybersecurity of Ghana has not matched the country's digitalization drive because of the state's lack of resources for adequate investment for a resilient cybersecurity ecosystem. The study underscores that such development has consequently resulted in the state's reliance on donor partners and prioritizing investors' interest over the country's own in its cyber policymaking and implementation processes.

7.4.3 Building synergy

The impact of collaboration on promoting cybersecurity is palpable. The study has elaborated on the justification for collaboration in cybersecurity management, especially for developing African countries, such as Ghana. By this, the study has contributed to an understanding of extending the established order of collaboration in addressing domestic and international issues in a liberal international system, into the cyber security domain.

7.4.4 Theoretical Contribution

Theoretically, the study deployed the Neo-institutionalism theory, whose central tenet places significance on formal and informal institutions. By this association, the study offered an opportunity to apply the theory's framework for an assessment. The study's identification of both formal and informal institutions as relevant in understanding and addressing the challenges of the country's cybersecurity management approach validates the theory's central tenets. In this regard,

the study has affirmed the applicability of neo-institutionalism in examining state management in general and cybersecurity in particular.

7.4.5 Methodological Contribution

Broadly, the study has contributed to the methodological approaches in international relations studies. This conclusion stems from the fact that the issue of cybersecurity concerns the broader field of International Security. The various threats of cyberspace fundamentally constitute a threat to states' sovereignty, and their borderless nature presents them as issues of international concern. How to address them, therefore, constitutes an IR question. Again, international collaboration through international and bilateral cooperation, which is required to address such threats, is central to international security and politics. The study also demonstrates the roles of domestic factors in states' cybersecurity threats manifestation. To gain a comprehensive understanding of a state's cyber ecosystem, the study has demonstrated the feasibility of balancing local and International response mechanisms termed "glocal".

BIBLIOGRAPHY

BOOKS

Berg, B. L. (2001). *Qualitative research methods for the social sciences.* Allyn & Bacon.

Bernard, H.R. 2002. *Research Methods in Anthropology: Qualitative and quantitative methods*. 3rd edition. AltaMira Press,Walnut Creek, California.

Betz D.J. & Stevens T. (2011). *Cyberspace and the State: Towards a Strategy for Cyber-power*. Routledge.

Biggam, J. (2012). Succeeding with your Master's Dissertation: A step-by-step handbook, 116.

Buchan, R. (2018). *Cyber espionage and international law*. Bloomsbury Publishing.

Centre for Cyber Security (June, 2021). *Threat Assessment: The threat of destructive cyberattacks*. First edition. www.cfcs.dk/globalassets/cfcs/dokumenter/trusselsvurderinger/en/

Chang, L. Y. (2012). *Cybercrime in the Greater China Region: Regulatory Responses and Crime Prevention across the Taiwan Strait*. Cheltenham: Edward Elgar Publishing.

Colarik, A. M. (2006). *Cyber terrorism: Political and Economic Implications*. Idea group Publishing Global. London

Collis, J. & Hussey, R. (2003), *Business Research: A Practical Guide for Undergraduate and Postgraduate Students,* Palgrave Macmillan, Houndmills

Creswell, J. W. (1998). *Qualitative inquiry and research design: Choosing among five traditions.* Sage Publications, Inc.

Creswell, J. W. (2003). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. (2nd Edition). Sage Publication, Inc.

Creswell, J. W. (2013). *Qualitative inquiry and research design. Choosing among five approaches* (3rd Ed.). London: Sage Publications.

Creswell, J. W. (2014). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. (4th ed.). London, UK: SAGE Publications, Inc. https://doi.org/10.1007/s13398-014-0173-7.2

Dawson, M. E., Jr. (2021). *Cyber warfare: Threats and opportunities*. Academic Press.

De Vaus, D. A., & de Vaus, D. (2001). Research Design in Social Research. Sage.

Dunn-Cavelty, M. (2010). Cyber-Security *In The Routledge Handbook of New Security Studies* 1st Edition. Routledge

Edgar, T. W., & Manz, D. O. (2017). *Research Methods for Cyber Security*. Syngress, ISBN 978-0-12-805349-2

Fridlund, B., & Hildingh, C. (2000). *Qualitative research methods in the service of health.* Studentlitteratur.

Gettinger, D. (2020). *The drone databook*. Center for the Study of the Drone. CSD-Drone-Databook-Web.pdf (bard.edu)

Giddens, A. (1979). *Central problems in social theory: Action, structure, and contradiction in social analysis* (Vol. 241). University of California Press.

Giddens, A. (1993). *New rules of sociological method*. Stanford University Press.

Graham, J., Olson, R., & Howard, R. (Eds.), (2016). *Cyber security essentials*. CRC Press, Francis &Taylor Group.

Harrison, L., & Startin, N. (2001). *Political research: An introduction*. 1st Edition. Routledge, London. https://doi.org/10.4324/9780203465370

Hughes, John A. & W. W. Sharrock, (2007). *Theory and Methods in Sociology: An Introduction to Sociological Thinking and Practice*. Basingstoke: Palgrave Macmillan ISBN 0333772865, 9780333772867

Karake-Shalhoub, Z., & Al Qasimi, L. (2010). *Cyber law and cyber security in developing and emerging economies*. Edward Elgar Publishing.

Katzenstein, P. J. (Ed.). (1996). *The culture of national security: Norms and identity in world politics*. Columbia University Press.

Kolodziej, E. A. (2005). *Security and International Relations* (Vol. 10). Cambridge: Cambridge University Press.

Kothari, C. R. (2004). *Research Methodology: Methods & Techniques*. New Age International (P) Ltd. https://doi.org/10.1017/CBO9781107415324.004

Krippendorff, K. (2004). *Content Analysis: An Introduction to its Methodology* (2nd Edition) Thousand Oaks. CA. Sage publications.

Layder, D. (2006). *Understanding social theory*. 2nd Edition Sage Publications 1-336.

Leedy, P. and Ormrod, J. (2001) *Practical Research: Planning and Design*. 7th Edition, Merrill Prentice Hall and SAGE Publications, Upper Saddle River, NJ and Thousand Oaks, CA.

Libicki, M. C. (2021). *Cyberspace in peace and war*. Second Edition, Naval Institute Press. ISBN 1682476170, 9781682476178

Lincoln, V., & Guba, E. (1985). *Naturalistic Inquiry*. Sage Publications Inc. London

Mack, N., Woodsong, C., MacQueen, M. K., Guest, G., & Namey, E. (2005). *Qualitative Research Methods: A Data Collector's Field Guide*. Family Health International. Retrieved from https://www.urbanreproductivehealth.org/sites/mle/files/datacollectorguideenrh.pdf

March, J. & Olsen, J. (1989). *Rediscovering Institutions: The Organisational Basis of Politics,* New York: Macmillan Publishers,

May, T. (2011). *Social Research: Issues, Methods and Process*. 4th Edition. McGrawHill Open University Press.

Mouzelis, N. (2003). *Sociological theory: what went wrong?: diagnosis and remedies*. Routledge London. https://doi.org/10.4324/9780203417591

Muller, L. P. (2015). *Cyber Security Capacity Building in Developing Countries*. Norwegian Institute of International Affairs (NUPI). http://www.jstor.org/stable/resrep07959

NCSG (National Cybersecurity Strategy Guide) (2021) *Guide to Developing a National Cybersecurity Strategy* 2nd Edition 2021-ncs-guide.pdf (un.org)

Neuendorf, K. A. (2017). *The content analysis guidebook.* 2nd edition. Sage Publication. Los Angeles (USA)

North, D. C. (1990). *Institutions and Institutional Change and Economic Performance*. Cambridge: Cambridge University Press,

Osula, A. M., & Rõigas, H. (Eds.). (2016*). International cyber norms: Legal, policy & industry perspectives.* NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/uploads/2018/10/InternationalCyberNorms_Appendix1.pdf

Patton, M. Q. (2002). *Qualitative research and evaluation methods*. 3rd Edition. London UK: Sage Publications

Peters, B. G. (2019). *Institutional theory in political science: The new institutionalism.* 4th Edition. Edward Elgar Publishing.

Peters, G. (2000) *Institutional theory, problem and prospects.* Vienna: institute of Advance Studies, https://nbn-resolving.org/urn:nbn:de:0168-ssoar-246573

Peters, G. (2005) *Institutional theory in political science: the new institutionalism,* 2nd edition, London: Bloomsbury Academic.

Ruane, J. (2005). *Essentials of Research Methods: A guide to Social Science Research.* Wiley https://books.google.com.gh/books?id=Hk2tF3TH_NUC

Scott, R. (2006). *Institutional theory: contributing to a theoretical research programme*. Oxford: Oxford University Press, p.2.

Shank, G. D. (2002). *Qualitative Research: A Personal Skills Approach.* Upper Saddle, New Jersey Columbus, Ohio: Merrill Prentice Hall. Retrieved from http://www2.clarku.edu/~mbamberg/class material/107/Qualitative Research, A personal sills Approach.pdf

Singh, Y. k. (2006). *Fundamental of Research Methodology and Statistics*. New Delhi: New Age International Publishers.URL: Fundamental of Research Methodology and Statistics (mkcl.org)

Stoessinger, J.G. (1993). *The Might of Nations. World Politics in Our Time.* 10th Edition. McGraw-Hill, SBN 0070616256, 9780070616257

Strauss, A. L., & Corbin, J. M. (1998). *Basics of qualitative research : techniques and procedures for developing grounded theory.* Sage Publications. Thousand Oaks, California

Tagert, A. C. (2010). *Cybersecurity challenges in developing nations* (Doctoral dissertation, Carnegie Mellon University), Pittsburgh, Pennsylvania, USA.

van der Meulen, N., Jo, E.A. & Soesanto, S., (2015). *Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses,* EPRS: European Parliamentary Research Service. Belgium. Retrieved from https://policycommons.net/artifacts/1335785/cybersecurity-in-the-european-union-and-beyond/1942499/ on 24 Mar 2023. CID: 20.500.12592/c5rvnq.

