

https://dspace.org/

Determinants of government cyber security capacity in developing countries

Rezaei, Amir Hossein

2025
University of the Witwatersrand, Johannesburg
https://hdl.handle.net/10539/49276
Rezaei, Amir Hossein. (2025). Determinants of government cyber security capacity in developing countries [Master's dissertation, University of the Witwatersrand, Johannesburg]. WIReDSpace. https://hdl.handle.net/10539/49276

Downloaded from a DSpace repository. https://dspace.org/





Determinants of government cyber security capacity in developing countries

Faculty of Commerce, Law, and Management
Wits School of Governance
University of the Witwatersrand

A research report submitted for the partial fulfilment of a Master of Management in the field of Governance (Public Policy)
2025

By: Amir Hossein Rezaei
Student Number: 381638
Supervisor: Dr Rekgotsofetse Chikane

i. Declaration

I, **Amir Hossein Rezaei** (Student No. 381638), confirm that I am the author of this research report and that I have submitted it only to the 7213A course at the Wits School of Governance (University of the Witwatersrand).

Dedication

To Parvin Soltani, Koroush Soltani, Zahra Ghanbari, and Shaun Johnson: May your beautiful souls rest in peace. This work is dedicated to your memory and to the love and guidance you generously offered me throughout my life.

Acknowledgements

To my parents, Hossein and Nasrin Rezaei, thank you for your unwavering support and love. You always encourage me to pursue knowledge and have stood by me through my undergraduate and honours degrees, even when I dropped out of university in 2009 and changed my choice of degree in 2010. I am deeply grateful for the sacrifices you have made and the hardships you have endured in building a life for Reza, Arash, and me in South Africa.

To my brother, Reza Rezaei, I am grateful for your continuous support and your love as my eldest brother. Your dedication to our family's wellbeing has been instrumental in enabling me to pursue my studies.

To Katie Yang, my partner, thank you for walking this journey with me every step of the way. Your incredible support and love have been invaluable, particularly when managing my epilepsy felt overwhelming and I questioned whether I could continue with this master's degree. Your love kept me going when I needed it most.

To Dr Rekgotsofetse Chikane, thank you for your supervision. Your guidance has been essential to completing this research report.

To Dr Halfdan Lynge, thank you for your guidance during the research proposal development and defence process.

To my medical doctors, thank you for your expertise and care in helping me navigate the complexities of managing my epilepsy whilst undertaking this master's degree.

To the Canon Collins Trust, thank you for partially funding this master's degree and for warmly welcoming me into the Canon Collins family.

ii. Abstract

This study aimed to identify and analyse the key determinants of government cybersecurity capacity in African and developing countries and assess the effect of these determinants on government cybersecurity capacity within these two groups of countries. The study employed quantitative analysis using ordinal logistic regression models and the sixth version of the Digital Society Project dataset, specifically examining longitudinal data from 2000 to 2023 in 50 African and 90 developing countries. In developing countries, there was a negative relationship between government social media monitoring and government cybersecurity capacity, whereas there was no significant relationship between government social media monitoring and government cybersecurity capacity in African countries. The findings indicated that the impact of state Internet control measures on government cybersecurity capacity varies based on the specific control measure and its application. It also showed that monitoring social media and legal frameworks have different effects on the government's cybersecurity capacity in these two groups of countries. A restrictive legal framework for state Internet content regulation was negatively correlated with government cybersecurity capacity in African countries. While this study has provided valuable insights into cybersecurity capacity building in African and developing countries, it also highlights the need for further research to address the identified limitations and explore new avenues for cybersecurity research in the Global South.

Keywords: Government cybersecurity capacity, African countries, developing countries, Internet filtering, Internet shutdown, social media monitoring, Internet regulation, privacy protection, online content regulation, ordinal regression, DSP dataset.

Table of Contents

i. Declaration *2*

ii. Abstract *5*

iii. List of Acronyms *9*

Chapter 1: Introduction *11*

1.1 Problem Statement **12**

1.2 Research Purpose **12**

1.3 Research Questions **13**

1.4 Research Objectives **13**

1.5 Research Hypotheses **13**

1.6 Scope and delimitations **14**

1.6.1 Scope 14

1.6.2 Delimitations 14

1.7 Significance of the study **14**

1.8 Theoretical Framework **15**

1.9 Conceptual Framework **15**

1.9 Methodology overview **15**

2.0 Summary **16**

Chapter 2: Literature Review *18*

2.1 Understanding Cybersecurity **18**

2.2 Cybersecurity and Digital Readiness Indexes **19**

2.2.1 Global Cybersecurity Index 20

2.2.2 National Cyber Security Index 25

2.2.3 Network Readiness Index 29

2.2.3 Cyber Defense Index 30

2.3 Building cybersecurity capacity **32**

2.4 Critical Analysis of Cybersecurity Indices **36**

2.4.1 Methodological Frameworks of Indices 36

2.4.2 Regional and Developmental Considerations 38

2.4.3 Recommendations for Improving Cybersecurity Indices 38

2.4.4 Overview of the Assessment of Cybersecurity Indices 39

2.5 Challenges faced by African and developing countries in building cybersecurity capacity **39**

2.5.1 Resource Constraints 40

2.5.2 Limited Digital Capacity 40

2.5.3 Weak Institutions and Bureaucracy 41

2.5.4 Lack of Comprehensive Policies 41

2.5.5 Political Underpinning 42

2.5.6 Insufficient National Cooperation 42

2.5.7 Insufficient International Cooperation 43

2.6 The securitisation of cyberspace **43**

2.6.1 Securitisation Processes in Cyberspace 44

2.6.2 Cyber Offense and Defense 44

2.6.3 State and Non-State Actors 45

2.6.4 Private Sector Involvement 45

2.6.5 Democratic versus Authoritarian Cyber Securitisation Approaches 46
2.6.6 Western versus Eastern Surveillance Practices 47
2.6.7 African Digital Authoritarianism 48
2.6.8 Theoretical Frameworks from Critical Security Studies and Securitisation Theory 49
2.6.9 Evaluation of CSS and Cyber Securitisation 50

2.7 Theoretical Framework of the Study 51
2.7.1 Foundations of Critical Security Studies 51
2.7.2 Alignment of DSP variables with CSS themes 51

2.8. Conceptual framework of the study 60
2.8.1 Cybersecurity Policy and Strategy 62
2.8.2 Cybersecurity Culture and Society 63
2.8.3 Legal and Regulatory Frameworks 64

2.9 Combination of CSS as the Theoretical Framework and CMM as the Conceptual Framework 70

2.10 Summary 70

Chapter 3: Research Methodology 72

3.1 Research Approach 72

3.2 Data Source 72

3.3 Data Collection and Expert Judgments 73

3.4 Addressing Challenges in Expert-Coded Data 73

3.5 Measurement Model 74
3.5.1 Reliability and Scale Perception 74
3.5.2 Overlapping Coding and Anchoring Vignettes 74
3.5.3 Output and Credible Regions 74

3.6 Data Presentation 74
i. Interval-Level Point Estimates 75
ii. Transformed Interval-Level Estimates 75
iii. Ordinal Versions 75

3.7 Variables used in the study 75

3.8 Data Preparation and Analysis 77

3.9 Justification for using Ordinal Variables 77

3.10 Justification for using Ordinal Logistic Regression Models 78

3.11 Data Categorisation and Model Estimation 80

3.12 Structure of Regression Models 81

3.13 Sub-hypotheses 82

3.14 Ethical Considerations 83

3.15 Limitations 84
3.15.1 Data Limitations 84
3.15.2 Regional Focus 84
3.15.3 Scope Limitations 84
3.15.4 Methodological Limitation 84

3.16 Summary 85

Chapter 4: Results and Discussion 86

4.1 Descriptive Statistics 87
4.1.1 African Countries 87
4.1.2 Developing Countries 92

4.2 Ordinal logistic regression results....96
4.2.1 African countries....96
4.2.2 Developing Countries....103
4.3 Summary of Key Statistical Results....108
4.4 Discussion of Findings....109
4.4.1 Internet Control Mechanisms and Cybersecurity Capacity: Divergent Pathways....110
4.4.2 Social Media Surveillance: The Erosion of Trust and Capacity....114
4.4.3 Legal and Regulatory Frameworks: The Form versus Function Dilemma....116
4.4.4 The Role of Private Actors in Online Content Monitoring and Regulation....117
4.4.5 Integration of the CSS and Oxford GCSCC CMM Frameworks....119
4.4.7 Emerging Questions for Complementary Qualitative Research....120
4.5 Summary....125
Interpretation of Comparative Findings....126
Chapter 5: Conclusion and Recommendations....128
5.1 Summary of Findings....128
5.2 Key Insights and Emerging Questions....129
5.3 Limitations and Implications for Future Research....130
5.3 Directions for Future Research....131
5.5 Conclusion....133
Reference List....134

iii. List of Acronyms

Acronym	Full Term
AI	Artificial Intelligence
AU	African Union
CERT	Computer Emergency Response Team
CIRT	Computer Incident Response Team
CDI	Cyber Defence Index
CMM	Cybersecurity Maturity Model for Nations
CSS	Critical Security Studies
DSA	Digital Services Act
DSP	Digital Society Project
DTS	Digital Transformation Strategy for Africa
DX4D	Digital Transformation for Development
EAC	East African Community
ECOWAS	Economic Community of West African States
GCHQ	Government Communications Headquarters
GCSCC	Global Cyber Security Capacity Centre
GDP	Gross Domestic Product
GDPR	General Data Protection Regulation
GCI	Global Cybersecurity Index
HDI	Human Development Index
ICT	Information and Communications Technology
IMF	International Monetary Fund
INTERPOL	International Criminal Police Organization
ISP	Internet Service Provider
ITU	International Telecommunication Union
LDC	Least Developed Countries
LTE	Long-Term Evolution
NCSI	National Cyber Security Index
NCS	National Cybersecurity Strategy
NRI	Network Readiness Index
NSA	National Security Agency

OECD	Organisation for Economic Co-operation and Development
SADC	Southern African Development Community
UN	United Nations
V-Dem	Varieties of Democracy Institute

Chapter 1: Introduction

This study will investigate the determinants of government cybersecurity capacity in African and developing countries using the sixth version of the Digital Society Project (DSP) dataset. Specifically, it will examine the factors of digital media freedom and state internet regulation within the dataset to identify and analyse their influence on government cybersecurity capacity in African and developing countries.

Over the last three decades, the Internet has established an extensive global network that generates billions of dollars annually for the global economy (Judge et al., 2021). According to Statista (2024), 67 percent of the global population, totalling approximately 5.44 billion people, use the Internet, a result enabled by technological advancements and reduced costs in the field. These factors have increased the accessibility, utility, and performance of the Internet (Tan et al., 2021).

Cyberspace serves as the major platform in which states, individuals, non-governmental organisations, and government bodies engage in economic, commercial, cultural, social, and governmental activities (Li & Liu, 2021). Cyber Security Intelligence (2017) states that cyberspace is a metaphorical area of the Internet that includes all the online activities people perform, including sending emails, browsing websites, and playing games.

Owing to its low entry barrier, lack of transparency, and difficulty tracing the geographical origins of cyber threats, cyberspace has attracted a wide spectrum of entities, including governments, organised crime groups, terrorist organisations, and private citizens. This results in an increase in cyberwarfare, cybercrime, cyberterrorism, and cyberespionage, distinguishing them from traditional national security threats that are typically more visible and carried out by identifiable actors (Li & Liu, 2021). Consequently, conventional national security measures have proven ineffective in cyberspace (Sarker, 2021).

Dutton et al. (2019) coined the term 'cybersecurity' to reflect the shift from emphasising computer security to protecting the extensive network of interconnected devices within the Internet. This shift reflects the evolving landscape of computer security,

highlighting resilience to unpredictable online attacks across all Internet-based environments.

1.1 Problem Statement

Globally, there has been substantial growth in the digitalisation of government operations and services, emphasising the importance of effective cybersecurity in protecting national security, economic stability, and citizen data. Despite the existence of some international standards for cyber-risk management, there remains a lack of international consensus on best practices or policies for cybersecurity capacity building, particularly in developing countries, making it difficult for governments to establish and implement cybersecurity measures (Dutton et al., 2019).

Digital infrastructure is rapidly growing in African countries, resulting in an increase in cyberattacks on critical infrastructure, government institutions, and private companies. According to INTERPOL (2021), more than 90 percent of the continent's businesses operate without the necessary cybersecurity protocols. In 2021, cybercrime reduced GDPs across Africa by 10 percent, resulting in a US$4 billion loss (Odueso, 2022). Notable incidents include the 2016 cyberattack in Liberia, which disrupted a major telecommunications operator's network (Allen, 2021), and the 2021 attack on South Africa's state-owned Transnet, which severely affected port operations (Reva, 2021). These incidents, along with attacks on the Nigerian National Security Agency and one of South Africa's major municipal governments, underscore the cyber vulnerabilities of these countries and the repercussions of inadequate cybersecurity capacity (Allen, 2021).

Addressing these cybersecurity vulnerabilities is crucial for creating a more secure and strong digital infrastructure, which will contribute to economic and social progress in African and developing countries. Understanding the determinants of government cybersecurity capacity in African countries is crucial for policymakers, international organisations, and stakeholders aiming to enhance cybersecurity capacity across the continent.

1.2 Research Purpose

The purpose of this study is to investigate the determinants of government cybersecurity capacity in African and developing countries. Specifically, this research

aims to identify the factors influencing government cybersecurity capacity, focusing on aspects such as state Internet regulation capacity and approach and digital media freedom.

1.3 Research Questions

The primary aim of this study is to answer the question: *what are the determinants of government cybersecurity capacity in African and developing countries?*

The secondary research question for this study is: *what is the effect of the determinants on government cybersecurity capacity?*

1.4 Research Objectives

- To identify the determinants of government cybersecurity capacity in African and developing countries.
- To determine the effects of the determinants of government cybersecurity capacity in African and developing countries.

1.5 Research Hypotheses

This study has three main research hypotheses, which are outlined below.

Hypothesis 1: Internet control measures and cybersecurity capacity
African and developing countries with stronger Internet control measures (filtering and shutdown capacities and practices) are more likely to have higher government cybersecurity capacity.

Hypothesis 2: Social media regulation and cybersecurity capacity
African and developing countries that actively regulate and monitor social media (shutdowns, monitoring, and censorship) are less likely to demonstrate higher government cybersecurity capacity.

Hypothesis 3: Legal and regulatory framework and cybersecurity capacity
A robust legal and regulatory framework, including data privacy protection and laws protecting online political speech, is positively correlated with higher government cybersecurity capacity in African and developing countries.

1.6 Scope and delimitations

1.6.1 Scope

This study employs a quantitative analysis of the sixth version of the DSP dataset, spanning from 2000 to 2023, to identify the factors that influence government cybersecurity capacity. The primary focus is on African countries because of their distinct vulnerabilities to cyber threats, as exemplified by incidents in Liberia, South Africa, Nigeria, and other countries (Allen, 2021; Odueso, 2022; Reva, 2021). In addition, the research will incorporate studies from other developing countries to identify common challenges and aggregate trends, thereby contributing to a more comprehensive comprehension of cybersecurity capacity-building in the Global South. Specifically, this study will examine the influence of state internet regulation capacity, as well as digital media freedom, on government cybersecurity capacity.

1.6.2 Delimitations

This study will specifically focus on African and developing countries, excluding an examination of government cybersecurity capacity in developed countries, as these countries face distinct challenges due to limited resources, rapid digitisation, and evolving cyber threats. In addition, the research will exclusively use the DSP dataset, excluding any other data sources. The analysis will not examine differences in cybersecurity capacity between African and developing countries, nor will it assess the cybersecurity capacity of individual countries within these regions. The study will not conduct a comparative analysis of the discussed cybersecurity and digital readiness indexes, as the emphasis is on analysing the determinants of government cybersecurity capacity rather than benchmarking African and developing countries against existing frameworks.

1.7 Significance of the study

This study aims to contribute to a deeper understanding of cybersecurity challenges and opportunities confronting African and developing countries, with the goal of providing valuable insights for policymakers and stakeholders by identifying the key determinants of government cybersecurity capacity. The findings are expected to guide efforts to address critical areas that require attention and investment in state Internet regulation and digital media freedom, which may lead to the improvement of cybersecurity capacity in these regions. This research seeks to contribute to

developing cybersecurity capacity in African and developing countries and strengthening their resilience to cyber threats.

Additionally, the study contributes to the broader academic discourse on cybersecurity, particularly by providing a perspective on cybersecurity capacity building in African and developing countries, which are often underrepresented in global cybersecurity research. The focus on state Internet regulation capacity and approach, digital media freedom, and their influence on government cybersecurity capacity provides a nuanced understanding of the Internet's political and social factors that shape cybersecurity policies and practices in African and developing countries.

1.8 Theoretical Framework

This study uses Critical Security Studies (CSS) to explore how and why countries securitise digital threats, expand surveillance, and construct cybersecurity capacity as a response to perceived risks, which justifies the selection of DSP variables related to filtering, shutdown, social media monitoring, privacy law, and regulatory capacity.

1.9 Conceptual Framework

This study uses the DSP dataset and the Oxford Global Cyber Security Capacity Centre's (GCSCC's) Cybersecurity Maturity Model for Nations (CMM) as a conceptual framework. It specifically examines the effect of digital media freedom and state Internet regulation capacity and approach on government cybersecurity capacity in African and developing countries. The DSP variables, such as Internet filtering, Internet shutdown, social media monitoring, privacy law, and regulatory capacity, correspond with the core dimensions of the Oxford GCSCC's CMM, thereby providing justification for the selection of these variables.

1.9 Methodology overview

The research methodology employs a quantitative analysis, utilising regression models to determine the factors influencing government cybersecurity capacity in African and developing countries. The nine variables used in the study are obtained from the sixth version of the DSP dataset.

2.0 Summary

This introductory chapter has established the importance of cybersecurity capacity in African and developing countries in the context of increasing digitalisation and evolving cyber threats. The chapter has shown that whilst the Internet has created substantial economic value and enabled unprecedented connectivity—with 67 percent of the global population now online—cyberspace's accessibility and lack of transparency have made it vulnerable to exploitation by both state and non-state actors. This vulnerability has required a shift in security thinking from traditional national defence approaches towards comprehensive cybersecurity systems capable of protecting interconnected digital infrastructure.