Wiener, N. (1948). *Cybernetics: Control and Communication in the Animal and the Machine* (2nd Edition), Cambridge, Massachusetss: The M.I.T Press.

Wong, A. (2016). *Cybersecurity: Threats, Challenges, Opportunities*. *ACS, Nov.*

Yin, R. K. (2018). *Case study research and applications* (Vol. 6). Thousand Oaks, CA: Sage.

Yin, R. (2003), *Case Study Research: Design and Methods*, Sage Publications, Thousand Oaks, CA.

BOOK CHAPTERS

Adler, E. (2013). Constructivism in international relations: Sources, contributions, and debates. *Handbook of international relations*, 2, 112-144.

Antunes, S. & Camisao, I. (2017) 'Realism', in Mcglinchey, S., Walters, R. and Scheinpflug, C. (eds) *International Relations Theory*. Briston: E-IR Foundations.

Arsneault, S., Northrop, A., and Kraemer, K. L. (2005). "Taking Advantage of the Information Age: Which Countries Benefit?" in *Handbook of Public Information Systems* G. D. Garson (ed.) (Second Edi.), Singapore: Taylor & Francis Ltd.

Baldwin, P. (1997). The past rise of social security: historical trends and patterns. In *Reforming the welfare state* (pp. 3-24). Berlin, Heidelberg: Springer Berlin Heidelberg.

Baylis, J. (2008). The Concept of Security in International Relations. In: *Globalization and Environmental Challenges. Hexagon Series on Human and Environmental Security and Peace*, vol. 3. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-75977-5_37

Bennett, A. and Elman, C. (2010) Case Study Methods. In C. Reus-Smit and D. Snidal (eds) *The Oxford Handbook of International Relations.* Oxford University Press: Oxford. Ch. 29.

Burchill, S., & Linklater, A. (2005). Introduction. In S. Burchill, A. Linklater, R. Devetak, J. Donnelly, M. Paterson, C. Reus-Smith & J. True (Eds.), *Theories of international relations* (3rd ed., pp. x, 310 p.). Basingstoke: Palgrave Macmillan

Calandro, E., Chavula, J., & Phokeer, A. (2019). Internet development in Africa: a content use, hosting and distribution perspective. In *e-Infrastructure and e-Services for Developing Countries: 10th EAI International Conference, AFRICOMM 2018, Dakar, Senegal, November 29-30, 2019, Proceedings 10* (pp. 131-141). Springer International Publishing.

Casson, M.C., Marina D.G, & Uma S. K. (2010). "Formal and Informal Institutions and Development." *World Development* 38 (2): 137–41.

de Guzman N. (2014), Internet Governance: Views from the Internet Society in Cheong, D.D. (ed) *Cybersecurity Some Critical Insights and Perspectives* 72-77 S. Rajaratnam School of International Studies, Nanyang Technological University

Dewey, G. (1996). Political institutionalism; legal perspective. In R. E. Goodwin and H. D. Klingeman (Eds.), *A handbook of political science*, Oxford: Oxford University Press, pp. 191-204.

Giddens, A. (2004). The constitution of society: Outline of the theory of structuration: Elements of the theory of structuration. In *Practicing History* (pp. 121-142). Routledge.

Guba, E. G., (1990). The Alternative Paradigm Dialog in E.G., Guba (ed.) *The Paradigm Dialog*, Newbury Park: Sage Publications, pp. 17-30.

Helmke, G. & Steven L. (2006). "Introduction." In Gretchen Helmke G. and Steven L. (ed.), *Informal Institutions and Democracy: Lessons from Latin America,* Baltimore: Johns Hopkins University Press, pp. 1–32.

Hirsch Ballin, E., Dijstelbloem, H., & de Goede, P. (2020). The Extension of the Concept of Security: *Security in an Interconnected World* (pp. 13-39). Springer, Cham.

Hudson, V. M. (2005). Foreign policy analysis: Actor-specific theory and the ground of international relations. *Foreign policy analysis,* 1-30.

Johnson, T. A. (2015). Cybersecurity Threat Landscape and Future Trends in *Cybersecurity-security: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare* (pp. 304-343). Routledge.

Kolasi, K. (2020). Structuration theory. *The Palgrave Encyclopedia of Global Security Studies.* Palgrave Macmillan. https://doi. org/10.1007/978-3-319-74336-3_360-1.

Lebogang, V., Tabona, O., & Maupong, T. (2022). Evaluating Cybersecurity Strategies in Africa. In M. Dawson, O. Tabona, & T. Maupong (Eds.), *Cybersecurity Capabilities in Developing Nations and Its Impact on Global Security* (pp. 1-19). IGI Global. https://doi.org/10.4018/978-1-7998-8693-8.ch001

Lecours, A., (2005). New Institutionalism, Issues and Questions. *In New Institutionalism* pp. 3-25. Toronto: University of Toronto Press.

Lowndes, V. (2002). Institutionalism. In David Marsh and Gerry Stoker (Eds.) *Theory and Methods in Political Science*, 2nd edition; New York: Palgrave Macmillan Publishers, p.90.

March, J. G., and Olsen J. P. (2005), Elaborating the New Institutionalism, in Robert Goodin (ed.), *The Oxford Handbook of Political Science* (2011; online edn, Oxford Academic, 5 Sept. 2013), https://doi.org/10.1093/oxfordhb/9780199604456.013.0008, accessed 22 Mar. 2023.

Mecridis, R. C., (1963). A Survey of the Field of Comparative Governance. In Eckstein H. & Apter D. E. (Eds.) *Comparative politics: A Reader*, New York: The Free press of Glencoe,

Meiser, J. (2017). 'Liberalism', In Mcglinchey, S., Walters, R. and Scheinpflug, C. (eds.) *International Relations Theory*. Briston: E-IR Foundations.

Orji, U. J. (2015, May). Multilateral legal responses to cyber security in Africa: Any hope for effective international cooperation?. In *2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace* (pp. 105-118). IEEE.

Orji, U. J., (2016). Regionalizing Cybersecurity Governance in Africa: an Assessment of Responses', *in Cherian Samuel & Munish Sharma (eds) Securing Cyberspace: International and Asian Perspectives,* Institute for Defence Studies and Analyses & Pentagon Press, New Delhi.

Ottis, R., & Lorents, P. (2010, April). Cyberspace: Definition and implications. *In International Conference on Cyber Warfare and Security* (p. 267). Academic Conferences International Limited.

Ouassini, A., & Amini, M. (2021). Cybersecurity in Ghana: Past, present, and future. In *Routledge Companion to Global Cyber-Security Strategy* (pp. 564-572). Routledge.

Razzaq, A., Hur, A., Ahmad, H. F., & Masood, M. (2013, March). Cyber security: Threats, reasons, challenges, methodologies and state of the art solutions for industrial applications.

In 2013 IEEE Eleventh International Symposium on Autonomous Decentralized Systems (ISADS) (pp. 1-6). IEEE. doi: 10.1109/ISADS.2013.6513420.

Rueschemeyer, D. and Evans, P. B. (1985). The state and economic transformation: towards an analysis of the conditions underlying effective interventions. In Evans, P. B. Rueschemeyer, D. & Skocpol, T. *Bringing the state back in*. London: Cambridge University Press.

Sabbah, C. (2018, May). Pressing pause: A new approach for international cybersecurity norm development. In Minárik, T. Jakschis, R & Lindström L. (Eds.) *10th International Conference on Cyber Conflict (CyCon)* (pp. 263-282). IEEE.

Sayer, A. (2010). Reductionism in social science. In Lee R.E. *Questioning nineteenth-century assumptions about knowledge II: Reductionism*, 5-56. State University of New York Press

Scott, W. R. (2005). Institutional theory: Contributing to a theoretical research program. *Great minds in management: The process of theory development*, *37*(2), 460-484.

Scott, W. R., (2004). "Institutional theory." In George Ritzer, (ed). *Encyclopedia of Social Theory*, Pp. 408-14 Thousand Oaks, CA: Sage.

Stivachtis, Y. (2017) The English School, In Mcglinchey, S., Walters, R. and Scheinpflug, C. (eds.) *International Relations Theory*. Briston: E-IR Foundations International Relations Theory – E-International Relations (e-ir.info)

Theys, S. (2017) "Constructivism", In Mcglinchey, S., Walters, R. and Scheinpflug, C. *International Relations Theory*. Briston: E-IR Foundations.

Tolnaiova, S. G., & Galik, S. (2020). Cyberspace as a New Living World and Its Axiological Contexts. In *Cyberspace*. London, UK: Intech Open.

Valeriano, B., & Maness, R. C. (2018). International relations theory and cyber security. *The Oxford handbook of international political theory*, 259.

Wendt, A., & Shapiro, I. (1997). The misunderstood promise of realist social theory. In K. R. Monroe (Ed.), *Contemporary empirical political theory* (pp. 166–187). Berkeley: University of California Press.

JOURNAL ARTICLES

Adu, K. K., & Adjei, E. (2018). The phenomenon of data loss and cyber security issues in Ghana. *Foresight*, *20*(2), 150-161.

Agbeko, M. (2021). Understanding Cyber Safety Behavior among Teenagers in Ghana. *International Journal of Computer Science and Information Security (IJCSIS)*, *19*(6).

Akinyetun, T. S. (2021). Poverty, Cybercrime and National Security in Nigeria. *Journal of Contemporary Sociological Issues*, *1*(2), 86-109.

Amankwa, E. (2021). Relevance of cybersecurity education at pedagogy levels in schools. *Journal of Information Security*, 12(4), 233-249.

Apau, R., & Koranteng, F. N. (2020). An overview of the digital forensic investigation infrastructure of Ghana. *Forensic Science International: Synergy*, *2*, 299-309.

Attuquayefio, P. K. (2012). Co-opting human security and deductions for security policy-making in Ghana. *Ghana Journal of Development Studies*, *9(1)*, 88-100.

Azmi, R., Tibben, W., & Win, K. T. (2016). Motives behind cyber security strategy development: a literature review of national cyber security strategy. *Research Online* University of Wollongong

Bada, M., Von Solms, B., & Agrafiotis, I. (2019). Reviewing national cybersecurity awareness for users and executives in Africa. *arXiv preprint arXiv:1910.01005*.

Bada, M., Von Solms, B., & Agrafiotis, I. (2018, November). Reviewing national cybersecurity awareness in Africa: an empirical study. In *Third International Conference on Cyber-Technologies and Cyber-Systems (CYBER 2018)*. Thinkmind Digital Library.

Baken, D. (2013). Cyber warfare and Nigeria's vulnerability'. *E-International Relations*, 3.

Bande, L. C. (2018). Legislating against Cyber Crime in Southern African Development Community: Balancing International Standards with Country-Specific Specificities. *International Journal of Cyber Criminology*, 12(1), 9-26.

Barkawi, T., & Laffey, M. (2006). The postcolonial moment in security studies. *Review of International Studies*, 32(2), 329-352.

Benedict, K. (2015). Global governance. *Bulletin of the Atomic Scientists*, Chicago, IL, USA

Bengtsson, M. (2016). How to plan and perform a qualitative study using content analysis. *NursingPlus open*, 2, 8-14.

Bennett, A. and Elman, C. (2007) 'Case Study Methods in the International Relations Subfield', *Comparative Political Studies*, 40, 2, 170-195.

Bluhm, W. T. (1984). Freedom in" The Social Contract": Rousseau's" Legitimate Chains". *Polity*, 16(3), 359-383.

Bodeau, D., Boyle, S., Fabius-Greene, J., & Graubart, R. (2012). Cyber security governance: A component of MITRE's cyber prep methodology. *Washington: MITRE Corporation. Disponível em: Acesso em*, 15.

Bodnieks, V. (2020). The New Institutionalism: A tool for analysing defence and security institutions. Security and Defence Quarterly, 32(5).

Borky, J. M., Bradley, T. H. (2019). Protecting information with cybersecurity. *Effective Model-Based Systems Engineering*, 345-404.

Brito, J., & Watkins, T. (2011). Loving the cyber bomb-the dangers of threat inflation in cybersecurity policy. *Harv. Nat'l Sec. J.*, *3*, 39.

Broadhurst, R. (2006). Developments in the global law enforcement of cyber-crime. Policing: *International Journal of Police Strategies and Management*, 29(3), 403.

Buja, A. G. (2021). Cyber Security Features for National E-Learning Policy. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, *12*(5), 1729-1735.

Bullock, J. A., Haddow, G. D., & Coppola, D. P. (2021). Cybersecurity and critical infrastructure protection. *Introduction to Homeland Security*, 425-497.

Burnard, P. (1991). A method of analysing interview transcripts in qualitative research. *Nurse education today*, *11(6)*, 461-466.

Burton, J. (2013). Small states and cyber security: The case of New Zealand. *Political Science*, *65*(2), 216-238.

Calderaro, A., & Craig, A. J. (2020). Transnational governance of cybersecurity: policy challenges and global inequalities in cyber capacity building. *Third World Quarterly*, 41(6), 917-938.

Catanzaro, M. (1988). Using qualitative analytical techniques. *Nursing research: Theory and practice*, 437, 456.

Dunn-Cavelty, M. (2013). From cyber-bombs to political fallout: Threat representations with an impact in the cyber-security discourse. *International Studies Review*, *15*(1), 105-122. https://doi.org/10.1111/misr.12023

Chen, J., Paik, M., & McCabe, K. (2014). Exploring internet security perceptions and practices in urban Ghana. In *10th Symposium on Usable Privacy and Security (SOUPS 2014)* (pp. 129-142).

Chua, C. F. (1986). "Radical Developments in Accounting Thought," The Accounting Review (61), pp. 601-632.

Collier, J. (2017). Strategies of cyber crisis management: Lessons from the approaches of Estonia and the United Kingdom. *Ethics and Policies for Cyber Operations: A NATO Cooperative Cyber Defence Centre of Excellence Initiative*, 187-212.

Craig, A. (2018). Understanding the Proliferation of Cyber Capabilities. *Council on Foreign Relations*. https://www. cfr.org/blog/understanding-proliferation-cyber-capabilities *(July 30, 2019).*

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review*, *4*(10).

Crandall, M., & Allan, C. (2015). Small states and big ideas: Estonia's battle for cybersecurity norms. *Contemporary security policy*, *36*(2), 346-368.

Danquah, P., & Longe, O. B. (2011). Cyber deception and theft: An ethnographic study on cyber criminality from a Ghanaian perspective. *Journal of Information Technology Impact*, *11*(3), 169-182.

DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organisational fields. *American sociological review*, 147-160.

Domingo, F. C. (2016). Strategic considerations for Philippine cyber security. *ADR Occasional Paper*, 9.1, 1-14. Retrieved from https://animorepository.dlsu.edu.ph/faculty_research/3215

Downe-Wamboldt, B. (1992). Content analysis: method, applications, and issues. *Health care for women international*, *13*(3), 313-321.

Dunn-Cavelty, M., & Wenger, A. (2020). Cyber security meets security politics: Complex technology, fragmented politics, and networked science. *Contemporary Security Policy*, *41*(1), 5-32.

Ebaye, S. E. (2009). The crisis of technological underdevelopment in Africa. *Lwati: A Journal of Contemporary Research*, 6(1).

Eboibi, F. E. (2020). Concerns of cyber criminality in South Africa, Ghana, Ethiopia and Nigeria: rethinking cybercrime policy implementation and institutional accountability. *Commonwealth Law Bulletin*, *46*(1), 78-109.

Eboibi, F. E. (2021). Cybercriminals and Coronavirus cybercrimes in Nigeria, the United States of America and the United Kingdom: cyber hygiene and preventive enforcement measures. *Commonwealth Law Bulletin*, *47*(1), 113-142.

Finnemore, M., & Sikkink, K. (1998). International norm dynamics and political change. *International organisation*, 52(4), 887-917.

Finnemore, M., & Hollis, D. B. (2016). Constructing norms for global cybersecurity. *The American Journal of International Law*, 110, 425–479. doi: 10.1017/S0002930000016894

Gautier, L., & Ridde, V. (2017). Health financing policies in Sub-Saharan Africa: government ownership or donors' influence? A scoping review of policymaking processes. *Global health research and policy*, *2*(1), 1-17.

Gcaza, N., & Von Solms, R. (2017). A strategy for a cybersecurity culture: A South African perspective. *The Electronic Journal of Information Systems in Developing Countries*, *80*(1), 1-17.

Giri. (2019). Cyber Crime, Cyber threat, Cyber Security Strategies and Cyber Law in Nepal. *Pramana Research Journal*, *9*(3), 662–672.

Golafshani, N. (2003). Understanding Reliability and Validity in Qualitative Research. *The Qualitative Report*, 8(4), 597–606. Retrieved from http://nsuworks.nova.edu/tqr

Grisby, A. (2017). The end of cyber norms. *Survival*, 59, 109 122. doi: 10.1080/00 396338. 2017 .1399730

Hall, P. A. & Taylor, R. C. (1996). Political science and the three new institutionalisms. *Political studies*, 44(5), 936-957.

Helmke, G. & Steven L. (2004). "Informal Institutions and Comparative Politics: A Research Agenda." Perspectives on Politics 2 (4): 725–40.

Herrington, L. M. (2013). Beyond Boston: Conspiracy theories and international relations. *E-International Relations*, *16*.

Hitchens, T., & Gallagher, N. W. (2019). Building confidence in the cybersphere: A path to multilateral progress. *Journal of Cyber Policy*, *4*, 4–21. doi: 10.1080/23738871.2019.1599032

Humayun, M., Niazi, M., Jhanjhi, N. Z., Alshayeb, M., & Mahmood, S. (2020). Cyber security threats and vulnerabilities: a systematic mapping study. *Arabian Journal for Science and Engineering*, *45*, 3171-3189.

Jaishankar, K. (2007). Establishing a theory of cybercrimes. *International Journal of Cyber Criminology*, *1*(2), 7-9.

Jiyong, P., Daegon, C., Kyu, L. J., & Byungtae, L. (2019). The Economics of Cybercrime: The Role of Broadband and Socioeconomic Status. *ACM Trans. Manage. Inf. Syst*, *10*(4).

Johns, F. (2021). Governance by data. *Annual Review of Law and Social Science*, 17, 53-71.

Kello, L. (2013). The meaning of the cyber revolution: Perils to theory and statecraft. *International Security*, *38*(2), 7-40.

Kelly, M. (2000). Inequality and crime. *The Review of Economics and Statistics*. 82 (4): 530–539

Korsell, L. (2020). Fraud in the Twenty-first Century. *European Journal on Criminal Policy and Research*, *26*(3), 285-291.

Kshetri, N. (2010). Diffusion and effects of cyber-crime in developing economies. *Third World Quarterly*, *31*(7), 1057-1079.