The problem statement has highlighted the serious cybersecurity challenges facing African countries, where rapid digital infrastructure growth has exceeded the development of adequate cybersecurity measures. With over 90 percent of African businesses operating without proper cybersecurity protocols, the continent experienced a 10 percent GDP reduction in 2021 due to cybercrime, totalling US$4 billion in economic losses. Major cyberattacks on critical infrastructure in Liberia, South Africa, and Nigeria have demonstrated the severe operational and economic consequences of insufficient government cybersecurity capacity, establishing the practical need for this investigation.

This study addresses the identified research gap by investigating the determinants of government cybersecurity capacity in African and developing countries, with particular focus on state Internet regulation capacity and approach, and digital media freedom. Through analysis of the Digital Society Project dataset (2000–2023), the research examines three main hypotheses concerning the relationships between Internet control measures, social media regulation, legal and regulatory frameworks, and government cybersecurity capacity. The research objectives focus on identifying key determinants and analysing their effects on cybersecurity capacity development across these regions.

The study is limited to African and developing countries, recognising their distinct challenges relating to resource constraints, rapid digitalisation, and evolving cyber

threats that differ from developed country contexts. By using CSS as the theoretical framework and the Oxford GCSCC's CMM as the conceptual framework, this research provides analytical tools for examining how countries respond to digital threats and build cybersecurity capacity. The variables selected from the DSP dataset—including Internet filtering, Internet shutdowns, social media monitoring, privacy law, and regulatory capacity—correspond directly with core dimensions of cybersecurity maturity, providing justification for the research design.

The significance of this study extends beyond immediate policy implications for African and developing countries. By providing empirical analysis in an under-researched area of global cybersecurity, this investigation seeks to inform evidence-based capacity-building strategies whilst contributing to academic discussion on the political, social, and regulatory determinants of cybersecurity in the Global South. The subsequent chapters will systematically examine relevant literature, outline the methodological approach, present findings, and discuss their implications for cybersecurity governance and capacity development in African and developing countries.

Chapter 2: Literature Review

The literature review provides a comprehensive understanding of the current state of cybersecurity in African and developing countries by analysing existing cybersecurity indices and the challenges faced by these countries. The Global Cybersecurity Index (GCI) and the National Cyber Security Index (NCSI) assess the cybersecurity capabilities of countries, whereas the Network Readiness Index (NRI) evaluates a country's readiness to capitalise on ICT potential for economic and social development. Additionally, the Cyber Defense Index (CDI) focuses on the digital preparedness of the world's leading economies, and can serve as a benchmark for developing countries can potentially achieve. Together, these indices enable governments, policymakers, academia, and cybersecurity specialists to monitor progress, identify gaps, and prioritise areas for improving cybersecurity capacity.

Furthermore, the theoretical and conceptual framework sections establish a foundation for subsequent quantitative analysis by focusing on CSS and the Oxford GCSCC's CMM dimensions and identifying relevant proxy measures within the DSP dataset. By methodically analysing the Oxford GCSCC's CMM and the DSP dataset, the researcher identified factors influencing government cybersecurity capacity in African and developing countries.

2.1 Understanding Cybersecurity

According to Creese et al. (2021), the widespread adoption and increasing significance of Information and Communication Technologies (ICTs) have raised concerns about the security of digital devices, data, networks, platforms, and ICT services, commonly referred to as digital security or cybersecurity. Cybersecurity is defined as "the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to protect the cyber environment, organisations, and users' assets" (ITU-T, 2008, p. 2).

Cybersecurity helps safeguard online data and applications from cyber threats, whereby malicious actors aim to gain access, amend, or erase sensitive information, extract funds from users, or disrupt the routine operations of businesses or

governmental entities. Common threats encompass malware, ransomware, social manipulation, phishing, and an array of others, posing a challenge to maintaining data security given the rapid rate of technological advancement.

In numerous African countries, the absence of cybersecurity laws and mechanisms is evident, exposing businesses to cyber threats and attacks. According to INTERPOL (2021), most African countries lack sufficient cybersecurity frameworks, with almost 90 percent of African businesses deficient in essential security measures to safeguard themselves. This insufficiency raises vulnerability to cyberattacks, potentially resulting in significant financial repercussions for these countries (INTERPOL, 2021). Consequently, the enhancement of cybersecurity capacity is increasingly recognised as a dependable strategy to tackle cybersecurity issues (Creese et al., 2021a).

2.2 Cybersecurity and Digital Readiness Indexes

In the existing digital environment, organisations have designed various cybersecurity indices to quantify cybersecurity, which serves as a framework for assessing cybersecurity initiatives, comparing performance, and pinpointing areas for development. This metric incorporates basic security metrics, control enablers, and capability tiers to efficiently assess the cybersecurity preparedness of countries. Moreover, the evaluation conducted by cybersecurity indexes delves into the notion of cyber risk from a diverse standpoint, considering not only the various existing threats but also the readiness of different nations, thus revealing the influence of socioeconomic factors such as the human development index (HDI), GDP, level of democracy, and state of peace on the overall levels of cyber risk. By utilising these specified metrics, both organisations and policymakers have gained valuable insights into the efficacy of their cybersecurity measures, allowing them to prioritise areas for enhancement and adapt their strategies to effectively combat and mitigate the risks posed by cyber threats within an ever-changing digital landscape (Malaivongs et al., 2022).

Among many existing indices, the GCI and the NCSI are two of the most notable cybersecurity indices that offer a mechanism for capacity building and a method to monitor progress for governments, policymakers, academia, and cybersecurity specialists. This discussion primarily focuses on these two indices due to their

comprehensive methodologies, global recognition, and relevance to the objectives of this study. Additionally, the other two indices were chosen for their distinctive approaches to evaluating cybersecurity readiness and resilience, which provide an understanding of the challenges advanced economies and developing countries face in boosting their cybersecurity capabilities.

2.2.1 Global Cybersecurity Index

The Global Cybersecurity Index (GCI) evaluates levels of cybersecurity development or involvement across five pillars for each country, namely legal measures, technical measures, organisational measures, capacity development, and cooperation, to assess the degree of cybersecurity development or participation in each country (Bruggemann et al., 2022; International Telecommunications Union, 2021a). The GCI is extensively acknowledged as a leading cybersecurity index that evaluates the extent of cybersecurity maturity and is actively employed by various countries to oversee their cybersecurity development (Mckinsey & Company, 2020). Mauritius was ranked 17th out of 194 countries, the highest-ranked position among African countries in the 2020 GCI report (International Telecommunications Union, 2021a). Egypt ranked 23rd and Tanzania 37th Ghana (43rd), Tunisia (45th), Morocco (50th), Benin (56th), Rwanda (57th), South Africa (59th), and Botswana (88th) were among the top ten ranked African countries (International Telecommunications Union, 2021a).

i. Legal Measures

The criteria for legal measures examine the laws that countries have in place to combat malicious cyber activities and the legislation that countries are developing to counter malicious cyber activities (International Telecommunications Union, 2021a). Notably, numerous countries have established data privacy protection laws, with 133 countries having passed such laws, while 15 are in the process of doing so, and 46 do not have any data privacy protection laws (International Telecommunications Union, 2021a). The 2020 GCI report found that 11 out of 44 African countries lacked legislation related to data protection, while 24 out of the 44 African countries had no legislation or policy for data breach and incident notification (International Telecommunications Union, 2021a). This highlights the necessity for African countries to accelerate the drafting and adoption of far-reaching data protection legislation and

regulations to safeguard the confidentiality and integrity of citizens' personal information.

Most countries have laws prohibiting illegal access, with few noticeable regional variations. 100 countries had established laws that consider online harassment and abuse illegal, whereas seventeen other countries were still busy legislating similar laws, and 77 countries did not have any laws prohibiting illegal access (International Telecommunications Union, 2021a). It was found that 50 percent of African countries had no online harassment laws.

ii. Technical Measures

The technical measures pillar examines the technical infrastructure of countries concerning monitoring, detecting, and responding to cyber threats and incidents (International Telecommunications Union, 2021a). Governments rely on Computer Incident Response Teams (CIRTs) to provide a unified point of contact to address nationwide cyber incidents. They facilitate prompt and well-organised measures, enabling countries to glean valuable insights from previous errors and reinforce their robustness in the face of digital threats (International Telecommunications Union, 2020). National CIRTs are often initiated and executed based on the laws and policies of countries. Typically, CIRTs are supervised by a specific department or governmental organisation. However, when a country is constrained by a budget to establish a national CIRT, it outsources CIRT operations to private companies.

Despite notable advancements in establishing CIRTs, numerous countries, especially those with limited resources, still grapple with substantial obstacles. The primary obstacles include inadequate funding, insufficient understanding of technology and cybersecurity, limited research and development, and difficulties in prioritising efforts amidst complex political landscapes. These challenges can significantly impede the effective implementation of technology to combat cybersecurity threats.

The 2020 GCI report uncovered a concerning trend amongst African countries, where more than half of the countries surveyed (23 out of 44) lacked a national CIRT. Moreover, a staggering 80 percent of these countries did not have a sector-specific CIRT in place. This underscores the urgent need for increased investment, capacity building, and international collaboration to support the development of CIRTs in these

African countries. By doing so, these countries can bolster their cybersecurity capabilities and respond more effectively to emerging threats.

iii. Organisational Measures

This pillar analyses the organisational measures, administration, and regulations of cybersecurity in countries (International Telecommunications Union, 2021a). Cybersecurity should be kept at the primary level of the administrative branch, and various state bodies should be assigned specific responsibilities for their country's cybersecurity responses. A national cybersecurity strategy (NCS) usually serves as the foundational element of organisational measures at the state level. The NCS is a collaborative framework involving multiple stakeholders that enables collaboration among government organisations, civil society organisations and private enterprises to effectively respond to work together in the wake of cyber incidents and prevent them (International Telecommunications Union, 2021a). The 2020 GCI report found that nearly 90 percent of African countries did not regularly update or modify their NCS frameworks to address the continuously changing cybersecurity threats and needs (International Telecommunications Union, 2021a). Additionally, about 77 percent of these African countries did not conduct national cybersecurity audits (International Telecommunications Union, 2021a).

With the rise of cyberattacks on critical infrastructure such as power grids, water treatment facilities, and transportation systems, it has become increasingly important to prioritise risk management measures aimed at reducing the likelihood and impact of serious incidents. Protecting critical infrastructure against cyber threats has become a dominant concern in national security agendas. However, a substantial number of countries have neglected critical infrastructure protection in their overall security frameworks. Significantly, half of the African countries (22 out of 44 countries) analysed in the 2020 GCI study did not address either critical infrastructure or cybersecurity resilience (International Telecommunications Union, 2021a).

iv. Capacity Building

The capacity-building pillar examines the accessibility and quality of cybersecurity education, research, and development programmes in the country (International Telecommunications Union, 2021a). Least developed countries (LDCs), which performed below par on the GCI, are often faced with a higher likelihood of

encountering limitations in resources while attempting to bridge the gap in their cybersecurity capabilities. Their capacity to safeguard their ICT systems may have been hindered by various factors, exhibiting a gap in specialised competencies and expertise, policy constraints, and a deficiency in ICT skills. While many African countries struggled with development, Tanzania, Rwanda, and Benin showed notable progress. These three countries possess a robust cybersecurity sector that was entirely domestically designed and developed (International Telecommunications Union, 2021a).

More countries added cybersecurity courses to their national primary and secondary educational curricula after the publication of the 2018 GCI report (International Telecommunications Union, 2021a). By the time the 2020 GCI study was completed, only a small proportion of countries (slightly above five percent) had taken the initiative to integrate basic online safety lessons into their primary school curricula, empowering young children to navigate the digital world safely. Furthermore, over seven percent of countries had incorporated cybersecurity-related resources into their secondary education programs, providing aspiring cybersecurity professionals with future career opportunities (International Telecommunications Union, 2021a). The reports above findings on the implementation of cybersecurity educational curricula did not exclusively focus on African countries.

Even though the 2020 GCI report does not exclusively mention African countries, it found that most countries (over 60 percent) have made concerted efforts to enhance cyber awareness among varying-sized entities, including smaller businesses, mid-sized companies, large corporations, public sector organisations, and government bodies (International Telecommunications Union, 2021a). This is a notable improvement compared to the 38 percent of countries that had not previously undertaken any cybersecurity awareness initiatives. These efforts involved providing valuable resources through national CIRTs, educating target audiences on essential online safety practices and cybersecurity standards, and offering network security solutions to support their cybersecurity posture (International Telecommunications Union, 2021a).

Even though the 2020 GCI report does not exclusively mention African countries, it found that 46 percent of countries provided national sector-specific cybersecurity

training to public sector and government officials (International Telecommunications Union, 2021a). A substantial majority of countries (80 percent) had initiated cybersecurity capacity-building programmes for ICT professionals, including those in small and medium-sized enterprises and the private sector. These training initiatives were delivered through various channels, including national CIRTs, national cybersecurity centres, and recognised courses that are offered by regional and international institutions. While some countries aim to significantly increase their pool of cybersecurity professionals, they face challenges in providing nationally funded training programmes. Instead, they rely on international training opportunities offered by reputable cybersecurity certification organisations. These organisations provide valuable training and certification programs that help bridge the skills gap in the cybersecurity workforce (International Telecommunications Union, 2021a).

v. Cooperation

The fifth pillar, cooperation, evaluates countries' participation in international information-sharing and collaboration initiatives (International Telecommunications Union, 2021a). Due to the digital landscape being borderless, collaboration is an essential strategy in addressing cybersecurity. Safeguarding the global cyber ecosystem requires collaboration at national, regional, and international levels as no single entity can ensure its security. Collaboration efforts involve countries with bilateral and multilateral agreements, as well as those involved in interagency and public-private partnerships. Bilateral and multilateral agreements play a vital role in setting norms and fostering international cooperation in cybersecurity. The primary objectives of cybersecurity collaboration include standardising minimum-security measures, sharing information and best practices, and establishing norms of behaviour (International Telecommunications Union, 2021a).

The 2020 GCI report indicated that 90 countries, not exclusively African countries, had negotiated bilateral cybersecurity agreements focusing on capacity development and information sharing. A total of 37 countries had bilateral agreements that encompassed the exchange of information and capacity-building initiatives but stopped short of providing mutual legal assistance. In the context of the 2020 GCI study, multilateral agreements are defined as those that engage three or more countries, distinct from broader international treaties such as the Budapest Convention

on Cybercrime (International Telecommunications Union, 2021a). A significant majority of countries, 57 percent, had already committed to multilateral agreements, whereas 46 countries had opted for bilateral agreements. Furthermore, 99 countries had signed or ratified multilateral agreements that prioritise information sharing and capacity building. 10 out of 44 African were participating in bilateral cybersecurity agreements whereas 19 African countries were participating in multilateral cybersecurity agreements (International Telecommunications Union, 2021a).

Beyond formal agreements, participation in international activities has significantly enhanced cybersecurity practices. Over 140 countries, not exclusively African countries, had engaged in a variety of cybersecurity-related activities, including international conferences, capacity-building workshops, bilateral partnerships, and multilateral conventions. These engagements provided opportunities for countries to learn about effective practices and new approaches to addressing cybersecurity threats. The 2020 GCI report highlighted that 86 countries, not exclusively African countries, are engaged or soon will be engaged in international or domestic public-private partnerships focusing on facilitating intelligence sharing, good practice exchanges, and communication of research and development needs.

Countries have also taken steps to strengthen their cybersecurity ecosystems by organising conferences and workshops and contracting private sector companies to develop training programmes for the public sector. A growing number of countries are developing science and technology parks, which serve as hubs for collaboration between the private and public sectors. These initiatives aim to build a comprehensive cybersecurity ecosystem (International Telecommunications Union, 2021a).

2.2.2 National Cyber Security Index

The National Cyber Security Index (NCSI) measures a country's ability to manage cyber threats. Experts calculate the NCSI score, which reflects the proportion of the highest achievable value a country has attained on each indicator, by considering both the country's digital development level and the relative importance of each cybersecurity measure (e-Governance Academy, n.d.).

The NCSI has utilised a group of 12 capacities split into three categories: strategic, preventative, and responsive (E-Governance Academy, n.d.-b). These categories

encompass 49 indicators to assess 176 countries' readiness to manage cyber threats and incidents. Despite its global scope, only 37 African countries have been analysed in the NCSI report. Morocco ranked the highest in Africa and 32nd out of 176 countries, with a score of 70.13 out of 100, followed by Benin (58th) with a score of 58.44 and Egypt (61st) with a score of 57.14. Conversely, South Sudan ranked the lowest overall in Africa, with a score of 1.30 out of 100 (e-Governance Academy, 2023).

i. Strategic Cybersecurity Indicators

The strategy cybersecurity category assesses the cybersecurity policy, global cybersecurity contribution, education and professional development, and countries' cybersecurity research and development capacities (E-Governance Academy, n.d.-b).

Cybersecurity Policy Capacity

The cybersecurity policy capacity area evaluates a country's ability to establish a unified and comprehensive cybersecurity strategy, ensuring a well-planned and coordinated approach to addressing cyber threats by evaluating high-level leadership, policy development, coordination, and the articulation of a national cybersecurity action plan. Effective governance frameworks and national strategies are deemed to be essential for managing digital risks and enhancing cybersecurity resilience (E-Governance Academy, n.d.-b).

Global Cybersecurity Contribution Capacity

The global cybersecurity contribution capacity area evaluates a country's participation in international collaborations aimed at developing a secure cyber ecosystem through cooperative diplomacy and initiatives to build capacity that promotes global cyber resilience and peaceful online interactions (E-Governance Academy, n.d.-b).

Education and Professional Development Capacity

The education and professional development capacity area assesses whether a country has a formal cybersecurity education and professional development system. It emphasises the significance of teaching children basic digital skills and cyber literacy as a foundational step towards higher education. Long-term educational opportunities are vital for developing a competent and experienced workforce in ICT and cybersecurity through the regular production of ICT professionals. In addition, the programme includes expert and interservice collaboration, with a focus on effective

techniques that can substantially enhance a country's cybersecurity capacity (E-Governance Academy, n.d.-b).