Kshetri, N. (2019). Cybercrime and cybersecurity in Africa. *Journal of Global Information Technology Management*, *22*(2), 77-81. https://doi.org/10.1080/1097198X.2019.1603527

Lauth, H. (2000). Informal Institutions and Democracy. *Democratization* 7 (4): 21–50 https://doi.org/10.1080/13510340008403683

Lewis, J. L., & Sheppard, S. R. (2006). Culture and communication: can landscape visualization improve forest management consultation with indigenous communities?. *Landscape and urban planning*, 77(3), 291-313.

Li, N., Tsigkanos, C., Jin, Z., Hu, Z., & Ghezzi, C. (2020). Early validation of cyber–physical space systems via multi-concerns integration. *Journal of Systems and Software*, *170*, 110742.

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, *7*, 8176-8186. https://doi.org/10.1016/j.egyr.2021.08.126

Luiijf, E., Besseling, K., & de Graaf, P. (2013). Nineteen national cyber security strategies. *International Journal of Critical Infrastructures*, *9*(1/2), 3. doi:10.1504/ijcis.2013.051608

Lun, Y. Z., D'Innocenzo, A., Malavolta, I., & Di Benedetto, M. D. (2016). Cyber-physical systems security: a systematic mapping study. *arXiv preprint arXiv:1605.09641*.

Lyytinen, K., & Rose, G. M. (2003). The disruptive nature of information technology innovations: the case of internet computing in systems development organisations. *MIS quarterly*, 557-596.

Madrid-Morales, D., Wasserman, H., Gondwe, G., Ndlovu, K., Sikanku, E., Tully, M., Umejei, E., & Uzuegbunam, C. (2021). Comparative approaches to mis/disinformation| motivations for sharing misinformation: A comparative study in six Sub-Saharan African countries. *International Journal of Communication*, 15, 20.

Makridis, C. A., & Smeets, M. (2019). Determinants of cyber readiness. *Journal of Cyber Policy*, 4(1), 72-89.

March, J. G., & Olsen, J. P. (1984). The New Institutionalism: Organisational Factors in Political Life. *The American Political Science Review*, *78*(3), 734–749. https://doi.org/10.2307/1961840

Mayring, P. (2000). Qualitative Content Analysis. *Forum: Qualitative Social Research, 1(2).* https://doi.org/10.17169/fqs-1.2.1089

McLean, S. (2013). Beware the botnets: Cyber security is a board level issue. *Intellectual Property & Technology Law Journal*, *25*(12), 22.

Mensah, R. O., Mensah, P., & Opoku, D. (2023). Experiences and perceptions of cybercrime victims in Ghana: The Perspective of digital consumers of agricultural produce. *Cogent Education*, 10(2), 2285623. https://www.tandfonline.com/doi/epdf/10.1080/2331186X.2023.2285623?needAccess=true

Mishra, A., Alzoubi, Y. I., Anwar, M. J., & Gill, A. Q. (2022). Attributes impacting cybersecurity policy development: An evidence from seven nations. *Computers & Security*, *120*, 102820.

Motsch, W., et al., 2020. Approach for dynamic price-based demand side management in cyber-physical production systems. *Procedia Manuf.* 51, 1748–1754.

Muna, S., & Díaz Pabón, F. A. (2022). The interaction of mass media and social media in fuelling ethnic violence in Ethiopia. *Conflict Trends*, 2021(4), 39-47.

Mussington, D. (2019). Strategic Stability, Cyber Operations and International Security. In *Governing Cyberspace during a Crisis in Trust: An essay series on the economic potential — and vulnerability — of transformative technologies and cyber security* (pp. 55–59). Centre for International Governance Innovation. http://www.jstor.org/stable/resrep26129.13

Ndungu, N., & Signé, L. (2020). The Fourth Industrial Revolution and digitization will transform Africa into a global powerhouse. *Foresight Africa Report*, *5*(1), 1-177.

Newman, E. (2010). Critical human security studies. *Review of International Studies*, *36*(1), 77-94.

Newman, E. (2022). COVID-19: A human security analysis. *Global Society, 36(4),* 431-454.

O'Donnell, G. (1996). Illusions About Consolidation. *Journal of Democracy*, 7(2), 34-51.

Orji, U. J. (2021). Moving beyond criminal law responses to cybersecurity governance in Africa. *International Journal of Criminal Justice*, 3(1), 60-98.

Orji, U. J. (2019). A Review of the ECOWAS Cybercrime Directive- Analysis of ICT offences with the Budapest Convention and key challenges hindering its implementation in Member States. *Computer Law Review International*, 20(2), 40-53. doi:10.9785/cri-2019-200204

Orlikowski, W.J. & Baroudi, J. J. (1991). Studying Information Technology in Organisations: Research Approaches and Assumptions. *Information Systems Research* 2(1), pp. 1-28.

Parkinson, J., Bariyo, N., & Chin, J. (2019). Huawei technicians helped African governments spy on political opponents. *Wall Street Journal*, *15*.

Peltier, T. R. (2005). Implementing an information security awareness program. *Inf. Secur. J. A Glob. Perspect.*, *14*(2), 37-49.

Peou, S. (2021). Toward a Global Human Security Governance?: Progress, Problems, and Prospects. *Hiroshima Peace Research Journal*, *8*, 71-90.

Polit, D. F., & Beck, C. T. (2006). Using research in evidence-based nursing practice. *Essentials of nursing research. Methods, appraisal and utilization. Philadelphia (USA): Lippincott Williams & Wilkins*, 12, 457-94.

Raphael, S., & Winter-Ebmer, R. (2001). Identifying the effect of unemployment on crime. *The journal of law and economics*, *44*(1), 259-283.

Reveron, D.S, Savage, J.E. (2020). Cybersecurity Convergence: Digital Human and National Security. *Orbis.* 64(4):555-570. doi: 10.1016/j.orbis.2020.08.005.

Richards, N. U., & Eboibi, F. E. (2021). African governments and the influence of corruption on the proliferation of cybercrime in Africa: wherein lies the rule of law?. *International Review of Law, Computers & Technology*, *35*(2), 131-161.

Roshanaei, M. (2021). Resilience at the core: critical infrastructure protection challenges, priorities and cybersecurity assessment strategies. *Journal of Computer and Communications*, *9*(08), 80-102.

Sabillon, R., Cavaller, V., & Cano, J. (2016). National cyber security strategies: global trends in cyberspace. *International Journal of Computer Science and Software Engineering*, *5*(5), 67.

Sarefo, S., Dawson, M., & Banyatsang, M. (2023). An exploratory analysis of the cybersecurity threat landscape for Botswana. *Procedia Computer Science*, *219*, 1012-1022.

Sarker, I. H. (2021). CyberLearning: effectiveness analysis of machine learning security modeling to detect cyber-anomalies and multi-attacks. *Internet of Things*, 14, 100393.

Savaş, S., & Karataş, S. (2022). Cyber governance studies in ensuring cybersecurity: an overview of cybersecurity governance. *International Cybersecurity Law Review*, *3*(1), 7-34.

Senol, M. & Karacuha, E. (2020). Creating and Implementing an Effective and Deterrent National Cyber Security Strategy. *Journal of Engineering*.

Shin, J., Choi, J. G., Lee, J. W., Lee, C. K., Song, J. G., & Son, J. Y. (2021). Application of STPA-SafeSec for a cyber-attack impact analysis of NPPs with a condensate water system test-bed. *Nuclear Engineering and Technology*, *53*(10), 3319-3326.

Shin, J., Son, H., & Heo, G. (2015). Development of a cyber security risk model using Bayesian networks. *Reliability Engineering & System Safety*, *134*, 208-217.

Siaw, A., Jiang, Y., Twumasi, M. A., & Agbenyo, W. (2020). The impact of internet use on income: The case of rural Ghana. *Sustainability*, 12(8), 3255.

Siegel, J. (2016). Meat space is cyberspace: the Pynchonian post-human in bleeding edge. *Orbit: A Journal of American Literature*, 4(2).

Signé, L., & Signé, K. (2021). How African States Can Improve Their Cybersecurity. *Brookings Institution Tech Stream. March*, *16*.

Snehi, M., & Bhandari, A. (2021). Vulnerability retrospection of security solutions for software-defined Cyber–Physical System against DDoS and IoT-DDoS attacks. *Computer Science Review*, 40, 100371.

Stenbacka, C. (2001). Qualitative research requires quality concepts of its own. *Management Decision.* Retrieved from http://www.emeraldinsight.com/doi/abs/10.1108/EUM0000000005801

Tamarkin, E., (2015). The AU's Cybercrime Response: A Positive Start, but Substantial Challenges ahead. *Institute for Security Studies (ISS).* South Africa. Retrieved from https://policycommons.net/artifacts/1447751/the-aus-cybercrime-response/2079526/ on 24 Mar 2023. CID: 20.500.12592/qcfbwp.

Tan, S., Xie, P., Guerrero, J. M., Vasquez, J. C., Li, Y., & Guo, X. (2021). Attack detection design for dc microgrid using eigenvalue assignment approach. *Energy Reports*, 7, 469-476.

Tankebe, J. (2008). Colonialism, legitimation, and policing in Ghana. *International journal of law, crime and justice*, 36(1), 67-84.

Tewksbury, R. (2009). Qualitative versus Quantitative Methods: Understanding Why Qualitative Methods are Superior for Criminology and Criminal Justice. *Journal of Theoretical and Philosophical Criminology*, 1(1). Retrieved from http://www.jtpcrim.org/January_Articles/Qualitative_Vs_Quantitave_Richard_Tewksbury.pdf

Turianskyi, Y. (2018). Balancing Cyber Security and Internet Freedom in Africa. *South African Institute of International Affairs.* URL: https://www.jstor.org/stable/resrep25912

Turianskyi, Y., 2020. Cybercrime and data privacy: how Africa can up its game. *Africa Portal.* South Africa. Retrieved from https://policycommons.net/artifacts/1443616/cyber-crime-and-data-privacy/2075349/ on 24 Mar 2023. CID: 20.500.12592/vqqv89.

van Vuuren, J. J., Leenen, L., & Pieterse, P. (2020). Development and implementation of cybercrime strategies in Africa with specific reference to South Africa. *Journal of Information Warfare*, 19(3), 83-101.

Von Solms, B., & Von Solms, R. (2018). Cybersecurity and information security–what goes where?. Information & Computer Security, 26(1), 2-9.

von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security, 38, 97–102*. https://doi.org/10.1016/j.cose.2013.04.004

Walker S. & Ian Tennant I., (2021, May 7). Time to engage: The UN wades into a global cybercrime treaty debate. *Global Initiative Against Transnational Crime*. Time to engage: The UN wades into a global cybercrime treaty debate | Global Initiative

Warner, J. (2011). Understanding cyber-crime in Ghana: A view from below. *International journal of cyber criminology*, *5*(1).

Warren, T. C. (2015). Explosive connections? Mass media, social media, and the geography of collective violence in African states. *Journal of Peace Research*, *52*(3), 297-311.

Waylen, G. (2014). Informal institutions, institutional change, and gender equality. *Political Research Quarterly*, *67*(1), 212-223.

Willett, W., Rockström, J., Loken, B., Springmann, M., Lang, T., Vermeulen, S., ... & Murray, C. J. (2019). Food in the Anthropocene: the EAT–Lancet Commission on healthy diets from sustainable food systems. *The lancet*, 393(10170), 447-492. doi:10.1016/s0140-6736(18)31788-4

Williams, C. (2007). Research methods. *Journal of Business & Economics Research (JBER)*, *5*(3).A

Willis B. (2014). The Advantages and Limitations of Single Case Study Analysis. *E-International Relations*

Wynn D. and Williams, C.K., (2012) Principles for Conducting Critical Realist Case Study Research in Information System. *MIS Quarterly* Vol. 36 No. 3 pp. 787-810

Zua, B. (2021). Literacy: Gateway to a world of exploits. *International Journal of Education and Literacy Studies*, 9(1), 96-104.

OFFICIAL PUBLICATIONS

Adu-Amanfoh K. & Allen N.D.F (2023, January 3). Learning from Ghana's Multi-stakeholder Approach to Cyber Security *African Center for Strategic Studies* URL:https://africacenter.org/spotlight/ghana-multistakeholder-cyber-security/

African Center for Strategic Studies (2022 April 26), *Mapping Disinformation in Africa* Mapping Disinformation in Africa – Africa Center for Strategic Studies

African Union (2012) "Rules of Procedure of the African Union Conference of Ministers in Charge of Communication and Information Technologies (CITMC)", Article 16:1 (a).

African Union (2019), "African Union Cybersecurity Expert Group Holds Its First Inaugural Meeting' https://au.int/en/pressreleases/20191212/african-union-cybersecurity-expert-group-holds-its-first-inaugural-meeting

African Union and Symantec Corporation, (November, 2016) *Cybercrime & Cybersecurity Trends in Africa, Symantec Corporation and African Union*, pp.53-55.

African Union, (2019). Peace and Security Council 850th Meeting Communiqué https://archives.au.int/bitstream/handle/123456789/6336/850th%20Meeting%20of%20the%20AUPSC%20on%20Cyber%20Security%2020%20May%202019_E%20.pdf?sequence=1&isAllowed=y

Aghajani, G., & Ghadimi, N. (2018). Multi-objective energy management in a micro-grid. *Energy Reports*, *4*, 218-225.

AU (2000). Constitutive Act of the African Union (2000, July 11), adopted at the Thirty-Sixth Ordinary Session of the Assembly of Heads of State and Government, Lome, Togo

AU (2014). "African Union Convention on Cyber Security and Personal Data Protection". *African Union*, June 27. Malabo

AU Commission (2008). Study on Harmonization of Telecommunication and ICT Policies and Regulation in Africa (draft report), p. 75, paragraph 3.3 A.2.ii.

Australian Cyber Security Center https://www.cyber.gov.au/acsc/individuals-and-families/threats.

Bank of Ghana (2020) Payment Systems Oversight. *Payment Systems Department* https://www.bog.gov.gh/wp-content/uploads/2022/02/Payment-Systems-Annual-Report-2020.pdf.

Budapest Convention (2022). *Convention on Cybercrime.* Council of Europe, https://rm.coe.int/special-edition-budapest-convention-en-2022/1680a6992e

COMESA (1994). Treaty Establishing the Common Market for Eastern and Southern Africa

COMESA (2011). Cyber Crime Model Bill. *Official Gazette of the Common Market for Eastern and Southern Africa* Vol. 16 No.2 (15 October 2011). www.comesa.int/wp-content/uploads/2020/05/2011Gazette-Vol.-16.pdf

Constitution of the Republic of Ghana, (1992). audit.gov.gh/files/publications/The_1992_Constitution_of_the_Republic_of_Ghana635603143.pdf

Côte d'Ivoire, (December 09, 2021) *National Cybersecurity Strategy of Côte d'Ivoire 2021-2025.* Strategie-Nationale-de-Cybersecurite-2021-2025-SNCS2025-.pdf (communication.gouv.ci)

Cybersecurity Act, (2020). Ghana Cybersecurity Act (1038) URL: cybersecurity.gov.gh/ documents/Cybersecurity%20A ct%202020%20(Act%201038).pdf

East African Communication Organisation, (2017). EAC Model ICT Policy URL: eaco.int/admin/docs/publications/EAC_MODEL_ICT_POLICY.pdf

ECOWAS Development Partners' Coordination Cell, (2022). *Organised Crime:West African Response On Cybersecurity & Fight Against Cybercrime (OCWAR-C)*

https://www.raosupportcellecowas.com/post/west-african-response-on-cybersecurity-and-fight-against-cybercrime-ocwar-c-1. Accessed on 22nd September, 2023.

ECOWAS Directive C/DIR.1/08/11 on Fighting Cybercrime, adopted at the Sixty Sixth Ordinary Session of the ECOWAS Council of Ministers at Abuja, Nigeria (August 2011).

ECOWAS Regional Cybersecurity and Cybercrime Strategy.

ENISA Threat Landscape 2021, "ENISA Threat Landscape 2021," ÈNISA, 2021.

Ghana Commercial Bank, (2023). *Sector Industry Study-Telecommunication Sector 2023*. https://www.gcbbank.com.gh/downloads/research/sector-industry-reports/270-telecom-sector-report-revised-2023-f/file

Guermazi B. (2021). Cybersecurity risks are global. We must address them with a coordinated, collaborative approach AUGUST 19, 2021 https://blogs.worldbank.org/digital-development/cybersecurity-risks-are-global-we-must-address-them-coordinated-collaborative-approach

International Telecommunications Union (2012). Understanding cybercrime: Phenomena, challenges and legal response. Geneva: International Telecommunications Union.

Interpol, (2021) "African Cyberthreat Assessment Report - *Interpol's Key Insight into Cybercrime in Africa*,"

Interpol, (2021). *The African Cyber threat Assessment Report*. Retrieved from: https://www.interpol.int/content/download/16759/file/AfricanCyberthreatAssessment_ENGLISH.pdf

ISC^2 Cybersecurity Workforce Study, (2022). "A critical need for cybersecurity professionals persists amidst a year of cultural and workplace evolution", Accessed from https://www.isc2.org//-/media/ISC2/Research/2022-WorkForce-Study/ISC2-Cybersecurity-Workforce-Study.ashx, Accessed on July 14, 2023

ITU (2020) Global Cybersecurity Index 2020, Retrieved from https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf on 14th April 2023

ITU HIPSSA Project (11-12 December 2008). Support for Harmonization of the ICT Policies in Sub-Saharan Africa. Addis Ababa, Ethiopia https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Pages/default.aspx

ITU, (2012). ITU National Cybersecurity Strategy Guide (F. Wamala, ed.), *Geneva: International Telecommunication Union* URL: http://www.itu.int/ITUD/cyb/cybersecurity/docs//ITUNationalCybersecurityStrategyGuide.pdf).

ITU, (2021, 1 September) *"Are African countries doing enough to ensure cybersecurity and Internet safety?"* Retrieved from https://www.itu.int/hub/2021/09/are-african-countries-doing-enough-to-ensure-cybersecurity-and-internet-safety/ on 16 July 2023.

KAIPTC, (2017, August 14) *Cyber Security challenges-Communications Minister*. https://www.kaiptc.org/lack-of-skills-set-is-major-contributor-to-cyber-security-challenges-communications-minister/

MFWA (2017). Cyber Security in Ghana, Key Issues and Challenges *Policy Brief* June, 2017 https://www.mfwa.org/wp-content/uploads/2017/09/cyber-security-Report.pdf

Ministry of Communications (2015, 23 July). *Ghana National Cyber Security Policy & Strategy* Cyber Policy Portal database Retrieved on January, 4 2023 URL: Ghana National Cyber Security Policy & Strategy • Page 3 • UNIDIR Cyber Policy Portal Database.

MISA & KAS, (2021, October 17). "Cybersecurity and Cybercrime Laws in the SADC Region: Implications on Human Rights." https://data.misa.org/api/files/1634498575242w6kap89lsf8.pdf

Neto I., Obiso M. & Baayen M. (2022). "How tailored national cybersecurity strategies enable safe, inclusive and sustainable digital development". June 8, 2022. *Digital Development.*URL:https://blogs.worldbank.org/digital-development/how-tailored-national-cybersecurity-strategies-enable-safe-inclusive-and

NIST (June, 2018) "Framework for improving critical infrastructure cybersecurity". *nist. gov/nistpubs/CSWP/NIST. CSWP, 4162018 URL:* https://www.nist. gov/sites/default t/files/documents/cyberframework/cybersecurityframework-021214.pdf, 2014. [Retrieved: June 2018].