Cybersecurity Research and Development Capacity

The capacity area of cybersecurity research and development evaluates a country's ability to foster research and development in the field of cybersecurity. It considers the incentives to encourage innovation and create a space that improves cybersecurity capabilities. Countries fund researchers to help improve their technological resilience against emerging risks and shape the overall cybersecurity environment (E-Governance Academy, n.d.-b).

ii. Preventative Cybersecurity Indicators

The prevention capacity area evaluates whether a country can prevent cyber risks in its digital ecosystem (including cloud services and supply chains). This includes threat assessments and increasing cybersecurity awareness. As technology continues to evolve and become increasingly intertwined with our daily lives, the likelihood of cyber threats and vulnerabilities has also grown. Therefore, it is essential to identify and comprehend the nature of these threats, as well as the underlying factors that exacerbate or mitigate them and the potential fallout that can result (E-Governance Academy, n.d.-b).

Cybersecurity of Critical Information Infrastructure Capacity

The cybersecurity critical infrastructure capacity reflects a nation's ability to form and administer its information structures, particularly those that have the potential to compromise a country's health, safety, security, or financial status. Competent risk management and regulatory measures are essential for ensuring the resilience of critical infrastructure. Competent risk management and regulatory measures are essential for ensuring the resilience of critical infrastructure (E-Governance Academy, n.d.-b).

Cybersecurity of digital enablers capacity

This capacity area examines national digital procedures to protect key digital infrastructures, such as electronic identity and trust services. The security and dependability of such digital systems are critical for ensuring the continuity of

government and administrative activities as well as facilitating trusted digital transactions (E-Governance Academy, n.d.-b).

Cyber threat analysis and awareness-raising capacity

This capacity area encompasses collecting, examining, and disseminating cyber threat intelligence. Its primary goal is to educate the public about cybersecurity risks and provide actionable insights to diverse stakeholders, enabling them to bolster their defence against potential threats (E-Governance Academy, n.d.-b).

Protection of personal data

The capacity area of protection of personal data concentrates on safeguarding online privacy and personal data and assessing the cyber-related dimensions of national data protection laws and their implementation frameworks. Ensuring robust data protection laws and organisational accountability is crucial for safeguarding individuals' privacy in cyberspace (E-Governance Academy, n.d.-b).

iii. Responsive Cybersecurity Indicators

The responsive category assesses a country's ability to identify, address, and recover from cyber incidents and crimes (E-Governance Academy, n.d.-b). Cyber operations and cyberspaces are increasingly integral to modern warfare. The United Nations (UN) Charter upholds the principle of self-defence, allowing states to protect themselves individually or collectively in the event of an armed attack. Cyber defences are being strengthened as a vital component of national defence, with numerous countries establishing dedicated cyber units for military operations. As cyber defence units become a standard component of national defence agencies, governments must ensure that they fully comply with International Humanitarian Law (E-Governance Academy, n.d.-b).

Cyber incident response capacity

The cyber incident response capacity area assesses developing and maintaining national capacities comprising prevention, detection, response, and recovery from cybercrime. It underlines the necessity of having a working CIRT at the national level (E-Governance Academy, n.d.-b).

Cyber crisis management capacity

The cyber crisis management capacity area assesses a country's preparedness to counter extensive cyber incidents or cyber-induced crises. It inspects the inclusion of cyber risks in the national crisis plan, crisis management implementation, and readiness to involve other stakeholders in the government's crisis management functions (E-Governance Academy, n.d.-b).

Fight against cybercrime capacity

This capacity area examines the extent and seriousness of a country's response towards cybercrime in terms of legislation and organisational structure, as well as cooperation with other countries (E-Governance Academy, n.d.-b).

Military cyber defence capacity

This capacity area focuses on the development of military cyber defence capabilities to safeguard national sovereignty, territorial boundaries, and constitutional stability against external threats. It assesses the establishment of military cyber bodies, rules, supervision, and the conduct of military cyber protection exercises (E-Governance Academy, n.d.-b).

2.2.3 Network Readiness Index

The Network Readiness Index (NRI) assesses a country's preparedness to utilise opportunities from ICT for economic and social growth (Portulans Institute, 2023b). Although it is not specifically a cybersecurity index, the NRI evaluates the preparedness of critical ICT against cyber threats (Portulans Institute, 2023b).

The NRI examines four pillars: technology, people, governance, and impact. The technology pillar evaluates the status of the country's ICT sector. The people pillar assesses the implementation of ICT by persons, companies, and authorities. The governance pillar analyses the country's policies and regulations regarding the use of ICT. The impact pillar focuses on the relativity of ICT usage regarding economic and social consequences. By providing a detailed assessment of these dimensions, the NRI serves as a valuable tool for policymakers and stakeholders to benchmark digital competitiveness, identify areas for improvement, and track progress over time (Portulans Institute, 2023b).

According to the 2023 NRI rankings, which analyses 134 countries, the most network-ready societies are predominantly in Europe (17 of the top 25 ranked countries), certain regions of Asia and the Pacific (with Singapore ranking second overall), and North America (with the United States ranking first overall). All three of these top-ranked countries are high-income countries. Conversely, the highest-ranked low-income countries are from Africa: Rwanda (99th), Uganda (117th), and Gambia (120th). The disparity in rankings between high and low-income countries underlines the importance of cybersecurity capacity building, as resource constraints often contribute to lower cybersecurity capacity for low-income countries. The highest-ranked African countries are Kenya (70th), South Africa (74th), and Mauritius (76th) (Portulans Institute, 2023a).

2.2.3 Cyber Defense Index

The Cyber Defense Index (CDI) evaluated the cybersecurity preparedness of the 20 largest and most digitally progressive economies. The assessment used four key pillars to gauge cybersecurity readiness, which encompassed evaluating critical infrastructure, cybersecurity resources, organisational capabilities, and adherence to policy guidelines (O'Brien, 2022).

i. Critical Infrastructure

This pillar investigates the reliability of telecommunication networks and the security of digital resources to enable essential economic activity. The indicators of this pillar measure ICT infrastructure capacity, the number of data centres per million people, secure Internet services per million people, Internet server infrastructure assets in each country, and the perceived resilience and security of critical infrastructure assets. The critical infrastructure pillar contributes 30 percent of the overall CDI score (O'Brien, 2022).

ii. Cybersecurity Resources

This pillar assesses the technological and legal measures in place in each country to safeguard cybersecurity assets, prohibit unauthorized access, and enforce cybersecurity standards. Indicators include a country's cybersecurity commitments, data privacy and protection legislation, and the effectiveness of organisational cybersecurity capabilities such as data analytics, Artificial Intelligence (AI), blockchain,

anti-phishing, and anti-ransomware. The cybersecurity resources pillar contributes 35 percent of the overall CDI score (O'Brien, 2022).

iii. Organisational Capacity

This pillar assesses institutions' digital maturity and expertise by incorporating conventional cybersecurity principles into operations in each country. The indicators examine the effectiveness of digital involvement among all stakeholders, governments' readiness to use AI technology in public services, and their knowledge of AI and cybersecurity implementation. The organisational capacity pillar contributes 20 percent of the overall CDI score (O'Brien, 2022).

iv. Policy Commitment

This pillar evaluates the effectiveness and quality of cybersecurity regulation, as well as the government's commitment to supporting resilient cybersecurity practices, which includes laws and regulations, public-private collaboration, and involvement in global Computer Emergency Response Team (CERT) programmes. The indicators assess regulatory quality, government efficiency in providing public services and implementing policies, and corporate perceptions of regulatory reliability. The policy commitment pillar contributes 15 percent of the overall CDI score (O'Brien, 2022).

The CDI report highlights that high-ranking countries such as Australia and the Netherlands have shown a strong commitment to cybersecurity through investments in digital infrastructure, data privacy regulations, and coordinated agencies. It further emphasises the need for both robust cybersecurity measures and a favourable policy environment that fosters innovation and growth (O'Brien, 2022).

Seven developing countries, none of which are African, qualified for the CDI 2022/2023 rankings. These countries included China, Saudi Arabia, Mexico, India, Brazil, Turkey, and Indonesia. These developing countries ranked in the lower tier of the CDI rankings which suggests that they encounter more challenges in strengthening and maintaining their digital infrastructure than developed countries. The report mentions China as an example for how excessive internet control can hinder innovation and economic growth, potentially negatively impacting long-term cybersecurity preparedness (O'Brien, 2022).

The CDI report proposes that these developing countries need to transition from long-term evolution (LTE) networks to fifth-generation (5G) networks to improve their cybersecurity capacity (O'Brien, 2022). However, transitioning from LTE to 5G networks requires substantial financial investments and technically competent organisations to assist with this process. Further research and analysis beyond the scope of the CDI is imperative for obtaining a more comprehensive understanding of the cybersecurity capacities of developing countries.

2.3 Building cybersecurity capacity

The Oxford GCSCC developed the CMM, which provides detailed guidelines to attain various levels of cybersecurity capacity (Creese et al., 2021). The CMM also enables researchers and policymakers to assess a country's cybersecurity capacity across five critical dimensions: cybersecurity policy and strategy; cybersecurity norms and practices; building cybersecurity knowledge and capabilities; legal and regulatory framework; and standards and technologies (Global Cyber Security Capacity Centre, 2021).

The cybersecurity policy and strategy dimension examine a country's ability to formulate and implement cybersecurity strategies, as well as bolster its cybersecurity resilience by enhancing incident response, cyber defence, and protection of critical infrastructure. This dimension focuses on the effective development and implementation of national cybersecurity strategies while upholding the advantages of a secure cyberspace crucial for government operations, international commerce, and societal well-being (Global Cyber Security Capacity Centre, 2021).

The cybersecurity culture and society dimension evaluate key aspects of promoting a responsible cybersecurity culture, which includes cyber risks in society, levels of trusts in online services, e-government, and e-commerce, as well as individuals' understanding of safeguarding personal information on the Internet. Furthermore, this dimension examines the presence of reporting systems for individuals to report cybercrimes, along with the impact of media and social media in shaping attitudes, values, and behaviours related to cybersecurity (Global Cyber Security Capacity Centre, 2021).

The building cybersecurity knowledge and capabilities dimension assesses the availability and quality of cybersecurity programs for different stakeholders, focusing on public awareness-raising, educational programs, and professional training opportunities (Global Cyber Security Capacity Centre, 2021).

The legal and regulatory framework dimension scrutinises the government's ability to develop and enforce national laws relevant to cybersecurity, focusing on regulatory mandates, cybercrime legislation, and associated legal frameworks. This dimension also examines the implementation and enforcement of cyber laws through law enforcement agencies, prosecution mechanisms, regulatory bodies, and court systems, while considering formal and informal cooperation mechanisms to combat cyber threats (Global Cyber Security Capacity Centre, 2021).

The standards and technologies dimension analyses the use of cybersecurity technology to protect individuals, organisations, and infrastructure. It also examines the implementation of standards, development of technologies, and the importance of a structured and comprehensive framework for cultivating cybersecurity expertise through education and continuous professional growth (Global Cyber Security Capacity Centre, 2021).

By 2020, the CMM had collected a substantial amount of data, enabling a comprehensive examination of the effects of varying degrees of capacity development. A total of 73 countries, representing every continent, had undergone CMM evaluations. The study investigated whether capacity development had an evident influence on the rate of Internet adoption among individuals, governments, and businesses. Upon examining capacity-building efforts across the 73 countries, a notable trend emerged: most countries were still in the early phases of development (Creese et al., 2021). This finding is important, as it underscores the widespread need for capacity-building initiatives, particularly in consideration of the study's findings on the positive correlations between capacity-building and increased Internet adoption (Creese et al., 2021).

The CMM study found a wide range of cybersecurity capabilities among the countries that were studied, rather than a simple division between those with and without capacity. Instead, there are subtle variations in capacity that are linked to a country's

economic status and Internet penetration. Notably, a country's wealth, which is measured by GDP per capita, has a dual impact on capacity-building. On one hand, it facilitates capacity development, and on the other hand, it amplifies the benefits of Internet adoption. This means that economic progress inadvertently exacerbates the disparities in capacity-building and ultimately, the outcomes of countries. While a country's wealth can facilitate capacity-building and unlock the economic and opportunity benefits associated with Internet use, it is not a guarantee of these outcomes. In fact, some countries may experience faster-than-expected capacity growth, while others may lag behind projections, despite their wealth. These findings build upon existing research, such as the World Bank's development report, which highlights the potential benefits of bridging the gap to digital access. Moreover, the evidence suggests that merely increasing Internet access is not enough; improving cybersecurity is also crucial, as it significantly impacts the functionality of Internet use (The World Bank, 2016). Therefore, traditional initiatives aimed at bridging the digital divide can be enhanced by national and international efforts to develop cybersecurity expertise, thereby ensuring that the benefits of Internet adoption are fully realised (Creese et al., 2021).

Another crucial aspect is that national cybersecurity infrastructure development initiatives have a profound impact on ICT adoption and use, as well as people's perceptions of freedom and accountability. Notably, the development of cybersecurity capabilities has a robust, statistically significant, and positive effect on overall ICT use, even when controlling for variables such as national wealth, which could otherwise explain the extent of individual, commercial, and governmental ICT adoption. This finding was supported by a rigorous multivariate analysis, which employed both simple linear regressions and more nuanced path modelling to examine the relationships between all the variables in the theoretical model (Creese et al., 2021).

Finally, the study's findings emphasised the need for intensified global efforts to enhance cybersecurity capacity. The observed statistical relationships strongly underscore the value of cybersecurity capacity building, which may be even more critical in countries where Internet use is more pervasive and integral to daily life. To address the global cybersecurity capacity gaps highlighted in the study, national and international authorities were recommended to prioritise initiatives aimed at building

broader cybersecurity capacity. Any reduction in cybersecurity capacity in one country puts every country at risk, as the global nature of the Internet means that vulnerabilities in one region can have far-reaching consequences. Therefore, a collective and coordinated approach to cybersecurity capacity-building is essential to mitigate these risks and ensure a safer and more secure digital environment for all (Creese et al., 2021).

The increasing importance of cybersecurity has prompted governments and international organisations to prioritise the development of countries' capabilities to defend against cyber threats (Creese et al., 2021). These efforts encompass a spectrum of strategies, ranging from educational initiatives and technical advancements to the establishment of new legal and policy frameworks. Despite the intuitive value of these proactive measures, empirical research on their effectiveness remains scarce due to their relative novelty.

Creese et al (2021) adopted a cross-national comparative approach to assess the empirical basis for investing in cybersecurity capacity-building. Drawing on field research for 73 countries, the comparative analysis accomplished three main objectives: it provided an overview of the status of cybersecurity capacity-building globally; it evaluated the impact of capacity-building initiatives while accounting for alternative contextual variables that may influence outcomes; and it investigated the factors contributing to national progress in cybersecurity capacity-building. The findings revealed a generally promising state of cybersecurity capacity across the studied nations and demonstrated that higher levels of maturity in cybersecurity capacity correlate with positive national outcomes.

A study by Onumo et al. (2017) challenged the idea that regional characteristics solely determine cybersecurity capacity. Instead, they found national development and Internet usage to be the primary factors, while regional contexts may still influence cybersecurity efforts, particularly in outlier countries. Additionally, the study highlighted the significance of trust in the Internet as a factor influencing cultural attitudes and practices related to cybersecurity.

2.4 Critical Analysis of Cybersecurity Indices

The emergence of numerous cybersecurity indices claiming to assess national cybersecurity readiness has become a notable development within the realm of digital governance. This study examines five indices discussed in this study: the 2020 GCI, the NCSI (2016-2023), the 2023 NRI, the CDI 2022/23, and the Oxford CMM. The researcher will assess whether these indices effectively measure operational cybersecurity capacity or merely reflect formal institutional intentions and policy appearances.

2.4.1 Methodological Frameworks of Indices

The 2020 GCI assessed 194 nations using 82 indicators through a self-reported questionnaire that required supporting documentation. This approach primarily depends on expert-assigned weightings and binary evaluation criteria, where a single piece of documentary evidence can achieve full points for specific indicators (International Telecommunications Union, 2021a, 2021b). The GCI methodology illustrates the typical balance between scope and consistency in cybersecurity assessment, as identified by the OECD (2024). Relying on self-reported documentary evidence leads to a systematic measurement bias, prioritising formal structures over actual operational effectiveness. As explicitly acknowledged by the ITU (2021a), GCI scores do not accurately reflect a country's level of cybersecurity or the effectiveness of its measures.

The NCSI evaluates governmental cybersecurity capabilities through three main pillars: strategic, preventive, and responsive capacities (E-Governance Academy, n.d.-a). This index includes 49 indicators distributed across 12 capacity areas and functions as a dynamic index with continuous updates rather than periodic assessments (E-Governance Academy, n.d.-a). Empirical analysis has shown that changes in the NCSI are more closely related to general socioeconomic development indicators than to actual measures of cybersecurity effectiveness, raising concerns about construct validity (Kuzior et al., 2024).

The NRI evaluates digital technology readiness through four main pillars: technology, people, governance, and impact (Portulans Institute, 2023b) This multifaceted

approach enables a comprehensive assessment of a country's digital ecosystem, considering not only technological infrastructure but also human capital, regulatory frameworks, and the societal effects of digital adoption (Portulans Institute, 2023b). Although cybersecurity is acknowledged within this framework, it is not highlighted as a standalone pillar, instead being integrated as a subset of broader technological considerations (Bánhidi & Dobos, 2024). Consequently, while the NRI remains a valuable tool for assessing overall digital readiness, its usefulness as a comprehensive gauge of cybersecurity capabilities is limited, potentially overlooking crucial aspects of a country's cyber resilience and preparedness.

The CDI assesses the 20 major global economies by analysing policy, organisational, and technological factors using a mixed-method approach. This approach integrates quantitative metrics with expert interviews and peer review processes. The methodology aims to evaluate both the actual and perceived cyber commitment of these major economies (O'Brien, 2022). Relying on expert weightings and qualitative assessments raises concerns about transparency and reproducibility, as these weights are determined by normative decisions rather than being empirically validated.