OECD, (2012). Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy. OECD Digital Economy Papers (No.322 ed., Vol. 211), OECD Publishing (doi: http://dx.doi.org/10.1787/5k8zq92vdgtl-en).

Official Gazette of the Common Market for Eastern and Southern Africa (COMESA) Vol. 16 No. 2 (15 October 2011).

Republic of Kenya. (2022) National Computer and Cybercrimes Coordination Committee Secretariat. National Cybersecurity Strategy.

SADC (2012) Southern African Development Community (SADC) Model Law On Computer Crime And Cybercrime www.itu.int/ITU-D/projects/ITU_EC_ACP/hipssa/docs/SA4docs/cybercrime.pdf

SADC (2018, 17 September) SADC convenes Cyber Security Workshop and SADC Regional Cyber Drill SADC convenes Cyber Security Workshop and SADC Regional Cyber Drill | SADC

Toussi, S. (2022, June 22). *Disinformation Pathways and Effects on Democracy and Human Rights in Africa: Case studies from Five Countries.* CIPESA https://cipesa.org/2022/06/new-report-disinformation-pathways-and-effects-on-democracy-and-human-rights-in-africa/

ECOWAS (1996). Treaty of ECOWAS (Revised, 24 July, 1993), 35 ILM 660,

Tunis Agenda for the Information Society (2005). WSIS 05/TUNIS/DOC/6(Rev.1)-E 18 November 2005 https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html

UNHRC, (2016, June 27) "Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development" https://www.article19.org/data/files/Internet_Statement_Adopted.pdf, accessed 10 April 2023.

UNCTAD (2003) *Africa's Technology Gap. Case Studies on Kenya, Ghana, Uganda and Tanzania.*

UNCTAD, (2021, 14 Dec) Cybercrime Legislation Worldwide Cybercrime Legislation Worldwide | UNCTAD

United Nations E-Government Survey (2018). Gearing E-Government to Support Transformation towards Sustainable and Resilient Societies. United Nations, New York. Publicadministration.un.org https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2018-Survey/E-Government%20Survey%202018_FINAL%20for%20web.pdf

UN General Assembly (2010, July 30). Note by the Secretary-General 65/201 - Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. A/65/201. New York: United Nations, 30 July 2010.

US Federal Bureau of Investigation, (2023, Feb 1). 2013 Internet Crime Report, Available at: http://www.ic3.gov/media/annualreport/2013_IC3Report.pdf [Accessed 27 August 2023]

World Economic Forum (2023). "Cybersecurity: How closing the skills gap can improve resilience and support a workforce in transition" Feb 1, 2023, Accessed from https://www.weforum.org/agenda/2023/02/cybersecurity-how-to-improve-resilience-and-support-a-workforce-in-transition/ on 14 July 2023.

World Economic Forum (January, 2024) Global Cybersecurity Outlook 2024 Insight Report Global Cybersecurity Outlook 2024 | World Economic Forum (weforum.org)

World Economic Forum (Jun 28, 2022) Cybersecurity: Steps cyber-resilient businesses must take now. What is 'cyber hygiene' and how can we achieve it? | World Economic Forum (weforum.org)

World Economic Forum, (January 18, 2023). *Experts at Davos 2023 call for a global response to the gathering "cyber storm".* Davos Experts at Davos 2023 sound the alarm on cybersecurity | World Economic Forum (weforum.org)

INTERNET SOURCES

Acayo, G. (2017). *Global Cybersecurity Index Overview*. International Telecommunication Union, 2nd Annual Meeting of Community of Practice on Composite Indicators and Scoreboards (9-10 November 2017, Ispra, Italy), slide 5.

Adu-Owusu P. (2024, March 19). "JoyNews; Youth Bridge Foundation organise National Dialogue on cybersecurity." *Myjoyonline.* https://www.myjoyonline.com/joynews-youth-bridge-foundation-organise-national-dialogue-on-cybersecurity/

Afreximbank (2022) "Pan-African Payment and Settlement System Launched by President Akufo-Addo Foreseeing $5 billion Annual Savings for Africa", 01/13/2022 Accessed from https://www.afreximbank.com/pan-african-payment-and-settlement-system-launched-by-president-akufo-addo-foreseeing-5-billion-annual-savings-for-africa/ on 13 July, 2023.

AfricanCERT (2020) https://www.africacert.org/about-us/

Aklama, B. (2023, 3 October). Ghana loses GHS49.5 million to Cyber Fraud in nine Months Citionline.com/citibusinessnews

Allen, N. & van der Waag-Cowling, N. (, 2021, July 15) *How African states can tackle state-backed cyber threats* URL: How African states can tackle state-backed cyber threats | Brookings

AmaniAfrica (2023) "Cybersecurity: Impact on peace and security in Africa" 13 April, 2023. https://amaniafrica-et.org/cyber-security-impact-on-peace-and-security-in-africa/ on 11 July 2023.

Arnould, V & Strazzari, F. (2017). African Futures: Horizon 2025. European Union Institute for Security Studies.

Canadian Center for Cyber Security, online https://cyber.gc.ca/en/glossary

Chellel K. (2019, December 20). The Hacker Who Took Down a Country www.bloomberg.com/news/features/2019-12-20/Spiderman Hacker Daniel Kaye Took Down Liberia's Internet - Bloomberg

Citi Newsroom, (2023, October 12). Slamm Foundation, ISC2 make strides in national cybersecurity education. https://citinewsroom.com/2023/10/slamm-foundation-isc2-make-strides-in-national-cybersecurity-education/

Consultancy.africa (13 March 2018) *Consulting firm opens first ever Cyber Immersion Centre in Nairobi* URL:Consulting firm opens first ever Cyber Immersion Centre in Nairobi (consultancy.africa)

Council of Europe (2023). *Parties/Observers to the Budapest Convention and Observer Organisations to the T-CY*. https://www.coe.int/en/web/cybercrime/parties-observers retrieved on 16 March 2023

Council of Europe (Accessed on 2024, March 29). The Global Action on Cybercrime (GLACY). From www.coe.int/en/web/cybercrime/glacyplus

Cyber Capacity Knowledge Portal (2024 March 29). Actor: African Civil Society on the Information Society (ACSIS). https://cybilportal.org/projects-by?page=region&_sft_region=sub-saharan-africa

Cybersecurity, cybercrime, and child online protection in Africa: National approaches and elements of foreign policy. URL: National cybersecurity and cybercrime policies in Africa - Diplo Resource (diplomacy.edu)

Datarportal (2023). "Digiatl 2023-Ghana" 13 February, 2023, Accessed from https://datareportal.com/reports/digital-2023-ghana, On 13 July, 2023.

Dionne, S. (2019). Boko Haram is Back with Better Drones. *The New York Times*. www.nytimes.com/2019/09/13 retrieve on 29, August 2023

Dzidzoamenu, I. (2022, October 3). *"ECG might have paid ransom over hacked system" StarrFMonline.* From: starrfm.com.gh/2022/10/ecg-might-have-paid-ransom-over-hacked-system-kwabena-donkor/#:~:text=October%203%2C%202022%20Former%20Minister%20for%20Power%2C%20Dr.,customers%20in%20some%20operational%20areas%20of%20the%20country

El Mehdi, B. (2020). Cybercrime: West African Banks Are Under-protected. Retrieved from https://www.theafricareport.com/22644/cybercrime-west-african-banks-are-under-protected/ on 20th October, 2023.

EU Cyber Direct (2021). Regionalised Multilateralism? EU-Africa Cooperation In Cyberspace, 13 April 2021, www.iss.europa.eu/sites/default/files/EUISSFiles/EU_Africa_Track1.5_Agenda_0.pdf

European Council & Council of the European Union (2022) European Union - African Union summit, (17-18 February 2022). Accessed on 2024, March 29,From www.consilium.europa.eu/en/meetings/international-summit/2022/02/17-18/

Finnemore, M., 2017. Cybersecurity and the Concept of Norms. United States of America. Retrieved from https://policycommons.net/artifacts/431552/cybersecurity-and-the-concept-of-norms/1402610/ on 22 Mar 2024. CID: 20.500.12592/2bz2gb.

Freedom House, (2016). "Freedom on the Net 2016: Silencing the messenger – communication apps under pressure", 14 November 2016, https://freedomhouse.org/article/freedom-net-2016-silencing-messenger-communication-apps-under-pressure, retrieved on 16 June 2023.

Frimpong, E.D. & Baneseh, M.A. (2017, May 01). "Hackers on rampage - Target media websites" *Graphiconline*. www.graphic.com.gh/news/general-news/hackers-on-rampage-target-media-websites.html

Gady, F. S. (2010). Africa's cyber WMD, Accessed March 24, 2010. http://www.foreignpolicy.com/articles/2010/03/24/africas_cyber_wmd?page=0,0.

Ghanaweb (2023, 9 September) *ECG was hacked - Energy minister confirms* ECG was hacked - Energy minister confirms (ghanaweb.com).

Ghanaweb (August 14, 2023) *Hackers break into government website with prostitution, other adverts.* URL: https://www.ghanaweb.com/GhanaHomePage/NewsArchive/Hackers-break-into-government-website-with-prostitution-other-adverts-1824575#:~:text=The%20official%20website%20of%20the,advertise%20escort%20services%20(prostitution).

Ghanaweb, (2017, April 20). "How pair Networks shuttered down the most important website of Ghana", Business News, 20 April 2017. https://www.ghanaweb.com/GhanaHomePage/business/How-pair-Networks-shutted-down-the-most-important-website-of-Ghana-530631 Retrieved on 15 July 2023.