The Oxford GCSCC's CMM employs a five-level maturity evaluation that concentrates on five key areas: cybersecurity policy and strategy; cyber culture and society; cybersecurity education and skills; legal and regulatory frameworks; and standards, organisations, and technologies (Global Cyber Security Capacity Centre, 2021). The CMM employs a participatory evaluation method by conducting workshops with multiple stakeholders and examining documentary evidence. (Global Cyber Security Capacity Centre et al., 2020). Creese et al. (2021) conducted an empirical evaluation of the Oxford GCSCC's CMM, revealing several methodological limitations that compromise its reliability and accuracy. The model is largely dependent on subjective evaluations obtained from modified focus groups, which introduce bias and reduce reproducibility. Additionally, its evaluations are influenced by external factors such as participant cooperation, the availability of public information, and differing interpretations of indicators, all of which contribute to inconsistent data quality. Furthermore, the model's national-level focus may be too broad to capture the intricate social and cultural dimensions of cybersecurity,

indicating a misalignment between the model's scope and the level of detail required for a thorough evaluation.

2.4.2 Regional and Developmental Considerations

Research in cybersecurity highlights a divide that reflects global economic disparities. The 2024 GCI notes that African countries have made the most progress in cybersecurity since 2021 (International Telecommunications Union, 2024), though this likely indicates initial improvements rather than significant advancements in cybersecurity capabilities. This trend implies that these indices may focus more on the ability to create legislation and report rather than on the effectiveness of actual cybersecurity. Ben Naseir et al. (2020) examined frameworks for building cybersecurity capacity in developing countries, revealing notable gaps between formal capacity assessments and the practical realities of cybersecurity capacity. The findings underscore the importance of context-specific strategies that consider resource limitations and implementation challenges beyond mere formal institutional development (Ben Naseir et al., 2020).

2.4.3 Recommendations for Improving Cybersecurity Indices

It is important for cybersecurity indices to undergo thorough psychometric validation, which includes evaluations of test-retest reliability, convergent validity, and discriminant validity. Establishing standardised validation frameworks tailored to cybersecurity measurement would represent progress in cybersecurity methodological frameworks. Integrating quantitative metrics with qualitative evaluations, such as independent verification processes and operational audits, can improve the accuracy and dependability of measurements while overcoming the shortcomings of relying solely on documentary evidence. Shifting from static snapshots to dynamic monitoring systems that capture the changing landscape of cybersecurity threats and defence mechanisms would provide more practical intelligence for shaping cybersecurity policies.

To more accurately differentiate between cybersecurity capacity and intention, it would be useful to develop indicators that focus on actual cybersecurity outcomes instead of formal frameworks. This approach requires the systematic collection of

data on incident responses, recovery metrics, and operational effectiveness, in addition to conventional cyber policy measures.

2.4.4 Overview of the Assessment of Cybersecurity Indices

The analysis indicates that the cybersecurity indices discussed in this study primarily reflect intentions towards cybersecurity and the development of formal cyber institutions, rather than the actual operational cybersecurity capacity. The persistent gap between high index scores and the persistent occurrence of cyber incidents worldwide underscores fundamental limitations in current measurement approaches.

These indices are hindered by systematic methodological challenges, such as self-reporting bias, inadequate validation processes, and issues with construct validity, which undermine their ability to accurately assess actual cybersecurity capacity. The study's findings suggests that these indices should be viewed more as indicators of cybersecurity commitment and institutional preparedness, rather than as measures of genuine cybersecurity effectiveness.

The field of cybersecurity capacity requires more advanced measurement frameworks that can accurately differentiate between formal cybersecurity structures and actual capacity. Without additional outcome metrics and rigorous validation methods, existing indices may create a misleading sense of security based on formal appearances rather than actual cybersecurity capacity.

Future research could focus on developing indices that capture the complex, dynamic, and multifaceted nature of cybersecurity capacity, while addressing the fundamental methodological issues identified in this analysis. Through these improvements, cybersecurity indices will offer reliable insights for policy development and capacity building in an increasingly digital world.

2.5 Challenges faced by African and developing countries in building cybersecurity capacity

Developing countries encounter several major obstacles when attempting to implement effective cybersecurity policies (Calderaro & Craig, 2020; Kabanda et al., 2018; Pawlak & Barmpaliou, 2017). These challenges include lack of resources, limited digital capacity, lack of comprehensive policies, political instability and

insufficient cooperation. Addressing these challenges requires substantial investment in resources, establishments of institutions, development of expertise, and enhancement of governance, elements that many countries lack to build a resilient cybersecurity system capable of safeguarding their digital future (Calderaro & Craig, 2020).

2.5.1 Resource Constraints

Many developing countries, particularly African countries, suffer major budgetary constraints that limit their ability to develop a skilled digital workforce, integrate modern technologies, and provide sufficient digital infrastructure as a country. These constraints are because of the government's low taxation collection, corruption in the public sector, the country's high debt level, and the country's reliance on a single source of revenue (Kayode-Ajala, 2023; Annarelli et al., 2020). Consequently, these governments often struggle to deliver basic services, let alone prioritise cyber capacity-building (Ifeanyi-Ajufo, 2023).

2.5.2 Limited Digital Capacity

Many developing countries' education systems still rely on traditional classroom learning, which lacks subjects that expose students to computer literacy, coding, data analysis, and cybersecurity at a young age. Furthermore, there is a scarcity of teachers who are qualified to teach these subjects. Most households in developing countries are unable to afford personal computers or smartphones; even in cases where they can acquire the devices, inadequate Internet access and poor technical infrastructure exacerbate poor digital literacy (Kayode-Ajala, 2023). These countries also have poor digital capacity, which makes it difficult for them to develop and maintain the technological competence required for effective cybersecurity (Dutton et al., 2019).

The lack of digital capacity is reflected in Africa's current cybersecurity situation. Despite the adoption of the Digital Transformation Strategy for Africa (DTS) and the development of policies such as the Continental Cybersecurity Strategy, many African countries continue to struggle with inadequate digital infrastructure and low levels of digital literacy.

2.5.3 Weak Institutions and Bureaucracy

Low-capacity states often have underdeveloped and ineffective government institutions, departments, and regulatory entities essential for implementing and enforcing cybersecurity policies (Muller, 2015; Signé & Signé, 2021).

Despite the comprehensive nature of the Malabo Convention on Cybersecurity and Personal Data Protection, most AU member states have yet to endorse it, which hinders its effectiveness and credibility (Chatham House, 2024). Only 15 out of 55 AU member states have officially approved the Malabo Agreement, and following its implementation in 2023, only one additional country has ratified it. This highlights the challenge of achieving widespread agreement and cooperation on cybersecurity policies. The slow rate of ratification underscores the issues of weak institutions and bureaucratic inefficiencies in implementing robust cybersecurity measures across the African continent (Chatham House, 2024).

2.5.4 Lack of Comprehensive Policies

The absence of comprehensive policies and regulations to promote digital transformation and cybersecurity poses a significant challenge. Without clear guidelines and frameworks, establishing a secure cyber environment is difficult (Ifeanyi-Ajufo, 2023). Moreover, many developing countries attempt to implement international standards that do not suit their local context, resulting in a mismatch that further strains their limited resources (Kayode-Ajala, 2023). The legal landscape is often fragmented and outdated. While some African countries have passed cybercrime laws, these are outdated and are not coordinated across the continent.

The AU’s Peace and Security Council (PSC) has recently made cybersecurity a key agenda point, leading to significant actions such as directing the AU Commission to expedite the development of a Continental Cybersecurity Strategy and adopting a continental child online protection policy (Chatham House, 2024). Additionally, the agreement on the Common African Position on the Application of International Law in Cyberspace at the AU summit has affirmed AU member states' obligations to uphold international law in cybersecurity governance. These initiatives represent crucial steps towards establishing comprehensive cybersecurity policies, yet the lack of widespread

ratification of the Malabo Convention still poses a significant barrier to unified and effective policy implementation (Chatham House, 2024).

2.5.5 Political Underpinning

Political instability and influence significantly impact the effectiveness of cybersecurity measures and governance mechanisms in developing countries. Inconsistent policy implementation and oversight due to political uncertainties weaken cybersecurity efforts (Ifeanyi-Ajufo, 2023). Additionally, many low-capacity states prioritise other pressing economic and social issues over cybersecurity, leading to underinvestment and policy inadequacy (Dutton et al., 2019).

AU member states face divergent cybersecurity challenges due to varying political, social, and cultural contexts, which are reflected in their cybersecurity governance dynamics. This diversity complicates the establishment of a unified approach to cybersecurity across the continent. Additionally, Africa has historically been marginalised in global cybersecurity governance forums. However, there has been a noticeable shift, with African countries showing increased interest and participation in the UN negotiations to agree on a global cybercrime treaty. Such involvement indicates a growing recognition of the importance of cybersecurity on the continent, but political instability and inconsistent policy implementation continue to hinder progress (Chatham House, 2024).

2.5.6 Insufficient National Cooperation

Corruption in the public sector undermines government integrity and its ability to provide essential services in many developing countries. With most digital service providers being private companies focused on profit, there is often a misalignment of interests and priorities. This misalignment can lead to inefficiencies, mismanagement, and a lack of accountability in public-private partnerships, ultimately hindering the development and implementation of robust digital and cybersecurity frameworks (Kayode-Ajala, 2023).

The AU's emerging cybersecurity agenda emphasises the importance of a multi-stakeholder approach, as outlined in Article 26 of the Malabo Convention, rather than an agenda focused solely on traditional peace and security perspectives. However, the implementation of this approach faces significant challenges due to insufficient

national cooperation. Many African governments and businesses do not fully recognise the severity of the cybersecurity threat and often prioritise other pressing economic and social issues over cybersecurity (Forbes, 2022). This lack of prioritisation and alignment of interests between public and private sectors exacerbates the difficulty in developing and enforcing effective cybersecurity frameworks (Chatham House, 2024).

2.5.7 Insufficient International Cooperation

Collaboration with other countries is crucial for gaining knowledge on best practices, lessons learned, and accessing additional resources and expertise to enhance cybersecurity capabilities. International actors and cybersecurity diplomats should prioritise strengthening scientific and technical knowledge in developing countries to boost cybersecurity readiness (Ifeanyi-Ajufo, 2023). However, low-capacity states are frequently less engaged and influential in international cybersecurity governance, standards, and cooperation mechanisms, further hampering their efforts to build effective cybersecurity frameworks (Calderaro & Craig, 2020).

In the context of Africa, there is a pressing need for member states to align their diplomatic strategies more effectively. Currently, African countries are divided in their partnerships among Russia, China, and Western countries, with the potential for these alliances to be complicated by geopolitical tensions such as the US-China competition (Chatham House, 2024). This fragmentation in diplomatic relations could undermine collective efforts to establish a coherent and effective cybersecurity agenda across the continent. The AU can play a crucial role in providing platforms for international cybersecurity cooperation, ensuring that African cyber diplomatic relations with the West, Russia, and China are balanced and practical rather than subservient. Enhanced international cooperation is essential for strengthening cybersecurity capabilities and aligning diplomatic strategies to address growing cyber threats (Chatham House, 2024).

2.6 The securitisation of cyberspace

CSS provides an important perspective for understanding how governments weaponise cyber technologies and securitise citizens in both domestic and international contexts. This section of the literature review examines the securitisation processes in cyberspace, the dynamics between offensive and defensive cyber

strategies, the complex relationships between state and non-state actors, domestic surveillance practices, international cyber competition, and the theoretical frameworks that explain these issues (Ramich & Piskunov, 2022).

2.6.1 Securitisation Processes in Cyberspace

The securitisation of cyberspace signifies a major shift in the way governments define and justify cyber threats. Drawing from the Copenhagen School's securitisation theory, cyberspace has evolved into a significant political arena, emphasising the importance of digital sovereignty and cybersecurity (Ramich & Piskunov, 2022). This process entails framing cyber threats as critical dangers that necessitate urgent actions beyond standard political procedures.

The securitisation of cyberspace functions through a variety of channels and involves numerous actors. Research indicates that cyberspace has evolved into a comprehensive political arena where conflicts among actors encompass political and economic threats, prompting state actors to formulate initial regulations and reach consensus on norms governing state conduct. (Ramich & Piskunov, 2022). The process of securitisation is not consistent and differs depending on the context and the actors involved. Some research indicates that the varied and inconsistent securitisation of cyber threats mirrors distinct national strategies and priorities. (Cavelty, 2024).

2.6.2 Cyber Offense and Defense

The relationship between offensive and defensive cyber capabilities highlights the intricate strategic considerations made by countries. Research by Arslan (2023) suggests that as countries enhance their cybersecurity capabilities, they are more likely to carry out disruptive activities against other countries in cyberspace. This observation contradicts the common belief that increased cyber defence leads to greater stability in cyberspace.

Spector (2022) suggests that China, Russia, and the United States are developing two offensive cyber capabilities that could change the strategic dynamics among these countries. These capabilities include malware designed to compromise nuclear

weapon systems and operations designed to disrupt critical infrastructure (Spector, 2022).

Russia's hybrid interference efforts demonstrate sophisticated offensive tactics that integrate cyber activities with disinformation to pose challenges to liberal democracies, such as France, Germany, and the UK (Kondratov & Johansson-Nogués, 2023). These actions aim to create friction between governments and their citizens while eroding trust in democratic institutions within these countries (Kondratov & Johansson-Nogués, 2023).

2.6.3 State and Non-State Actors

The cyber realm fundamentally blurs the lines between state and non-state entities. As noted by Pagallo (2015), identifying the perpetrators of cyber-attacks is often challenging, as these attacks can be executed by either non-state actors or state actors. This issue of attribution poses considerable difficulties for legal systems and strategic planning. Moreover, it allows states to use proxy actors while maintaining plausible deniability.(Khalil et al., 2024). Egloff (2022) claims that there is a growing trend of states depending on private actors for both offensive and defensive functions, leading to the emergence of what researchers call ‘semi-state actors’ in the realm of cybersecurity. These actors operate in ambiguous areas between governmental and private control, frequently advancing state objectives while allowing for plausible deniability.

2.6.4 Private Sector Involvement

Digital espionage reveals the complex interconnections between countries, exploit vendors, state-sponsored cyber actors, and technology platforms (Datta, 2024). The political economy of nation-states offers insights into their dual roles as intermediaries and customers within cyber networks (Datta, 2024). The conflict between governmental oversight and the capabilities of the private sector enhances the influence of private actors while necessitating policy measures to reorganise cyber networks (Datta, 2024).

2.6.5 Democratic versus Authoritarian Cyber Securitisation Approaches

In cyberspace, securitisation efforts transcend traditional regime boundaries, as both democratic and authoritarian governments employ digital tools to control their populations (Ramich & Piskunov, 2022). However, the mechanisms and justifications vary between these regime types.

Democratic Approaches: Securitisation of Legal Structures

Western democracies often secure cyberspace by implementing legal structures that uphold procedural legitimacy while enhancing their surveillance capabilities. The Five Eyes intelligence alliance, which includes Australia, Canada, New Zealand, the United Kingdom, and the United States, serves as a prime example of this strategy. These countries leverage the intricate interdependence of information flows through advanced intelligence-sharing systems (Datta, 2024). These systems manage the flow of information in a way that resembles a panopticon, differing from more straightforward authoritarian control techniques (Datta, 2024).

Western democracies grapple with the inherent conflict between the need for security and the principles of liberal democracy. The resilience of these democracies and their dedication to safeguarding fundamental rights have been challenged by digital security initiatives, leading to constitutional issues in both national and international law (Pagallo, 2015). Studies on authoritarian surveillance indicate that even in democratic countries, the public's awareness of the potential for government misuse of digital governance tools leads to decreased support, reflecting citizens' concerns about excessive surveillance (Karpa & Rochlitz, 2023).

Authoritarian Approaches: Comprehensive Digital Control

Authoritarian governments adopt more thorough and straightforward methods for cyber securitisation. Digital authoritarianism encompasses strategies that utilise digital tools to suppress critical discussions and demands for accountability from those in power by obstructing the flow of information and limiting free speech (Michaelsen & Ruijgrok, 2024). These systems function through four primary methods: online censorship, Internet shutdowns, digital surveillance, and the manipulation of online information (Michaelsen & Ruijgrok, 2024). China's system illustrates a ‘chokepoint’

effect where the government directly manages technology vulnerabilities, in contrast to the more decentralised method of the Five Eyes (Datta, 2024).

2.6.6 Western versus Eastern Surveillance Practices

Governments are increasingly employing cyber technologies for monitoring their citizens and enhancing security measures. The transformation of corporate internet infrastructure into a tool of power allows the U.S. government to utilise its regulatory authority over privately managed critical infrastructure. This enables extensive internet surveillance by extracting information from other countries, conducting large-scale influence operations by disseminating information into these nations, and increasingly imposing unilateral cyber sanctions on other countries.(Freuler, 2023).

The surveillance activities of Western nations, as demonstrated by the operations of the National Security Agency (NSA) and the UK's Government Communications Headquarters (GCHQ) that were exposed in the Snowden leaks, are conducted under legal frameworks while engaging in widespread monitoring (Amnesty International UK, 2025). In the aftermath of 9/11, these systems transitioned from focusing on specific targets to conducting widespread surveillance, incorporating aspects of a surveillance state that pose a challenge to the principles of liberal democracy (Gros et al., 2017). Surveillance efforts go beyond just safeguarding national security; they also aim to advance economic objectives and exert international influence (Gros et al., 2017). The Five Eyes intelligence alliance exemplifies an advanced model of global surveillance collaboration, characterised by frequent vulnerability disclosures and the management of information through intricate, interconnected networks (Datta, 2024). This strategy centralises cyber power in private actors while still retaining democratic oversight mechanisms, though these are considerably restricted (Datta, 2024).

In Eastern countries, particularly China, surveillance methods illustrate a more pronounced governmental control over digital systems and the actions of citizens. The Chinese digital surveillance apparatus increases its investment in surveillance technologies as a reaction to collective movements, with violent protests leading to notably higher funding levels (Rothschild, 2024). Iran's digital authoritarianism demonstrates how external threats can create an environment that allows governments to enhance their censorship and surveillance capabilities (Michaelsen,

2018). The Iranian government views the Internet as a strategic arena due to its opposition to the United States, prompting the regime to develop a national Internet that is less susceptible to external influence and open to state control (Michaelsen, 2018). China is frequently regarded as the leading example of a digital authoritarian nation with a robust domestic tech industry. In contrast, Iran is more similar to a second tier of ambitious digital authoritarian countries, such as Russia, Venezuela, Myanmar, and Saudi Arabia, which heavily rely on the global technology sector to sustain their digital authoritarian strength (Conduit, 2025).

2.6.7 African Digital Authoritarianism

Internet shutdowns have become more widespread in African countries, particularly during elections and contentious political periods (Stremlau & Dobson, 2022). A study involving ten African nations—namely Egypt, Ethiopia, Cameroon, Kenya, Nigeria, South Africa, Sudan, Uganda, Zambia, and Zimbabwe—identified 115 examples of strategies employed to restrict online civic engagement (Roberts, 2021). In these ten African countries, the top five strategies employed to restrict online civic space include digital monitoring, spreading false information, cutting off internet access, implementing restrictive internet laws, and detaining individuals for their online activity (Roberts, 2021). These strategies collectively establish control over the flow of digital information.

In African countries, Internet shutdowns frequently serve as attempts to reestablish control in a historical context marked by disputes over borders, authority, and national identity.(Stremlau, 2025). This highlights the wider conflicts between postcolonial countries and global tech firms, where shutdowns are employed as a means for states to assert their authority against perceived foreign influence.

Ethiopia's Authoritarian Dilemma

Ethiopia serves as a prime example of the 'Authoritarian Dilemma', where countries aim to advance digital growth while retaining tight control (Grinberg, 2017). The Ethiopian government has implemented widespread surveillance, intimidation tactics, and selective censorship to both encourage development and suppress digital opposition (Grinberg, 2017). With a state monopoly on digital services, Ethiopia

demonstrates how authoritarian regimes use surveillance to bypass traditional intelligence gathering methods (Grinberg, 2017).

Zimbabwe's Hybrid Surveillance System

Zimbabwe uses intricate networks of both governmental and non-governmental actors engaged in a wide-ranging and multifaceted system of hybrid online and offline surveillance (Stevens et al., 2023). The surveillance system integrates digital mass surveillance with traditional human intelligence, resulting in extensive monitoring capabilities that go beyond individual targets and impact entire communities (Stevens et al., 2023). This hybrid method illustrates how developing countries tailor surveillance technologies to fit their specific environments and limited resources.

Tanzania's Cybercrime Legislation

Tanzania has enacted cybercrime laws that criminalises online dissent by categorising political opposition as security threats (Cross, 2021). The Tanzanian government employ these laws to legitimise the suppression of online rights, framing it within broader themes of security and development.(Cross, 2021). This example demonstrates how legal systems can be utilised as instruments of digital authoritarianism while retaining their legitimacy through the rhetoric of security.

The literature provides examples of digital authoritarianism practices across multiple African countries, offering comparative insights. The integration of critical security studies with case studies strengthens the theoretical understanding of cyber securitisation processes.

2.6.8 Theoretical Frameworks from Critical Security Studies and Securitisation Theory

The integration of CSS into cyber governance highlights the shortcomings of conventional security methods. Research indicates that relying solely on technical cybersecurity measures is insufficient to tackle cybersecurity issues, and that strong collaborative efforts among diverse stakeholders, including citizens, government, industry, and academia, are essential (Zeadally, 2014). This finding highlights the need for more comprehensive approaches that go beyond technical solutions. The integration of CSS and digital governance literature provides a more nuanced understanding of these complex phenomena.

2.6.9 Evaluation of CSS and Cyber Securitisation

The effectiveness of CSS lies in its capacity to uncover the socially constructed aspects of cyber threats and the political mechanisms that legitimise them. Nonetheless, the fast-paced development of cyber technologies poses challenges for theoretical models originally designed for more conventional security areas.

Although there is empirical evidence for the securitisation of cyberspace and the expansion of offensive cyber capabilities, there is still a limited understanding of the long-term impacts of domestic surveillance and the securitisation of citizens. Additionally, the issue of attribution in cyberspace presents methodological difficulties for researchers examining these issues. Existing research offers valuable insights into cyber securitisation processes but also has several shortcomings. Most studies concentrate on major powers, such as the US, China, and Russia, with insufficient focus on middle powers and developing countries.

While the theoretical frameworks are advanced, they often struggle to keep pace with the rapid changes in digital technologies and their political uses. The research indicates that cyber securitisation processes occur across different regime types but with unique characteristics. Democratic countries encounter more constraints due to legal systems and public scrutiny, necessitating more sophisticated justification strategies. In contrast, authoritarian regimes can enforce more direct control measures but must address legitimacy issues and technological dependencies.

The merging of state and non-state actors in cyberspace introduces new challenges for international law and governance. The incorporation of private sector capabilities into state surveillance systems raises concerns about democratic accountability and the corporate responsibility of technology companies. The global reach of digital technologies means that cyber securitisation practices transcend borders, with authoritarian innovations potentially impacting democratic practices and vice versa. This situation underscores the need for international collaboration on digital rights and cyber governance standards.

2.7 Theoretical Framework of the Study

CSS offers a conceptual framework for analysing how eight digital control variables, derived from the DSP dataset, influence governmental cybersecurity capacity. This section, informed by CSS scholarship, is organised into four parts: the foundations of CSS; the connection between DSP variables and CSS themes; empirical synthesis; and the theoretical implications along with suggestions for future research.

2.7.1 Foundations of Critical Security Studies

CSS developed as a response to conventional security models that focus on state-centred methods, promoting a wider and more detailed perspective on security that extends beyond merely protecting territories (Newman, 2010). In assessing the cybersecurity capacity of governments, three key aspects of CSS are particularly relevant: the Securitisation Theory from the Copenhagen School, Emancipatory Security from the Welsh School, and Post-Structuralist Approaches.

Securitisation Theory examines how political narratives can transform issues like cyber-attacks into existential threats, thereby justifying extraordinary measures. Emancipatory Security centres on human security, investigating how capacity building can both empower and oppress, with a focus on democratic accountability. Post-Structuralist Approaches study how discourses and the interaction of knowledge and power influence security practices and create vulnerabilities. Collectively, these three strands of CSS enable us to perceive the DSP's measure of government cybersecurity capacity as a construct shaped by social and power dynamics.

2.7.2 Alignment of DSP variables with CSS themes

DSP defines government cybersecurity capacity as the state's ability to counter cybersecurity threats with skilled staff and resources (Coppedge et al., 2024). The study will align each of the eight DSP independent variables to CSS concepts of securitisation and power.

Government social media monitoring

DSP measures the comprehensiveness of state surveillance over political content on social media platforms (Coppedge et al., 2024). Social media platforms include Facebook, Flickr, Friendster, Google+, Instagram, Myspace, LinkedIn, Signal, Slack,

Snapchat, VKontakte, Weibo, WhatsApp, and X (Coppedge et al., 2024). In the context of securitisation theory, surveillance is frequently seen as a fundamental tool that enhances the state's ability to observe and exert control. Scholars examining the concept of securitisation suggest that certain matters are intentionally portrayed as major security threats, thereby legitimising the state's use of extraordinary measures, such as increased surveillance activities (Otukoya, 2024). Empirical evidence shows that extensive social media monitoring correlates with strengthened technical cybersecurity capacity but can erode public trust (Afiyah, 2024; Park & Lee, 2018).

Government Internet filtering capacity

DSP's measurement of whether the government has the technical capacity to censor content reflects the legal and institutional authority to impose censorship. Government Internet filtering capacity involves the control and regulation of political information dissemination, often through censorship and surveillance. This process can act as a securitisation mechanism, where political content is perceived as a potential threat, requiring extraordinary measures to address the perceived risk.

Government censorship of online political material serves to influence public opinion and manage narratives, aligning with securitisation strategies. By limiting or altering political information, governments can justify the enforcement of stringent security measures, emphasising the necessity for surveillance and control to uphold order (Otukoya, 2024). Moreover, implementing Internet filtering strategies can lead to substantial investments in cybersecurity infrastructure, as governments aim to protect themselves from perceived threats both within their borders and abroad, thereby further entrenching the securitisation of political discourse.

By examining cross-national studies, it becomes evident that stronger government Internet filtering corresponds with increased resource allocation towards cybersecurity agencies and the strengthening of security measures, as governments respond to and prepare for threats identified through a security-focused perspective (Jones, 2009; Vuori, 2008). The manner in which these elements interact with each other illustrates that securitisation extends beyond mere policy, embedding itself within legal and

institutional frameworks, which significantly impacts societal freedoms and civil rights (Vuori & Paltemaa, 2015).

Government Internet filtering in practice

The relationship between DSP's government Internet filtering in practice variable and CSS, particularly through the lens of securitisation theory, involves examining the gap between formal legal powers to filter online content and the actual enactment of these powers in practice. According to CSS's securitisation theory, legal structures that permit content filtering evolve into authentic security measures only when they are implemented and executed. This concept is crucial for comprehending how theoretical authority is transformed into practical applications.

The DSP's measure of how often online political content is restricted corresponds with CSS's focus on this discrepancy in practice. In theory, laws and regulations exist to manage or restrict certain online content for security purposes. Nonetheless, the actual enforcement of these laws—specifically, how often and under what circumstances content is blocked—highlights the practical application of these security measures (Monaci & Persico, 2025; Llansó, 2020).

Moreover, post-structuralist CSS emphasises the role of practice in shaping both governmental authority and the vulnerabilities of citizens, which is directly relevant to the topic of filtering online content. This highlights a dual aspect where the state's ability to control information demonstrates its authority, while simultaneously, the methods employed for filtering content can pose threats to citizens, particularly concerning freedom of expression and access to information (Llansó, 2020; Fasel & Weerts, 2024). The European Union's Digital Services Act (DSA) seeks to enhance the regulation of content moderation, highlighting the intricate task of aligning regulatory systems with the principles of free speech and user rights. These systems must carefully balance the promotion of security with the prevention of undue censorship, thereby illustrating the difficulties in translating security legislation into actionable practices (Quintais et al., 2023).

Fundamentally, the DSP's measure of Internet filtering exemplifies the practical use of securitisation principles, highlighting the state's attempts to convert legal authority into

active security measures. This real-world application can both strengthen the state and create vulnerabilities for citizens, as explored within the context of CSS and securitisation theory.

Government Internet shut down capacity

The technical ability of a government to shut down access to domestic Internet, known as Internet shutdown capacity, is closely linked with DSP capacity scores. This indicates that a higher capability for implementing Internet shutdowns is linked to increased state control over digital spaces. Such actions strengthen the state's exclusive control over digital force, restricting the influence of non-state entities in the digital sphere (Gohdes, 2024; Gozgor et al., 2024).

The relationship between Internet shutdown capacity and state monopoly on digital force is complex and reflects broader trends in Internet governance and digital rights. Internet shutdowns and censorship are often justified by governments under national security narratives, which have been observed in various contexts such as Ethiopia and Myanmar. These actions are a part of broader strategies to control information flow and maintain state power, especially during times of political unrest or dissent (Ayalew, 2019; Padmanabhan et al., 2021). The state’s ability to disable the Internet and implement similar digital controls not only enhances a state's ability to manage and enforce digital compliance but also presents considerable obstacles to global digital governance frameworks that aim to balance national priorities with global digital freedoms and human rights (Mueller, 2010).

In the context of digital sovereignty, many countries are moving towards reinforcing state power over the digital domain, which often conflicts with multi-stakeholder governance models that emphasise shared control among various stakeholders. This shift is part of a larger dialogue on digital sovereignty, where states assert greater control over digital infrastructure and data as a means of national security and economic protection (Pohle & Santaniello, 2024; Solum, 2009). The digital rights landscape in Africa highlights the tensions between state control and citizens' digital rights. Governments are employing tools, such as digital surveillance and Internet

shutdowns, to close civic spaces, which reduces citizens' ability to engage in governance and exercise their rights in online environments (Roberts, 2021).

The evolving landscape of Internet governance highlights an increasing shift towards digital sovereignty, where nations aim to reinforce their authority over crucial digital domains, potentially at the expense of digital rights and freedoms. The relationship between the technological ability to enforce shutdowns, the state's regulatory ambition through DSP capacities, and the obstacles to international Internet governance is important for comprehending contemporary state tactics in the digital age.

Internet legal regulation content

DSP's measure of legal removal rights highlights the significance of law in securitisation. A comparative analysis of data protection across East African countries, including Kenya, reveals diverse legal frameworks and enforcement challenges, underscoring the need for enhanced data protection regulations to foster trusted digital economies.(Shao et al., 2025). This suggests potential for digital violations due to inadequate regulation and enforcement.

Studies on the impact of digitisation underscore improvements in legal infrastructure and access to justice in countries such as Kenya and Ghana, facilitated by technologies like blockchain, which ensure greater integrity and security in legal processes (Djuraev et al., 2025). Nevertheless, digitisation also poses risks related to cybersecurity and digital literacy disparities, which could increase digital rights concerns.

Privacy protection by law content

The alignment between CSS concepts of power and securitisation with the DSP Privacy protection by law variable reveals a tension in digital governance. Power dynamics in CSS examine how states exercise authority and control, while securitisation refers to the process by which issues are framed as existential threats requiring extraordinary measures that bypass normal political processes (Buzan et al., 1998). The concept of power in CSS suggests that states, through securitisation, may prioritise national security at the expense of individual privacy. This

is particularly evident in the use of technologies such as AI, which can be a tool for both enhancing security and infringing on privacy (Nadella et al., 2024). The securitisation process directly challenges legal privacy protection principles by potentially creating areas where privacy rights are undermined (Gutwirth & De Hert, 2022).

Moreover, privacy and data protection laws are designed to create transparency and limit the power that states, and political entities can exert over individuals' data. Global data privacy laws, including frameworks such as the EU's General Data Protection Regulation (GDPR), aim to balance technological innovation with the protection of individual privacy rights. However, as a study on global data privacy laws points out, these frameworks are frequently challenged by the rapid advancement of technology that can sometimes outpace regulatory efforts (Ehimuan et al., 2024). The interaction of these factors shows how data protection laws are inherently involved in the discussions about power and securitisation. For example, political micro-targeting, which involves the processing of personal data for political communication, underscores the need for strong privacy laws to regulate political surveillance activities (Witzleb & Paterson, 2021).

The DSP privacy protection scale, ranging from 0 to 4, is closely linked to the ideas of power and securitisation. Lower scores on this scale (0-2) suggest significant government access rights, indicating a high level of securitisation in digital environments. In this context, the state has effectively portrayed data access as a security imperative, thereby justifying exceptional surveillance powers that take precedence over individual privacy rights (Lyon, 2003). Conversely, higher levels (scale of 3-4) indicate minimal securitisation, where privacy is safeguarded except in exceptional circumstances, reflecting a power dynamic that prioritises individual rights over state security interests.

The Privacy protection by law content variable measures the extent of securitisation present in legal systems: when governments legally allow extensive access to personal data (scale of 0-2), they have institutionalised a security approach that prioritises state security over citizen privacy. In contrast, restrictive legal frameworks (scale of 3-4) signify a successful challenge to securitisation narratives, upholding

privacy as a fundamental right rather than viewing it as a security risk (Bigo, 2002). The period from 2000 to 2023 illustrates the progression of digital securitisation, especially following the events of 9/11 and throughout the 'War on Terror'. During this period, numerous countries increased their surveillance capabilities under the guise of security, highlighting how securitisation processes become ingrained in legal frameworks and gradually make extraordinary governmental powers seem normal (Mechkova et al., 2019).

Although CSS and securitisation offer a framework for understanding how countries handle security threats, the conflict with privacy rights, as highlighted by the DSP Privacy protection by law content variable, reveals a complex arena. This highlights the necessity for ongoing adjustments in legal frameworks to ensure that privacy is not excessively compromised by the politics of securitisation and the exercise of power (Caprioli, 2004; Petersen, 2011).

Government online content regulation approach

DSP's government online content regulation approach variable ranges from state-controlled regulation to the delegation of this responsibility to private actors. This can be understood through the lenses of securitisation and governance: when the state exerts significant control, it aligns with speech acts that legitimise emergency actions, while delegating authority suggests governance through private or hybrid actors.

Governments have justified extraordinary measures, such as Internet shutdowns, by invoking national security or the protection of election integrity. This demonstrates how state power on the DSP scale is linked to securitising speech acts and enforcing exceptional measures (Thumfart, 2024). CSS emphasises that legitimate emergency measures should be temporary and reversible, implying that permanent regulatory control signifies a shift towards governance centred on security (Thumfart, 2024).

Applying traditional broadcast regulations or criminal laws to social media platforms illustrates how regulatory measures are adapted to push states further along the DSP scale, aiming for stricter oversight of online content. In Nigeria, authorities have held people responsible for their remarks on social media, particularly when these remarks

criticise government officials and are deemed offensive (Obia, 2023). This reflects an inclination among Nigerian authorities to regulate what is considered acceptable content on social media, akin to the control that regulators currently exercise over broadcasting content (Obia, 2023). China's Cybersecurity Law and the rhetoric of internet sovereignty represent a full state-centric digital sovereignty model where content control is institutionalised rather than delegated to private actors (Pohle et al., 2024).

The movement toward delegation or co-regulation on the DSP scale reflects different governance strategies, shifting enforcement burdens to social media platforms and producing new power asymmetries. Nigeria's Platform Code of Practice institutionalises a co-regulatory model that shifts certain content moderation and compliance responsibilities to social media platforms rather than primarily punishing users, illustrating a move away from pure state control toward hybrid governance (Obia, 2025).

Moving toward delegation or co-regulation in online content moderation, which often involves private companies managing and enforcing rules, can alleviate the need for blatant emergency measures by allowing more flexible approaches. However, this shift can also create significant accountability gaps. For instance, private content moderation practices can lack transparency and accountability, resulting in practices that enhance existing power imbalances. This is evident in cases where moderation rules align with Western norms, sidelining non-Western voices and perpetuating historical injustices (Shahid & Vashistha, 2023). Furthermore, algorithmic moderation can introduce arbitrariness, as machine learning models may provide conflicting outputs, leading to biased or inconsistent content moderation (Gomez et al., 2024).