Henderson R. & Mackenzie J. (2019, October 25). Johannesburg City Crippled as Hacker Demands Bitcoin Ransom www.bloomberg.com/news/articles/2019-10-25/south-africa-s-johannesburg-shuts-billing-over-security-breach

Hunter M & Tilley A., (2017, July 28) 'Cybercrimes Bill makes cyberspace less secure,' Daily Maverick, https://www.dailymaverick.co.za/article/2017-07-28-groundup-cybercrimes-billmakes-cyberspace-less-secure/#.WeCyN2hL82w, accessed 13 October 2017.

Internet World Stats, (2022), http://www.internetworldstats.com/stats1.htm, Accessed on 9 April 2023.

ITU (2022) ITU Definition of Cybersecurity [Online] (2022) Available: https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx

Kemp, S. (2014). Digital 2024: Ghana.*DataReportal (2024)* datareportal.com/reports/digital

Knight, T. & le Roux J., (2023, June 29). "The disinformation landscape in West Africa and beyond" *In-Depth Research & Reports.* From www.atlanticcouncil.org/in-depth-research-reports/report/disinformation-west-africa/

Merriam-Webster. 2016a. "Definition of Strategy," (available at http://www.merriamwebster.com/dictionary/strategy; retrieved May 17, 2016).

Mustapha, S. & Boateng, C. (2024, 09 February) "EOCO liaises with telcos, banks to combat organised crime" *Graphic Online* https://www.graphic.com.gh/news/general-news/ghana-news-eoco-liaises-with-telcos-banks-to-combat-organised-crime.html

Nartey, L. (2023, January 18) "Cyber Security experts warn of projected increase in cyber-attacks in 2023" *3News.com/Ghana*. URL:Cyber Security experts warn of projected increase in cyber-attacks in 2023 | 3News - First In News | Ghana News Updates

National Peace Council (2024 March 27). *Countering mis/disinformation and propaganda requires collaborative efforts – Peace Council.* Accessed on 30 March, 2024 from

https://www.peacecouncil.gov.gh/2024/03/28/countering-mis-disinformation-and-propaganda-requires-collaborative-efforts-peace-council/

NCA, (2023, November 15). "NCA Collaborates with CSA to Hold Cybercrime and Cybersecurity Sensitisation for Staff." https://nca.org.gh/2023/11/15/nca-collaborates-with-csa-to-hold-cybercrime-and-cybersecurity-sensitisation-for-staff/

Nyavor, G. (2014, December 12) "Ghana Gets National Data Centre by 2015," *JoyOnline*. Available at: www.myjoyonline.com/ghana-gets-national-data-centre-by-2015/

Renals, P. (2020). SilverTerrier: 2019 Nigerian Business Email Compromise Update. SilverTerrier: 2019 Nigerian Business Email Compromise Update (paloaltonetworks.com)

Sackitey, D. (2024, 17 September). Staff involvement in Bank fraud rises 46%, losses hit GH¢63m in 2023 – BoG Report URL: Staff involvement in Bank fraud rises 46%, losses hit GH¢63m in 2023 – BoG Report (citinewsroom.com)

Shani, A., (2019, June 1) *Just Think What Goebbels Could Have Done With Facebook*. HAARETZ https://www.haaretz.com/world-news/.premium.magazine-just-think-what-goebbels-could-have-done-with-facebook-1.7308812 . Accessed 19 September, 2023

Swinton, S., Hedges, S. (2019). Cybersecurity Governance, Part 1: 5 Fundamental Challenges [Online]. Retrieved 9 November 2020 from https://insights.sei.cmu.edu/insider-threat/2019/07/cybersecurity-governance-part-1-5-fundamental-challenges.html

Teleanu, S., & Kurbalija, J. (2022). Stronger digital voices from Africa: Building African digital foreign policy and diplomacy. *Diplo* https://dspace.diplomacy.edu/handle/123456789/268

Tunggal, A. T., (2022). What is a Cyber Threat? https://www.upguard.com/blog/cyber-threat. updated Aug 17, 2022

US Embassy in Ghana, (2020, January 23). "U.S. and Ghana Partner to Build Capable and Resilient Security and Justice Sector Institutions" https://gh.usembassy.gov/u-s-and-ghana-partner-to-build-capable-and-resilient-security-and-justice-sector-institutions/

Yusuf, M. (July 28, 2023). Report: Six African Countries Restricted Internet Access Due to Protests or Political Crisis. VOA URL: www.voanews.com/a/report-six-african-countries-restricted-internet-access-due-to-protests-or-political-crisis/7202326.html

UNPUBLISHED SOURCES

Affum C., (2019). Cybersecurity Practices among Foreign Banks in Ghana. *MPhil thesis submitted to the University of Ghana*

Aggrey-Darko, E. (2012). Parliament and public policy making under Ghana's fourth republic. 1993-2008" (*Unpublished PhD Thesis, submitted to the University of Ghana*) 2012.

Akuako, E. (2022). The Sakawa Boys: A Critique of Policing of Cybercrime in Ghana. *An MA thesis submitted to the University of Brock*

Appiah, J.A. (2014). The African Union and the Quest for Peace and Security in Africa: 2002 - 2012 (*Unpublished PhD Thesis, submitted to the University of Ghana)*

Asamoah, B. (2019). Twenty-first Century Terrorism and National Security: An assessment of Ghanaian Consciousness and Preparedness. *(Unpublished thesis submitted to the University of Cape Coast) URL: ir.ucc.edu.gh/xmlui/bitstream/handle/123456789/7645/Asamoah%2C%202019.pdf*

Baylon, C., & Antwi-Boasiako, A. (2016). Increasing internet connectivity while combatting cybercrime: Ghana as a case study.

Botchwey, G. (2018). E-governance and cybersecurity: User perceptions of data integrity and protection in Ghana. In *5th Biennial Social Science Conference of the University of Education, Winneba, Ghana*.

Cole, K., Chetty, M., LaRosa, C., Rietta, F., Schmitt, D. K., Goodman, S. E., & Atlanta, G. A. (2008). Cybersecurity in Africa: An assessment. *Atlanta, Georgia, Sam Nunn School of International Affairs, Georgia Institute of Technology*.

Craig, A. (2020). Capabilities and conflict in the cyber domain: an empirical study (*Doctoral dissertation, Cardiff University*).

Forson-Adaboh, K. (2022). Assessing maritime cyber security awareness in navies of the Gulf of Guinea countries: a case study of Ghana. *MSc dissertation submitted to World Maritime University*. Retrieved from Google Scholar

Van Raemdonck N. (January 2021). Cyber diplomacy in Africa.*Vrije University, Bruseel*. DOI:10.13140/RG.2.2.29455.10406

OTHER SOURCES

Adomako, Kwasi and Mohamed, Nabeel and Garba, Aminata and Saint, Martin, Assessing Cybersecurity Policy Effectiveness in Africa via a Cybersecurity Liability Index (March 16, 2018). TPRC 46: The 46th Research Conference on Communication, Information and Internet Policy 2018, Available at SSRN: https://ssrn.com/abstract=3142296 or http://dx.doi.org/10.2139/ssrn.3142296

Al-Ghamdi. (2021). Guide to developing a National Cyber Security Strategy. *Materials Today: Proceedings*

Business Software Alliance (2018) 'Software Management: Security Imperative, Business Opportunity'https://gss.bsa.org/wpcontent/uploads/2018/05/2018_BSA_GSS_Report_en.pdf

Calandro, E & Berglund, N. (2019) 'Cyber Capacity Building in SADC', Research ICT Africa https://researchictafrica.net/wp/wpcontent/uploads/2019/11/33_Calandro_Berglund_Unpacking-Cyber-Capacity-Building-1.pdf

HMG (the Her Majesty's Government), (2010). A Strong Britain in an Age of Uncertainty: The National Security Strategy, London: Her Majesty's Government ISBN 9780101795326, doi: Cm 7953).

Ifeanyi-Ajufo (n.d). *Negotiating Africa's digital partnerships: Interview Series. Global* Economic Governance Programm, University of Oxford from: https://www.geg.ox.ac.uk/content/nnenna-ifeanyi-ajufo-current-state-cybersecurity-africa-tendency-towards-cyber. Retrieved on 30 March, 2024

Mattern, M., & McKay, C. (2018). Building Inclusive Payment Ecosystems in Tanzania and Ghana (No. 30274). *The World Bank Group*.

Motiwala, A. (February 2017). "*Cyber Security in Ghana: Evaluating Readiness for the Future.* Policy Brief 1, Accra: KAIPTC.