In Africa, digital public infrastructure and digital transformation for development (DX4D) projects can be seen as efforts to enhance sovereignty or build capacity, but they may also involve elements of control and resource extraction. These projects illustrate how sovereignty claims can justify greater state involvement in content moderation (Pohle et al., 2024). Examining Uganda's extensive DX4D projects highlights how these initiatives' coercive and material impacts influence the future of low and lower-middle-income countries in the Global South (Kalema, 2024; Pohle et

al., 2024). Ultimately, these projects, under the pretence of public-sector reform, promote dominant interests while neglecting public values and local strategic priorities (Kalema, 2024).

Government capacity to regulate online content

The DSP variable, government capacity to regulate online content, aligns fundamentally with critical security studies through securitisation theory, where state capacity determines whether security rhetoric translates into concrete digital governance. African examples demonstrate how different capacity levels (scale of 0-4) shape securitisation outcomes—from Ethiopia's limited capacity relying on Internet shutdowns to South Africa's institutionalised digital governance.

The alignment of government capacity to regulate online content with critical security studies is explained through the "speech act plus capacity" framework and securitisation theory. Securitisation theory emphasises that security is constructed through speech acts, which define certain issues as existential threats, necessitating urgent government measures (Schumann, 2025). In the context of regulating online content, governments may frame online extremism or hate speech as security threats through these speech acts, thus initiating a process to address these perceived threats (Otukoya, 2024).

South Africa demonstrates institutionalised digital governance through formal cybersecurity strategies and comprehensive legal frameworks (i.e., high capacity, scale of 3-4). Securitisation occurs through national security and economic protection narratives, with formal policy processes incorporating multiple stakeholders (Stremlau & Dobson, 2022; Czuba, 2025). Rwanda exhibits techno-authoritarian capacity with considerable investment in digital infrastructure. Development and security narratives often justify extensive monitoring with systematic content removal and limited civil society input (Kumar, 2024; Roberts & Oosterom, 2024).

Both countries, despite their differing methodologies, underline a global trend where digital technologies are repurposed to strengthen or consolidate state power. In South Africa, this manifests through institutional governance seeking broader security mandates, while in Rwanda, the focus on infrastructural development aligns with a

strong central government that emphasises control and stability (Da Vinha, 2024; Matfess, 2015).

Nigeria demonstrates moderate capacity (scale of 2-3)_ through active policy development but inconsistent enforcement, with high-profile platform confrontations serving factional political interests (Gravett, 2020). Tanzania implements a ‘slow shutdown’ strategy using incremental legal measures to gradually extend state control. Public order narratives justify systematic legal framework development rather than technical shutdowns (McGee, 2023).

The Democratic Republic of Congo (DRC) and Ethiopia exhibit a low-capacity level (scale of 0-1), where the employment of Internet control and counter-insurgency narratives highlights substantial institutional and capacity issues. These challenges hinder effective governance and lead to authoritarian measures often defended by national security arguments.

In Ethiopia, governance is marked by authoritarian traits, which are evident in the state's limited ability to manage infrastructure, such as implementing Internet shutdowns. These measures are frequently defended with counter-insurgency arguments, aiming to uphold control and stability. However, they also highlight the absence of institutional growth. The state's dependence on controlling infrastructure instead of developing strong governance systems, underscores its capacity constraints (Rami, 2024). The DRC has minimum regulatory framework and limited technical expertise, contributing to weak institutional structures regarding cybersecurity. Consequently, responses tend to be improvised and reactive, rather than organised and well-regulated. The absence of robust governance systems in the DRC underscores the difficulties in addressing crises with unified policies for online content regulation, highlighting a dependence on temporary solutions instead of systematic regulation.

2.8. Conceptual framework of the study

According to Mechkova et al. (2024), the DSP dataset offers a significant advancement in the availability and quality of cross-country data at the intersection of politics and the digital space. The DSP provides a comprehensive dataset that covers

179 countries over the period of 2000 to 2023 (Digital Society Project, 2024b). This dataset includes 35 indicators that cover crucial aspects such as online censorship, politicisation of social media, coordinated information operations, foreign influence, domestic political monitoring, and government cybersecurity capacity (Mechkova et al., 2024). The DSP's extensive coverage and annual global data provides a consistent and longitudinal perspective essential for in-depth analysis (Mechkova et al., 2024).

The DSP dataset complements and expands on existing datasets, such as Freedom House's Freedom on the Net, offering broader geographical and temporal coverage (Mechkova et al., 2024). Rigorous diagnostic tests have validated the DSP indicators, affirming their reliability and utility (Mechkova et al., 2024). The detailed case studies, such as those generalising insights from China's digital political landscape and contrasting Ethiopia's digital environment with existing measurements, further demonstrate the unique insights provided by the DSP dataset.

The study focuses on government cybersecurity capacity in African and developing countries, so the dependent variable mostly contains legal and regulatory aspects of cybersecurity rather than specific technical measures (such as encryption technologies, software vulnerabilities, or infection rates.)

This study's conceptual framework utilises variables from the DSP dataset, which are proxy measures of three CMM dimensions: policy and strategy, culture and society, and the legal and regulatory framework (Global Cyber Security Capacity Centre, 2021). The researcher systematically categorised these variables according to their corresponding CMM dimensions and their Likert-scale measurements. Table 2.1 below provides an overview of these proxy measures and their alignment with the CMM framework.

Table 2.1: Overview of CMM dimensions and proxy measures

CMM Dimensions	**Proxy measures**
Cybersecurity Policy and Strategy	Government cyber security capacity
Cybersecurity culture and society	Government social media monitoring
	Government Internet filtering capacity
	Government Internet filtering in practice

Cybersecurity Legal and regulatory framework	Government Internet shut down capacity
	Internet legal regulation content
	Privacy protection by law content
	Government online content regulation approach
	Government capacity to regulate online content

Source: Coppedge et al. (2024) and Global Cyber Security Capacity Centre (2021)

2.8.1 Cybersecurity Policy and Strategy

The government cybersecurity capacity variable from the DSP dataset will be used as a proxy measure for the policy and strategy dimension of the CMM.

Government cyber security capacity

The government cybersecurity capacity variable assesses the government's capacity to address cybersecurity threats, which requires skilled staff and resources. Effective cybersecurity policy and strategy depend on the government's capacity to counter cyber threats, making this variable relevant to this dimension.

Government cybersecurity capacity is critical for mitigating harm from cyber threats. One important variable that gauges this capacity is the government's technical skills and resources to counter cyber-attacks. Evidence suggests that various governments are at different stages of developing these capacities. For instance, the WannaCry incident highlighted the urgent need for coordinated action and underscored the reality that many countries have outdated or ambiguous national legislation and methods for combating cybercrime. Governments that clamp down on physical protests are also extending these tactics into the digital realm, employing online surveillance of their citizens (Wall & Ward, 2017).

Furthermore, some governments intentionally use citizens' online activities as evidence against dissenting voices, showcasing the darker potential of technology. This underscores the importance of avoiding a simplistic perspective on technology solely as a liberating force for global citizens. While technology can increase transparency, oppressive governments can also utilise it for monitoring, control, and propaganda (Jeffrey, 2016). This situation implies that while some governments may have resources to combat unsophisticated cyber threats, they may lack the capacity to deal with more sophisticated attacks. This aligns with a response level of "1: Not

really" to "2: Somewhat" (Coppedge et al., 2024). The use of outdated laws to suppress dissent indicates limited technological advancement and strategic planning in cybersecurity, highlighting the need for significant improvements in both policy and resources to effectively counter sophisticated cyber threats.

Additionally, extreme government control over the Internet, as exemplified by Ethiopia's actions during periods of civil unrest, further indicates the disparity in cybersecurity capacity. The Ethiopian government shut down the Internet in 2016 after riots between police and the Oromo and Amhara ethnic groups, demonstrating a reactionary rather than a proactive approach to potential cyber threats (Freedom House, 2016). This reflects a limited capacity to effectively counteract cyber threats, corresponding to a lower response level in the government cybersecurity capacity variable.

2.8.2 Cybersecurity Culture and Society

The government social media monitoring variable from the DSP dataset will be used as a proxy measure for the culture and society dimension of the CMM.

Government social media monitoring

The government social media monitoring variable examines the comprehensiveness of government surveillance on social media, reflecting public perception and behaviour in cyberspace. It influences societal attitudes towards online privacy and security, which is a crucial element of cybersecurity culture.

The extent of government social media monitoring provides insight into the level of surveillance and control exercised over political content. Various countries exhibit different levels of comprehensiveness in their surveillance efforts. For example, the youth in Kenya are leveraging social media to highlight key governance concerns, including the misappropriation of government funds and corruption claims against government officials. Bloggers have faced charges under Section 132 of the Penal Code, a colonial-era law, for criticising government officials on social media (Jeffrey, 2016). This indicates that the government actively monitors social media content, particularly when it pertains to political dissent, suggesting a response level of "2: Somewhat comprehensive" to "3: Limited". This level of surveillance shows that while the government does not universally surveil all social media content, it prioritises

key political issues and acts against dissenting voices, reflecting a strategic but not all-encompassing approach to monitoring.

China's digital political environment is characterised by a complex relationship of censorship, surveillance, and control (Mechkova et al., 2024). The government allows online media to proliferate but exercises tight control over content, censoring any material deemed threatening to political stability. This censorship is carried out through a collaborative effort between government agencies, leaders, and different levels of government, with the surveillance of political content on social media being "0: extremely comprehensive" (Coppedge et al., 2024). Furthermore, the government engages in a massive and consistent campaign of astroturfing, with paid actors posting regime-friendly disinformation in a coordinated manner. While the government permits posts that reflect negatively on the government, giving a false impression of freedom of speech, it removes any discussion online that has the potential to lead to mass mobilisation or collective action (Mechkova et al., 2024). This extensive level of control and monitoring aligns with the highest response level of "0: Extremely comprehensive" (Coppedge et al., 2024), demonstrating a deeply entrenched and pervasive surveillance system aimed at maintaining political stability and control (Bennett & Naim, 2015).

2.8.3 Legal and Regulatory Frameworks

The government internet filtering capacity, government internet filtering in practice, government internet shut down capacity, privacy protection by law content, government online content regulation approach, and government capacity to regulate online content variables from the DSP dataset will be used as proxy measures for the legal and regulatory framework dimension of the CMM.

Government Internet filtering capacity

The government Internet filtering capacity variable assesses the government's technical ability to censor information online, which involves regulatory measures that authorise such actions. It reflects the legal framework that governs Internet filtering.

The capacity of governments to filter internet content has evolved alongside the advancement of digital technology and the increasing reliance on the Internet for

information dissemination. According to Irum and Al Sharqi (2015), countries use media censorship to control and manipulate information flow. In the digital age, the Internet's ability to rapidly disseminate information across borders has necessitated sophisticated surveillance and filtering tools to maintain societal order and suppress information that could challenge governmental authority, thus, indicating a response level of "2: The government has adequate capacity to block access to most, but not all, specific sites on the Internet if it wanted to" (Coppedge et al., 2024) or higher. Governments in China, Russia, and India have legalised electronic surveillance, enabling them to have comprehensive control over online activities (Shabaz, 2018). China's extensive measures, including its robust firewall, illustrate a high capacity to block objectionable content, aligning with response levels of “3” or “4” on the filtering capacity scale (Bennett & Naim, 2015).

Government Internet filtering in practice

The government Internet filtering in practice variable explores the frequency of government censorship practices. It reflects the enforcement of legal regulations concerning online content and the practical application of internet censorship laws.

The actual practice of internet filtering varies significantly across different political regimes. Authoritarian regimes and centralised governments often employ overt and covert censorship to stifle dissent and maintain control. Irum and Al Sharqi (2015) noted that tech-savvy activists have adapted to circumvent crude censorship methods, but governments have also evolved their strategies. Countries such as North Korea, Cuba, and China rank among the most censored globally, using tactics like limiting press freedom and manipulating media ownership to control information flow (Karlekar & Dunham, 2014). These practices reflect a high frequency of Internet filtering, with response levels such as "0: Extremely often" or "1: Often" (Coppedge et al., 2024).

In less mature democracies such as Hungary, Ecuador, Turkey, and Kenya, there is a concerning trend of adopting censorship practices observed in autocratic regimes (Bennett & Naim, 2015). Governments in these countries employ stealth censorship methods, outsourcing censorship responsibilities and exerting financial pressure on media entities to control information flow while maintaining a democratic façade, indicating a response level of "2: Sometimes" or "3: Rarely" (Coppedge et al., 2024), depending on the extent and subtlety of the practices used.

Government Internet shut down capacity

The government Internet shut down capacity variable examines the government's capacity to shut down Internet access, which is closely tied to legal and regulatory frameworks that govern such actions. It reflects the extent of governmental control over Internet infrastructure under legal frameworks.

There is a growing trend of Internet shutdowns in Africa, often coinciding with highly contested or closely fought elections, sparking concerns about censorship and the suppression of free expression. These shutdowns have become representative of a broader global divergence in internet governance and regulation perspectives. Governments across the continent justify these actions as necessary measures to combat misinformation, safeguard electoral integrity, and ensure national security. However, international organisations, non-governmental organisations, and social media platforms criticise shutdowns as unacceptable forms of censorship and information control. They argue that such actions are often abused by political actors to stifle dissenting voices and manipulate electoral outcomes (Bennett & Naim, 2015).

Stremlau and Dobson (2022) offer a distinct perspective by contextualising internet shutdowns within the historical continuum of information controls deployed during elections. Traditional forms of information management during elections, such as media blackouts and restrictions on public gatherings, are widely accepted and deemed as legitimate mechanisms to uphold competitive democratic processes. The authors raise critical questions about shutdowns' novelty and appropriateness as responses to genuine concerns about social media manipulation and election integrity. This historical perspective underscores the evolving strategies of governments to maintain control over information flow during sensitive periods.

Furthermore, Stremlau and Dobson (2022) explain that online content control is a crucial but frequently forgotten factor during the implementation of internet shutdowns which highlight social media companies' inability to effectively handle misinformation and disinformation in specific African contexts, particularly during sensitive periods of elections. This failure exacerbates the perceived need for Internet shutdowns, reflecting a governmental response level of "3: The government has the capacity to shut down roughly three-quarters of domestic access to the Internet" (Coppedge et al., 2024) or higher. The capacity to implement such extensive measures

demonstrates the significant control certain African governments exert over digital information channels during election times.

Privacy protection by law content

The privacy protection by law content variable examines the legal framework for protecting users' privacy and data. It reflects regulatory measures in place to safeguard personal information, a critical component of comprehensive cybersecurity legislation.

According to Makulilo (2015), data privacy protection efforts in Africa vary significantly across subregional groupings. The Economic Community of West African States (ECOWAS) is the initial and sole subregional organisation in Africa that has developed a structured framework for laws concerning data protection. This framework is outlined in the Supplementary Act on Personal Data Protection within ECOWAS, established in 2010. This comprehensive framework underscores the region's commitment to safeguarding personal data and privacy, aligning with a response level of "4: The legal framework explicitly allows the government to access personal information on the Internet only in extraordinary circumstances" (Coppedge et al., 2024).

The East African Community (EAC) has established two legal structures concerning data privacy: the EAC Legal Framework for Cyber Laws, drafted in 2011, and the EAC Bill of Rights, which received approval in 2012. These instruments provide a foundational basis for data privacy protections within the EAC, albeit with varying levels of enforceability and effectiveness. This situation reflects a response level of "3: The legal framework explicitly allows the government to access only a few types of personal information on the Internet" (Coppedge et al., 2024), indicating some level of protection but with room for improvement.

Similarly, the Southern African Development Community (SADC) introduced the SADC Model Law on Data Protection in 2012. However, there has been limited progress in making this law binding on member states, primarily due to implementation challenges. These regional instruments, except for the ECOWAS framework, are non-binding and serve as guidelines for member states to develop their national legislation on data privacy. This scenario aligns with a response level of "2: The legal framework explicitly allows the government to access many types of personal data on the

Internet" (Coppedge et al., 2024), indicating that while there are guidelines, their non-binding nature limits their effectiveness.

Internet legal regulation content

The internet legal regulation and content variables assesses the scope of content covered by internet regulations, reflecting the legal boundaries set by the government for online speech and content. It directly relates to the regulatory aspect of cybersecurity.

The type of content that is covered in the legal framework to regulate the Internet is a crucial dimension of government control. According to De Lanerolle (2016), the scope and enforcement of legal regulations on Internet content indicate a government's capacity to control online information. Governments with broad legal frameworks that allow for the removal of various types of content demonstrate extensive regulatory control. For example, laws enabling the removal of politically sensitive content align with a response level of "0: The state can remove any content at will" (Coppedge et al., 2024). This suggests that governments with comprehensive legal measures can exert significant control over online content (De Lanerolle, 2016).

The existence of the Access to Information Act and the misuse of older laws in Kenya highlight the complexity of the legal framework surrounding internet content regulation (The Bloggers Association of Kenya, 2016). This scenario aligns with a response level of "2: The legal framework is ambiguous. The state can remove some politically sensitive content, while other content is protected by law" (Coppedge et al., 2024), highlighting that while there are laws promoting transparency, there are also legal ambiguities that allow for the suppression of certain types of content.

Government online content regulation approach

The government online content regulation approach variable assesses whether the government either utilises its own resources or relies on private entities to monitor and regulate online content. It reflects the implementation and practical application of legal and regulatory frameworks concerning internet governance.

The extent to which a government uses its resources or relies on private actors to monitor and regulate online content is another key aspect of internet governance.

According to Makulilo (2015), the involvement of private sector entities in content regulation indicates a collaborative approach. Governments that distribute the regulatory burden to private actors, such as Internet Service Providers (ISPs), demonstrate a mixed approach to online content regulation. This aligns with the response level of "2: Some online content monitoring and regulation is done by the state, but the state also involves private actors in monitoring and regulation in various ways" (Coppedge et al., 2024). Such collaborations can be instrumental in expanding regulatory capacity, indicating that strategic partnerships with private actors are essential for effective online content management (Makulilo, 2015).

Government capacity to regulate online content

The government capacity to regulate online content variable assesses whether the government has the necessary staff and resources to ensure that online activity complies with existing regulations. By evaluating the government's capacity to remove illegal content and enforce its laws comprehensively, this variable reflects the quality and clarity of the legal frameworks in place.

The diverse cyber policies and data privacy efforts across Africa also relate to the variable, government capacity to regulate online content. For instance, while ECOWAS has a concrete framework, the implementation challenges faced by other regions like the EAC and SADC suggest limited regulatory capacity. This aligns with a response level of "2: Somewhat. The state has the capacity to regulate only some online content or some portions of the law" Coppedge et al., 2024), indicating that while there is some capacity to regulate, it is not comprehensive across all regions.

A government’s capacity to regulate online content is influenced by its resources and institutional frameworks. According to the Bloggers Association of Kenya (2016), governments with sufficient resources and well-established institutions can regulate a broad spectrum of online content, aligning with the response level of "4: Yes, the government has sufficient capacity to regulate all online content". This suggests that strategic partnerships and collaborations with private actors are vital for comprehensive online content regulation (The Bloggers Association of Kenya, 2016).

2.9 Combination of CSS as the Theoretical Framework and CMM as the Conceptual Framework

By framing government cybersecurity capacity as a concept shaped by social and political factors, including law, practice, and institutional dynamics, CSS enables an examination of how and why states address cyber threats, enhance surveillance, and build capacity in response to perceived risks. This approach justifies the choice of DSP variables related to Internet monitoring, filtering, regulation, and shutdown capacity.

The CMM offers a structured method for assessing national cybersecurity capacity, focusing on areas such as cybersecurity policy and strategy, culture and society, and the legal and regulatory framework. DSP variables, such as Internet filtering, shutdown, social media monitoring, privacy law, and regulatory capacity serve as proxy indicators for three CMM dimensions, supporting the rationale for selecting these DSP variables.

2.10 Summary

This literature review has examined cybersecurity and digital readiness indices (the GCI, NCSI, NRI, and CDI) and identified important differences in cybersecurity capacity between African, developing, and developed countries. The review highlighted the challenges that African and developing countries face when building cybersecurity capacity, including resource constraints, limited digital skills, weak institutions, inadequate policies, political instability, and insufficient national and international cooperation.

The literature review explored how governments use digital control and surveillance mechanisms through the lens of CSS, examining securitisation processes, offensive and defensive cyber operations, and the roles of state and non-state actors. It demonstrated that cybersecurity governance differs between democratic and authoritarian systems, with varying approaches to surveillance and digital control. African countries employ diverse strategies—from internet shutdowns to social media monitoring and censorship—often justified under national security narratives. These practices reveal tensions between government efforts to build cybersecurity capacity and the protection of digital rights and freedoms.

The Oxford GCSCC CMM provided a structured framework for this study, offering five dimensions for assessing cybersecurity capacity: cybersecurity policy and strategy, cybersecurity culture and society, building cybersecurity knowledge and capabilities, legal and regulatory frameworks, and standards and technologies. By aligning DSP variables with CMM dimensions, this study identified proxy measures that reflect government cybersecurity capacity development across these dimensions.

CSS serves as the theoretical framework for this study, enabling examination of how governments securitise digital threats and build cybersecurity capacity in response to perceived risks. The DSP variables—including Internet filtering, Internet shutdowns, social media monitoring, privacy law, and regulatory capacity—correspond with CSS concepts of securitisation, power dynamics, and the gap between formal capacity and operational practice. This combination of CSS as the study's theoretical framework and CMM as the study's conceptual framework provides a robust approach for investigating the determinants of government cybersecurity capacity in African and developing countries.

Chapter 3: Research Methodology

This chapter outlines the research approach, data source, data preparation and analysis, reasons for using ordinal variables and ordinal logistic regression models, and statistical techniques used to deal with heteroscedasticity and heterogeneity while investigating the relationships between digital media freedom, state Internet regulation practices, and government cybersecurity capacity. It also introduces the sub-hypotheses (i.e., statistical hypotheses), which are assessed and discussed in the Results and Discussion chapter. This chapter concludes with a brief discussion on how the researcher considered ethical issues and the limitations of this study.

3.1 Research Approach

The study employed a quantitative research approach using secondary data. Ordinal logistic regression models were used to examine the relationship between government cybersecurity capacity (the dependent variable) and eight independent variables related to digital media freedom and state Internet regulation capacity and approach.

The decision to use ordinal logistic regression is primarily influenced by the nature of the dependent variable, government cybersecurity capacity, which comprises of ordered categories. Unlike multinomial logistic regression, which disregards inherent ordering and compromises statistical power, this model explicitly utilises the hierarchy in response levels. It does so by modelling cumulative probabilities through proportional odds, assuming consistent predictor effects across outcome thresholds, thereby enhancing interpretability and efficiency.

By respecting the ordinal structure, the model avoids the unrealistic assumption of equal interval spacing required by linear regression, while more robustly capturing trends than methods that treat the outcome as nominal. Validating the proportional odds assumption ensures the model's appropriateness, making it the theoretically aligned and statistically efficient choice for ordered outcomes.

3.2 Data Source

The study utilised data from the sixth version of the publicly available, open-source DSP dataset (Mechkova et al., 2024). This version is a country-year longitudinal

dataset that comprises of 179 countries and 35 indicators from 2000 to 2023 (Digital Society Project, 2024a; Mechkova et al., 2024). The DSP dataset examines the political landscape of the Internet and social media, containing specific indicators relevant to this study, such as government cybersecurity capacity, Internet filtering practices, and social media monitoring (Coppedge et al., 2024). The Varieties of Democracy Institute (V-Dem) provided the infrastructure for the collection of the DSP data (Digital Society Project, 2024b).

3.3 Data Collection and Expert Judgments

According to Coppedge et al. (2024), V-Dem uses a rigorous recruitment process to select expert coders (Country Experts) to ensure that the data collected is accurate and reliable. At least five Country Experts are allocated for each country-year indicator, with a minimum of three experts being citizens or permanent residents of the country that is being analysed. This approach helps mitigate potential biases and ensures that the data that has been collected is informed by local knowledge and expertise (Coppedge et al., 2024).

The recruitment protocol of V-Dem involves a thorough vetting process wherein potential Country Experts are evaluated based on five key criteria (Coppedge et al., 2024). First, their expertise in the relevant country and thematic areas is assessed, typically demonstrated through advanced degrees, publications, and professional experience. Second, consideration of their connection to the country, with a preference for nationals or permanent residents. Third, evaluate their willingness to devote time and effort to the project and their ability to deliberate carefully over the survey questions. Fourth, prioritisation of impartiality, avoiding individuals with potential conflicts of interest or biases. Lastly, V-Dem evaluates Country Experts based on the diversity of their professional backgrounds.

3.4 Addressing Challenges in Expert-Coded Data

While expert-coded data are invaluable, they pose several challenges, primarily due to the variability in judgments across different experts and contexts. To address these issues, V-Dem uses a sophisticated measurement model that aggregates expert-coded data while accounting for uncertainties and potential biases (Marquadt, 2023). The model is based on the premise that the concepts being measured are unobserved

but can be inferred from the imperfect manifestations captured by expert ratings (Marquadt, 2023; Coppedge et al., 2024).

3.5 Measurement Model

The V-Dem measurement model operates by converting the ordinal categories used by experts to a single continuous latent scale, thereby estimating the values of the unobserved concepts (Coppedge et al., 2024). This process involves several key steps such as reliability and scale perception, overlapping coding and anchoring vignettes, and output and credible regions.

3.5.1 Reliability and Scale Perception

The model estimates the reliability of each expert relative to others and the degree to which their perception of the response scale differs. This is achieved through iterative estimation, where the model weights an expert's contribution based on their reliability and scale perception.

3.5.2 Overlapping Coding and Anchoring Vignettes

Patterns of overlapping coding (i.e., experts coding multiple countries) and the use of hypothetical cases (i.e., anchoring vignettes) help in estimating systematic differences in scale perception across different sets of experts. This ensures that the final estimates account for these variations and provide a consistent measure across cases.

3.5.3 Output and Credible Regions

The output of the model is an interval-level point estimate of the latent trait, typically ranging from -5 to 5, along with its associated measurement error. These point estimates are the best representation of the unobserved concepts for use in statistical analysis.

3.6 Data Presentation

V-Dem provides several versions of the estimates of the DSP data to facilitate interpretation and usability (Coppedge et al., 2024):

i. Interval-Level Point Estimates

These estimates are directly output from the measurement model and are suitable for statistical analysis.

ii. Transformed Interval-Level Estimates

To aid substantive interpretation, these estimates are linearly transformed back to the original coding scale used by the experts, typically ranging from 0 to 4.

iii. Ordinal Versions

For applications requiring ordered categorical values, V-Dem also provides ordinal versions of each variable, along with credible regions for each type of estimate (Coppedge et al., 2024).

3.7 Variables used in the study

Table 3.1: Description of variables

Dependent variable	**Description**		
v2smgovcapsec	**Government cyber security capacity**		
No	No. The government does not have the capacity to counter even unsophisticated cyber security threats.		
Not Really	Not really. The government has the resources to combat only unsophisticated cyber attacks.		
Some what	Somewhat. The government has the resources to combat moderately sophisticated cyber attacks.		
Mostly	Mostly. The government has the resources to combat most sophisticated cyber attacks.		
Yes	Yes. The government has the resources to combat sophisticated cyber attacks, even those launched by highly skilled actors.		
Independent Variables	**Digital Media Freedom**	**State Internet Regulation Capacity and Approach**	
v2smgovfilcap	**Government Internet filtering capacity**	**v2smregcon**	**Internet legal regulation content**
No Capacity	The government lacks any capacity to block access to any sites on the Internet.	Any Content	The state can remove any content at will.
Limited Capacity	The government has limited capacity to block access to a few sites on the Internet.	Remove Most Content	The state can remove most content, and the law protects speech in only specific, and politically uncontroversial contexts.
Adequate Capacity	The government has adequate capacity to block access to most, but not all, specific sites on the Internet if it wanted to.	Ambiguous Framework	The legal framework is ambiguous. The state can remove some politically sensitive content, while other is protected by law.
Complete Capacity	The government has the capacity to block access to any sites on the Internet if it wanted to.	Remove Controversial Content	The law protects most political speech, but the state can remove especially politically controversial content.

v2smgovfilprc	**Government Internet filtering in practice**
Extremely Often	Extremely often. It is a regular practice for the government to remove political content, except to sites that are pro-government.
Often	Often. The government commonly removes online political content, except sites that are pro-government.
Sometimes	Sometimes. The government successfully removes about half of the critical online political content.
Rare	Rarely. There have been only a few occasions on which the government removed political content.
Never	Never, or almost never. The government allows Internet access that is unrestricted, with the exceptions mentioned in the clarifications section.
v2smgovshutcap	**Government Internet shut down capacity**
No Capacity	The government lacks the capacity to shut down any domestic Internet connections.
Quarter	The government has the capacity to shut down roughly a quarter of domestic access to the Internet.
Half	The government has the capacity to shut down roughly half of domestic access to the Internet.
Three Quarter	The government has the capacity to shut down roughly three quarters of domestic access to the Internet.
Complete	The government has the capacity to shut down all, or almost all, domestic access to the Internet.
v2smgovsmmon	**Government social media monitoring**
Extremely comprehensive	Extremely comprehensive. The government surveils virtually all content on social media.
Mostly Comprehensive	Mostly comprehensive. The government surveils most content on social media, with comprehensive monitoring of most key political issues.
Somewhat Comprehensive	Somewhat comprehensive. The government does not universally surveil social media but can be expected to surveil key political issues about half the time.
Limited	Limited. The government only surveils political content on social media on a limited basis.
Not at all	Not at all, or almost not at all. The government does not surveil political content on social media, with the exceptions mentioned in the clarifications section.
Remove if violate legal criteria	The law protects political speech, and the state can only remove content if it violates well-established legal criteria.
v2smprivcon	**Privacy protection by law content**
Any Type	The legal framework explicitly allows the government to access any type of personal data on the Internet.
Most types	The legal framework explicitly allows the government to access most types of personal data on the Internet.
Many Types	The legal framework explicitly allows the government to access many types of personal data on the Internet.
Few Types	The legal framework explicitly allows the government to access only a few types of personal information on the Internet.
Only Extraordinary circumstances	The legal framework explicitly allows the government to access personal information on the Internet only in extraordinary circumstances.
v2smregcap	**Government capacity to regulate online content**
No	No, almost all online activity happens outside of reach of the state, where it lacks the capacity to remove illegal content.
Not Really	Not really. The state has extremely limited resources to regulate online content.
Some What	Somewhat. The state has the capacity to regulate only some online content or some portions of the law.
Mostly	Mostly. The state has robust capacity to regulate online content, though not enough to regulate all content and all portions of the law.
Sufficient	Yes, the government has sufficient capacity to regulate all online content.
v2smregapp	**Government online content regulation approach**
All Content	All online content monitoring and regulation is done by the state.
Most Content	Most online content monitoring and regulation is done by the state, though the state involves private actors in a limited way.
Some Content	Some online content monitoring and regulation is done by the state, but the state also involves private actors in monitoring and regulation in various ways.
Little Content	The state does little online content monitoring and regulation, and entrusts most of the monitoring and regulation to private actors.

	None	The state off-loads all online content monitoring and regulation to private actors.

Source: Coppedge et al. (2024)

The study investigated the relationship between government cybersecurity capacity and eight factors related to digital media freedom and state Internet regulation capacity and approach.

The independent variables included in the study measure government Internet filtering capacity, government Internet filtering in practice, government Internet shutdown capacity, and government social media monitoring. Additionally, the study examined the impact of Internet legal regulation content, privacy protection by law, government capacity to regulate online content, and government online content regulation approach on government cybersecurity capacity. These eight independent variables represent different aspects of a government's ability to control and monitor the digital landscape, which may have significant implications for its overall cybersecurity capacity (Merhi & Bregu, 2020). The names of these variables and their corresponding descriptions have been provided in Table 3.1 above.

3.8 Data Preparation and Analysis

Stata was used to conduct the data analysis and extract the results (StataCorp, 2024). The dataset was checked for missing values and inconsistencies. South Sudan and Palestine/Gaza were excluded from the analysis because of the insufficient number of data points available for these countries. Including these countries in the analysis would have resulted in unreliable and potentially biased estimates due to their limited data. Additionally, insufficient data points do not provide a robust basis for drawing meaningful conclusions or ensuring the statistical power necessary for ordinal logistic regressions. Ultimately, excluding these two countries ensured the integrity and reliability of the study's findings, allowing for more accurate and generalisable insights into the relationship between the independent variables and government cybersecurity capacity in African and developing countries.

3.9 Justification for using Ordinal Variables

Both theoretical and practical considerations justify the decision to use ordinal variables from the DSP dataset. In theory, the concepts under investigation, such as

government cybersecurity capacity, are inherently ordinal. These variables represent ordered categories that reflect varying levels of capacity rather than precise, measurable quantities. Using ordinal variables aligns with the nature of the data and provides a more accurate representation of the underlying constructs.

In practice, attempts to estimate the ordinal logistic model using continuous versions of the variables, such as mean and median values, led to significant convergence issues. These issues arose because continuous variables often introduce complexities in the estimation process, particularly when the underlying data does not meet the assumptions required for treating them as continuous. The ordinal logistic model is specifically designed to handle ordinal data, where the focus is on the order of categories rather than exact numerical differences between them. This model effectively captures the ordinal nature of the data, ensuring reliable and interpretable results.

Furthermore, using continuous dependent variables in this context is inappropriate because the DSP dataset was derived from expert judgments that are best understood within an ordinal framework. The transformation of these ordinal ratings into continuous scales, such as means or medians, would not only obscure the ordinal relationships but also potentially introduce biases and inaccuracies. Continuous measures assume equal intervals between points, which do not necessarily exist in expert-coded data. Therefore, the use of ordinal variables maintains the integrity of the data, aligns with the theoretical underpinnings of the measured constructs, and avoids the convergence issues with continuous variable versions. This approach ensures that the analysis remains robust, valid, and accurately reflects the nature of government cybersecurity capacity.

3.10 Justification for using Ordinal Logistic Regression Models

Given the ordinal nature of the dependent variable, government cybersecurity capacity (v2smgovcapsec), which ranges from 0 to 4, the ordinal logistic regression model is a more appropriate choice to use in comparison to linear probability models (DeMaris, 1995).

Unlike linear regression, which assumes a continuous and normally distributed dependent variable, ordinal logistic regression is designed to handle ordinal data

where the response categories have a natural ordering (Kauermann, 2000). This is crucial as the different levels of the outcome variable represent a clear progression in the government's ability to counter cyber threats, from complete inability to the capacity to combat even highly sophisticated attacks.

Using linear probability models is not suitable for this type of ordinal dependent variable (Peng et al., 2002). These models assume a linear relationship between the predictors and the outcome, which does not align well with the inherent ordering of the response categories. Moreover, linear probability models can produce fitted values outside the 0 to 1 range, leading to predictions that are nonsensical in the context of an ordinal dependent variable (Stoltzfus, 2011).

Conversely, the ordinal logistic regression model uses a cumulative logit link function to capture the ordered nature of the dependent variable (Kauermann, 2000). This link function transforms the ordinal outcome into a linear combination of the predictors, allowing for the estimation of the probability of each response category given the values of the independent variables.

The model parameters in an ordinal logistic regression, known as logits, represent the log-odds of being at or below a particular response category, providing a more meaningful interpretation than the linear coefficients of a linear probability model (Hosmer & Lemeshow, 2000). This ordinal structure is crucial in the study, as it allows for a nuanced understanding of how the independent variables influence the government's capacity to address cybersecurity threats at different levels of sophistication.

The ordinal logistic regression model is the more suitable choice for analysing the dependent variable, as it can appropriately model the ordered categorical nature of the dependent variable, leading to more accurate and interpretable results compared to linear probability models.

Linear probability models assume a linear relationship between the predictors and the outcome variable, which can be expressed as:

$$P(Y = 1|X) = \beta_0 + \beta_i X_i$$

where P is the probability of the outcome, β_0 is the intercept, β_i is the slope coefficient, and X_i is the predictor variable.

This linear formulation can lead to predictions outside the 0 to 1 range, which is problematic for an ordinal dependent variable.

The ordinal logistic regression model, on the other hand, uses a cumulative logit link function to capture the ordered nature of the response variable. The cumulative logit is defined as the log of the odds of being at or below a particular response category:

$$logit(p) = \log\left(\frac{p}{1-p}\right)$$

Where is the probability of a positive response.