Opoku-Afari M. (2021). A Directive for the Protection of Critical Information Infrastructure (CII) and the Cyber Security Authority (CSA). https://www.bog.gov.gh/wp-content/uploads/2021/10/1ST-Deputy-Governors-Speech-Official-Launch-Of-National-Cyber-Security-Awareness-Month-2021.pdf

Seger, A. (2016). The Budapest Convention on Cybercrime: A framework for capacity building. *Global Cyber Expertise Magazine*, 2. URL: GlobalCyberExpertiseMagazine_issue2-1.pdf (thegfce.org)

Sulieman, A. (2020) 'The African Union Cybersecurity Expert Group (AU-CSEG)', Global Cyber Expertise Magazine, vol. 7 URL:https://thegfce.org/wp-content/uploads/2020/04/Global-Cyber-Expertise-Magazine_edition7_April2020.pdf

Appendix 1 Interview Respondents

INSTITUTIONS	OFFICERS INTERVIEWED	NUMBER OF PERSONS INTERVIEWED	GENDER
Ministry of National Security	Director, Intelligence	1	M
Cyber Security Authority	Senior Offices	2	M
National Communication Authority	Senior Offices	2	M
National Signals Bureau	Director, cyber security	1	M
Cybersecurity Experts Association	President and 3 members	4	M
E-Crime Bureau	Lead, Cyber Security Analysis	1	M
Media Foundation for West Africa	Program officer, Digital Rights	1	F
UPSA (Cybersecurity Unit)	Lecturer cybersecurity unit	1	M
Ghana Police Service	Senior officers(CID, Police Training School)	2	M
Ghana Armed Forces	Senior Officer (cyber defence Unit)	1	M
AITI-KACE	Instructors (cybersecurity Unit)	2	M
EOCO	Director (IT/Cyber)	1	M
Ghana Commercial Bank	Senior Officer (IT Section)	1	M
GTBank	Cybersecurity Unit lead	1	M
Omni Bank	Senior Officer (cyber unit)	1	M
MTN Ghana	Senior Officer (cyber section)	1	M
Vodafone Ghana	Senior Officer	1	M
African Center for Strategic Studies	Executive member	1	M
Slamm Technology Solutions	Senior Officers	2	M
AU Commission	Cybersecurity Working Group (member)	1	M
Hackers	Anonymous	3	M
First Focus group discussion	Trade union members, entrepreneurs,	4	2M 2F
Second Focus group discussion	students, prison officers, hawkers	4	2M 2F

Appendix 2 Ethical Clearance

UNIVERSITY OF GHANA
ETHICS COMMITTEE FOR THE HUMANITIES (ECH)
P. O. Box LG 74, Legon, Accra, Ghana

My Ref. No: ECH 280/ 22-23

August 25, 2023

Gideon Nlibe Bilijoe
Legon Center for International Affairs and Diplomacy
University of Ghana
Legon

ETHICAL CLEARANCE
(ECH 280/ 22-23)

The Ethics Committee for the Humanities (ECH) conducted a full board review and approved your protocol titled:

STATE RESPONSE TO CYBER THREATS IN AFRICA: AN EXAMINATION OF GHANA'S CYBERSECURITY STRATEGY

PRINCIPAL INVESTIGATOR: **GIDEON NLIBE BILIJOE**

Please note that the final review report must be submitted to the Committee at the completion of the study. Your research records may be audited at any time during or after the implementation. Any modification of this research project must be submitted to ECH for review and approval prior to implementation.

Please report all serious adverse events related to this study to ECH within seven (7) days verbally and in writing within fourteen (14) days.

This certificate is valid until August 24, 2024. You are required to submit annual reports for continuing review.

Please accept my congratulations.

Yours Sincerely,

Professor C. Charles Mate-Kole
ECH Chair

Cc: Dr. Amanda Jennifer Coffie, Legon Center for International Affairs and Diplomacy, UG
Dr. Phillip Attuquayefio, Legon Center for International Affairs and Diplomacy, UG
Dr. Festus Kofi Aubyn, West Africa Network for Peacebuilding (WANEP), Accra

Tel: +233 30 393 3866 Email: ech@ug.edu.gh

Appendix 3 Interview Guide

UNIVERSITY OF GHANA

LEGON CENTRE FOR INTERNATIONAL AFFAIRS AND DILPOMACY

PhD THESIS

CATEGORY: INTERVIEW GUIDE FOR INTERNAL STAKEHOLDERS AND ACADEMICS

INTRODUCTION

Thank you very much for this opportunity to have this interview session with you. I am **GIDEON NLIBE BILIJOE, a PhD Candidate at the Legon Centre for International Affairs and Diplomacy (LECIAD),** university of Ghana. I am conducting a research on ***STATE RESPONSE TO CYBER THREATS IN AFRICA: AN EXAMINATION OF GHANA'S CYBERSECURITY STRATEGY***. The research specifically examines Ghana's National Cyber Security Policy and strategies and seek to establish whether or not its provisions are adequate to enhancing safety of the cyberspace in the country. This interview is only for academic purpose. The session will be recorded and your responses would be treated with utmost confidentiality. The session will last for about 20minutes, and any time you feel like discontinuing with the interview, you may draw my attention.

Thank you.

NAME OF THE INTERVIEWE ....

ORGANIZATION/PORTFOLIO OF INTERVIEWEE .....

1. What is Cyber security in your view and what are the specific dominant cyber threats in Ghana?
2. What are the specific roles of the state in the promotion of cyber safety?
3. What obstacles do you consider as hindrances to the efforts of African states attempt to improving the security of their cyber spaces?
4. Has the Ghanaian state any distinct cyber threat character that would require some special initiatives to secure its cyberspace?
5. What strategies do you think will help to better enhance cyber security safety in Ghana?
6. What policies or strategies has the Ghanaian state put in place to address its cybersecurity concerns?
7. What role(s) does your institutions play in the implementation of these strategies?
8. To what extent do you think these strategies are appropriate and adequate for the task?
9. What are the main challenges, if any, in the country's approaches or strategies for cyber security enhancement?
10. Do you think **social norms** provide any dynamism to cybercrime in Ghana? **If YES**, what are they and how can that be tackled?
11. Beyond cyber security laws and infrastructure, what other measures can Ghana undertake to enhance the security of its cyber space?
12. What other thing do you have to say as far as Ghana tapping into the opportunities provided by the cyberspace is concerned?

THANK YOU

DATE OF INTERVIEW: .....

UNIVERSITY OF GHANA

LEGON CENTRE FOR INTERNATIONAL AFFAIRS AND DIPLOMACY

PhD THESIS

CATEGORY: INTERVIEW GUIDE FOR INTERNAL STAKEHOLDERS (TELCOS)

INTRODUCTION

Thank you very much for this opportunity to have this interview session with you. I am **GIDEON NLIBE BILIJOE**, a **PhD Candidate at the Legon Centre for International Affairs and Diplomacy (LECIAD),** university of Ghana. I am conducting a research on ***STATE RESPONSE TO CYBER THREATS IN AFRICA: AN EXAMINATION OF GHANA'S CYBERSECURITY STRATEGY***. The research specifically examines Ghana's National Cyber Security Policy and strategies and seek to establish whether or not its provisions are adequate to enhancing safety of the cyberspace in the country. This interview is only for academic purpose. The session will be recorded and your responses would be treated with utmost confidentiality. The session will last for about 20minutes, and any time you feel like discontinuing with the interview, you may draw my attention.

Thank you.

NAME OF THE INTERVIEWER …… …… …….

ORGANIZATION & POSITION OF INTERVIEWEE …….

1. What is Cyber security in your view and what are the dominant cybersecurity threats in Ghana?
2. What are the specific roles of the state in the promotion of cyber safety?
3. Has the Ghanaian cyber ecosystem system any distinct cyber threat character that would require some special initiatives to secure its cyberspace?
4. What policies or strategies has the Ghanaian state put in place to address the cybersecurity concerns in the telecom sector?
5. Is there a Computer Emergency Response Team (CERT) for the Telecom Sector? **If Yes**, what are its prospects and challenges?
6. To what extent do you think the strategies put in place by the state are appropriate and adequate for cyber safety promotion in the telecom sector in Ghana?
7. What are the main challenges in the country's approaches or strategies for the telecom sector cyber security enhancement?
8. What strategies do you think will help to better enhance cyber security safety in Ghana?
9. Do you think **social norms** provide any dynamism to cybercrime in Ghana? **If YES**, what are they and how can that be tackled?
10. Beyond cyber security laws and infrastructure, what other measures can Ghana undertake to enhance the security of its cyber space?
11. What other things would you recommend as far as Ghana tapping into the opportunities provided by the cyberspace is concerned?

THANK YOU

DATE OF INTERVIEW: ……

UNIVERSITY OF GHANA

LEGON CENTRE FOR INTERNATIONAL AFFAIRS AND DILPOMACY

PhD THESIS

CATEGORY: INTERVIEW GUIDE FOR EXTERNAL ACTORS

INTRODUCTION

Thank you very much for this opportunity given me to have an interview with you. I am **GIDEON NLIBE BILIJOE**, a **PhD Candidate at the Legon Centre for International Affairs and Diplomacy (LECIAD),** university of Ghana. I am conducting a research on ***STATE RESPONSE TO CYBER THREATS IN AFRICA: AN EXAMINATION OF GHANA'S CYBERSECURITY STRATEGY***. The research specifically examines Ghana's National Cyber Security Policy and strategies and seek to establish whether or not its provisions are adequate to enhancing safety of the cyberspace in the country. This interview is only for academic purpose. The session will be recorded and your responses would be treated with utmost confidentiality. The session will span for about 30minutes, and any time you feel like discontinuing with the interview, you may draw my attention.

Thank you.

NAME OF THE INTERVIEWEE …….

ORGANIZATION/PORTFOLIO OF INTERVIEWEE ……..

1. How does your outfit conceptualize Cyber security and what are the specific dominant cyber threats in West/Africa?
2. What are the specific roles of AU/ECOWAS in the promotion of cyber safety?
3. Is there any distinctive cyber threat character that would require some kinds of initiatives to secure their cyberspace in Africa?
4. What obstacles do you consider as hindrances to the efforts of improving security in the cyber spaces in West/Africa?
5. What strategies do you think will help to better enhance cyber security safety in Africa?
6. What policies, strategies has the AU/ECOWAS put in place to address its cybersecurity concerns?
7. What roles does your institutions play in the implementation of these strategies?
8. To what extent do you think these strategies are appropriate and adequate for the task?
9. What are the main challenges, if any, are there in the approaches or strategies towards the enhancement of cybersecurity?
10. Do you think **social norms** provide any dynamism to cybercrime in Africa? **If YES**, what are they and how can that be tackled?
11. Beyond cyber security laws and infrastructure, what other measures can be undertaken to enhance the security cyber space?
12. What other thing do you have to say as far as states tapping into the opportunities provided by the cyberspace is concerned?

DATE OF INTERVIEW: .....