This formulation ensures that the predicted probabilities for each response category are non-negative and sum to 1, addressing the limitation of linear probability models that can produce fitted values outside the 0 to 1 range.

Moreover, the logit coefficients represent the change in the log-odds of being at or below a particular response category for a unit change in the predictor (i.e., independent) variable, which provides a more meaningful interpretation compared to the linear coefficients of a linear probability model.

3.11 Data Categorisation and Model Estimation

The DSP dataset was divided into two distinct categories: African countries and developing countries. Countries were categorised as "African" according to V-Dem's handbook on country coding units (Coppedge et al., 2024). "Developing" countries were defined as those that did not fit into either the "African" or "developed" categories. Developed countries are those that meet certain criteria, such as having an HDI of 0.80 or higher (United Nations Development Programme, 2024), being classified as advanced economies by the IMF (2024), being considered high-income economies by the World Bank (2024), and having a GDP per capita (purchasing power parity) exceeding US$25,000 per year (International Monetary Fund, 2024).

Due to a low number of observations, South Sudan was excluded from the analysis of African countries, and Palestine/Gaza was excluded from the analysis of developing

countries. This study does not include developed countries in its analysis. The final analysis focused on 50 African and 90 developing countries.

3.12 Structure of Regression Models

Four different ordinal logistic regression models were used to systematically include the eight independent variables in African and developing countries.

The first model included two key variables: Government Internet filtering capacity (v2smgovfilcap) and Government Internet filtering in practice (v2smgovfilprc). These variables are fundamental in understanding government control over Internet content.

The second model focused exclusively on Government Internet shut down capacity (v2smgovshutcap), which examines governments' broader power over Internet access.

The third model incorporated two variables: Government social media monitoring (v2smgovsmmon) and Internet legal regulation content (v2smregcon).

In the fourth model, three additional variables were analysed. The variables included in this model are Privacy protection by law content (v2smprivcon), Government capacity to regulate online content (v2smregcap), and Government online content regulation approach (v2smregapp),

This structured statistical modelling approach enables a detailed investigation into how digital media freedom and state internet regulation impact government cybersecurity capacity in African and developing countries. It also helps address and mitigate methodological challenges encountered during the estimation process.

According to Mark and Sul (2003), heteroscedasticity, or the unequal variance of the error terms, can be addressed by using robust standard errors (Mark & Sul, 2003). Robust standard errors are a type of standard error estimation that is robust to the presence of heteroscedasticity, which can lead to incorrect inferences if not properly accounted for. Robust standard errors for inference and testing of the regression coefficients were used in the ordinal logistic regression models to account for potential heteroscedasticity.

Given the cross-sectional nature of the data, autocorrelation was not a primary concern. This is because autocorrelation mainly affects models where observations are ordered sequentially or spatially, which is often not the case with categorical independent variables (Florax & De Graaff, 2004). The study used categorical independent variables, which help address the challenges associated with the assumptions of normality (Giacalone et al., 2018) and multicollinearity commonly found in classical regression models (Midi et al., 2010; Shrestha, 2020). By their inherent nature, categorical independent variables offer a more straightforward modelling approach, eliminating the need for transformations or complex collinearity diagnostics typically required with continuous variables.

According to Swamy and Fikkert (2002), the inclusion of country and time fixed effects in the models help to address the issue of heterogeneity, or the presence of unobserved factors that vary across countries and/or time periods and may be correlated with the independent variables. Fixed effects models control for all time-invariant characteristics of a country and all country-invariant characteristics over time, thereby reducing the risk of omitted variable bias (Swamy & Fikkert, 2002). The study employed country and time fixed effects in the ordinal logistic regression models to address the potential issue of heterogeneity in the data.

3.13 Sub-hypotheses

Based on the variables used in the study, the below mentioned sub-hypotheses (i.e., statistical hypotheses) will be assessed and discussed in the Results and Discussion chapter of this study.

Table 3.2: Null and Alternative Hypotheses

	Null Hypothesis	Alternative Hypothesis
1	There is no significant relationship between government Internet filtering capacity and government cybersecurity capacity.	There is a significant relationship between government Internet filtering capacity and government cybersecurity capacity.
2	There is no significant relationship between government Internet filtering in practice and government cybersecurity capacity.	There is a significant relationship between government Internet filtering in practice and government cybersecurity capacity.

3	There is no significant relationship between government Internet shutdown capacity and government cybersecurity capacity.	There is a significant relationship between government Internet shutdown capacity and government cybersecurity capacity.
4	There is no significant relationship between government social media monitoring and government cybersecurity capacity.	There is a significant relationship between government social media monitoring and government cybersecurity capacity.
5	There is no significant relationship between Internet legal regulation content and government cybersecurity capacity.	There is a significant relationship between Internet legal regulation content and government cybersecurity capacity.
6	There is no significant relationship between privacy protection by law content and government cybersecurity capacity.	There is a significant relationship between privacy protection by law content and government cybersecurity capacity.
7	There is no significant relationship between government capacity to regulate online content and government cybersecurity capacity	There is a significant relationship between government capacity to regulate online content and government cybersecurity capacity.
8	There is no significant relationship between government online content regulation approach and government cybersecurity capacity.	There is a significant relationship between government online content regulation approach and government cybersecurity capacity.

3.14 Ethical Considerations

The study did not involve animal experimentation or the use of human subjects, human tissue or other material, or patient records so it should not have any ethical risks.

The DSP dataset does not contain the personal information of any individuals and V-Dem has policies in place to ensure that the identity of their Country Experts are not revealed (Coppedge et al., 2024).

Additionally, the researcher received an ethics waiver clearance (Protocol Number: WSG-2023-08W) from the Wits School of Governance's Ethics Committee to conduct this study.

3.15 Limitations

While this study provides valuable insights into the determinants of government cybersecurity capacity in African and developing countries using the DSP dataset, several limitations must be acknowledged. These limitations can be summarised as follows:

3.15.1 Data Limitations

- The use of ordinal variables might reduce the precision of the analysis and potentially lead to information loss; and
- The DSP dataset, while comprehensive, relies on expert assessments that could be subjective and may not cover all aspects of cybersecurity capacity.

3.15.2 Regional Focus

The study's focus on African and developing countries limits the generalisability of findings to other regions of the world.

3.15.3 Scope Limitations

- The focus on the aggregate trends of specific regions and the absence of sub-national analysis might overlook variations in cybersecurity capacity within countries and between different types of countries; and
- The set of determinants examined are not exhaustive, and the study does not explore the broader implications of cybersecurity capacity for other important outcomes such as socio-economic development or national security.

3.15.4 Methodological Limitation

The study's reliance on quantitative analysis limits the researcher's ability to fully understand the contexts and motivations behind government actions related to digital media freedom and state approaches to Internet regulation.

3.16 Summary

This chapter has outlined the research methodology employed in this study to investigate the relationship between digital media freedom, state Internet regulation, and government cybersecurity capacity. The study uses a quantitative approach and analysed data from the sixth edition of the Digital Society Project (DSP) dataset using ordinal logistic regression models.

The chapter first detailed the rigorous data collection and expert judgement processes used to develop the DSP dataset, before describing the data preparation and analysis steps. South Sudan and Palestine/Gaza were excluded due to insufficient data points. The rationale for using ordinal variables and ordinal logistic regression models was explained, highlighting the ordinal nature of the dependent variable and the convergence problems encountered when attempting to use continuous variables instead.

The dataset was then divided into two groups: African countries and developing countries. Separate regression models were estimated for each group to examine the eight independent variables. Methodological challenges, including heteroscedasticity and heterogeneity, were addressed by using robust standard errors and country and time fixed effects. Eight null and alternative sub-hypotheses were formulated to provide a clear framework for the subsequent data analysis and discussion.

Despite its contributions, the study has certain limitations. These include the use of ordinal variables, which may reduce analytical precision, reliance on potentially subjective expert assessments, a regional focus limited to African and developing countries, examination of aggregate trends rather than country-specific variations, and reliance on quantitative analysis alone which limits insight into the context and motivations behind government actions.

The following chapter will present and discuss the results of the analysis based on this research methodology.

Chapter 4: Results and Discussion

This study offers a detailed examination of the effect that various digital media freedom and state internet regulation factors have on government cybersecurity capacity in African and developing countries. The frequency distributions provide a descriptive overview of the data, highlighting the heterogeneity in responses across the different categories of variables. The ordinal logistic regression results offer insights into the relationships between the dependent variable and the independent variables, controlling for the ordinal nature of the data. The findings indicate significant variations in the relationships between the variables for African and developing countries, suggesting that country-specific and time-specific factors should be considered in the analysis. In this chapter, the researcher presents the findings of the quantitative analysis, provides a summary of the results, and discusses the key findings of the study.

4.1 Descriptive Statistics

4.1.1 African Countries

Table 4.1: Frequency distributions for African Countries

	Freq.	Per.	Cum.		Freq.	Per.	Cum.
v2smgovcapsec				**v2smregcap**			
No	89	7.42	7.42	No	51	4.25	4.25
Not Really	668	55.67	63.08	Not Really	555	46.25	50.5
Somewhat	422	35.17	98.25	Somewhat	422	35.17	85.67
Mostly	21	1.75	100	Mostly	172	14.33	100
Total	1200	100		Total	1200	100	
v2smgovfilcap				**v2smregapp**			
No Capacity	21	1.75	1.75	All Content	135	11.25	11.25
Limited Capacity	448	37.33	39.08	Most Content	367	30.58	41.83
Adequate Capacity	493	41.08	80.17	Some Content	598	49.83	91.67
Complete Capacity	238	19.83	100	Little Content	100	8.33	100
Total	1200	100		Total	1200	100	
v2smgovfilprc				**v2smregcon**			
Extremely Often	22	1.83	1.83	Any Content	66	5.5	5.5
Often	98	8.17	10	Remove Most Content	145	12.08	17.58
Sometimes	222	18.50	28.5	Ambiguous Framework	349	29.08	46.67
Rarely	589	49.08	77.58	Remove Controversial Content	293	24.42	71.08
Never	269	22.42	100	Remove if violate legal criteria	347	28.92	100
Total	1200	100		Total	1200	100	
v2smgovshutcap				**v2smprivcon**			
No Capacity	32	2.67	2.67	Any Type	29	2.5	2.5
Quarter	130	10.83	13.5	Most types	121	10.42	12.92
Half	144	12.00	25.5	Many Types	344	29.63	42.55
Three Quarter	283	23.58	49.08	Few Types	300	25.84	68.39
Complete	611	50.92	100	Only Extraordinary circumstances	367	31.61	100
Total	1200	100		Total	1161	100	
v2smgovsmmon							
Extremely comprehensive	3	0.25	0.25				
Mostly Comprehensive	233	19.42	19.67				
Somewhat Comprehensive	484	40.33	60				
Limited	393	32.75	92.75				
Not at all	87	7.25	100				
Total	1200	100					

Source: Author's computation using Stata

The results for the African countries presented in Table 4.1 above, are interpreted as follows:

Government cyber security capacity (v2smgovcapsec)

A small proportion of African governments (approximately 7.42%) do not have the capacity to counter even unsophisticated cybersecurity threats. The majority of African governments (55.67%) have the resources to combat only unsophisticated cyberattacks. Over a third of African governments (35.17%) have the resources to combat moderately sophisticated cyber-attacks, while a small minority (1.75%) have the resources to combat the most sophisticated cyberattacks.

These findings indicate that a significant majority of African governments lack the capacity to deal with sophisticated cyber threats, with most only equipped to handle unsophisticated attacks.

Government Internet filtering capacity (v2smgovfilcap)

A small proportion of African governments (1.75%) lack the capacity to block access to Internet sites. However, a significant proportion (37.33%) have limited capacity to block a few sites on the Internet. Most African governments (41.08%) have adequate capacity to block most specific sites on the Internet, while nearly one-fifth (19.83%) have complete capacity to block any sites on the Internet. These findings suggest that many African governments have some level of ability to filter Internet content, with a significant proportion having limited or adequate capacity to do so.

These findings indicate that while a small proportion of African governments lack filtering capacity, a substantial portion have either limited or adequate capacity. This indicates a potential risk for Internet censorship, even if not all African governments currently exercise this power extensively.

Government Internet filtering in practice (v2smgovfilprc)

A small proportion (1.83%) of African governments engage in extremely frequent Internet filtering, regularly removing political content except from pro-government sites. 8.17% of African governments often filter online political content, except for sites that are pro-government. A significant proportion (18.5%) of governments sometimes filter critical online political content, successfully removing about half of it. Almost half of African governments (49.08%) rarely filter political content, with only a few instances

of removal. Over one-fifth (22.42%) of African governments never, or almost never, filter the Internet, allowing unrestricted access with some exceptions.

These findings suggest varying levels of Internet filtering in practice. While nearly half of African governments rarely filter content, a significant minority does so occasionally or even more frequently.

Government Internet shut down capacity (v2smgovshutcap)

A small proportion of African governments (2.67%) lack the capacity to shut down any domestic Internet connections. Just over one-tenth of African governments (10.83%) have the capacity to shut down roughly a quarter of domestic access to the Internet, while a similar proportion (12%) have the capacity to shut down roughly half of domestic access to the Internet. A significant proportion of African governments (23.58%) have the capacity to shut down roughly three-quarters of domestic access to the Internet, while most African governments (50.92%) have the capacity to shut down all, or almost all, domestic access to the Internet.

These findings suggest that the majority of African governments have the capacity to shut down most or all domestic internet access. This highlights the concerning potential for widespread disruptions to communication and information flow.

Government social media monitoring (v2smgovsmmon)

A very small proportion of African governments (0.25%) have extremely comprehensive social media monitoring, surveilling virtually all content. About one-fifth of African governments (19.42%) have mostly comprehensive monitoring, surveilling most content and key political issues. A significant proportion of African governments (40.33%) have somewhat comprehensive monitoring, surveilling key political issues about half the time. Almost one-third of African governments (32.75%) have limited social media monitoring, only surveilling political content on a limited basis. Lastly, approximately 7.25% of African governments do not surveil political content on social media.

These findings suggest a wide range of social media surveillance, from limited to mostly comprehensive, which could indicate that African governments have varying degrees of interest in monitoring online political content.

Government capacity to regulate online content (v2smregcap)

A small proportion of African governments (4.25%) lack the capacity to regulate online content, with almost all online activity falling outside of government control. Approximately 46.25% of African governments have extremely limited resources to regulate online content. A significant proportion of African governments (35.17%) have some capacity to regulate online content, but only for certain types of content or portions of the law. About 14.33% of African governments have robust capacity to regulate online content, though not enough to regulate all content and all portions of the law.

These findings suggest that a significant majority of African governments face challenges in regulating online content due to limited resources and capacity. This indicates that the majority of governments are unable to effectively monitor and control all online activity within their borders.

Government online content regulation approach (v2smregapp)

About 11.25% of African governments monitor and regulate all online content by themselves. A significant proportion of African governments (30.58%) monitor and regulate most content, but private actors are only involved in a limited way. Almost half of African governments (49.83%) monitor and regulate some content themselves, while also involving private actors in monitoring and regulation in various ways. The smallest proportion of African governments (8.33%) offload all online content monitoring and regulation to private actors.

These findings suggest that a small minority of African governments choose to fully regulate online content, and many rely on private actors for assistance. This could lead to inconsistencies in regulation and potential challenges in holding private actors accountable.

Internet legal regulation content (v2smregcon)

In approximately 5.5% of African countries, the state has the authority to remove any online content. In a significant proportion of African countries (12.08%), the state can remove most content, with legal protections for speech limited to specific, non-political contexts. About 29.08% of African countries exhibit ambiguous legal frameworks

where the state can censor politically sensitive content while other forms of expression remain protected. In about 24.42% of African countries, the law protects most political speech, but the state retains the power to remove particularly controversial content. A substantial proportion of African countries (28.92%) have robust legal protections for political speech, allowing content removal only in cases of clear legal violations.

These findings suggest that while a significant proportion of African countries have legal frameworks aimed at protecting political speech, many also grant the state the authority to remove content under specific circumstances. This suggests a complex legal landscape where freedom of expression may be vulnerable to varying degrees of government intervention.

Privacy protection by law content (v2smprivcon)

A small minority (2.50%) of African countries have legal frameworks that explicitly allow their government unrestricted access to online personal data. In contrast, 10.42% permit access to most types of online personal data, and a substantial proportion (29.63%) allow access to many types of online personal data. However, 25.84% of countries restrict government access to only a few types of online personal data, and a significant proportion (31.61%) permit access to online personal data only under extraordinary circumstances.

These findings indicate that while a considerable proportion of African countries have legal frameworks in place to protect online personal data, a concerning minority allow broad government access. This raises concerns about data privacy and surveillance practices within African countries.

4.1.2 Developing Countries

Table 4.2: Frequency distributions for Developing Countries

	Freq.	Per.	Cum.		Freq.	Per.	Cum.
v2smgovcapsec				**v2smregcap**			
No	111	5.14	5.14	No	106	4.91	4.91
Not Really	725	33.56	38.7	Not Really	765	35.42	40.32
Somewhat	720	33.33	72.04	Somewhat	623	28.84	69.17
Mostly	510	23.61	95.65	Mostly	523	24.21	93.38
Yes	94	4.35	100	Sufficient	143	6.62	100
Total	2160	100		Total	2160	100	
v2smgovfilcap				**v2smregapp**			
No Capacity	178	8.24	8.24	All Content	455	21.06	21.06
Limited Capacity	755	34.95	43.19	Most Content	454	21.02	42.08
Adequate Capacity	476	22.04	65.23	Some Content	935	43.29	85.37
Complete Capacity	751	34.77	100	Little Content	292	13.52	98.89
Total	2160	100		None	24	1.11	100
v2smgovfilprc				Total	2160	100	
Extremely Often	186	8.61	8.61	**v2smregcon**			
Often	296	13.70	22.31	Any Content	268	12.41	12.41
Sometimes	373	17.27	39.58	Remove Most Content	266	12.31	24.72
Rarely	566	26.20	65.79	Ambiguous Framework	504	23.33	48.06
Never	739	34.21	100	Remove Controversial Content	341	15.79	63.84
Total	2160	100		Remove if violate legal criteria	781	36.16	100
v2smgovshutcap				Total	2160	100	
No Capacity	231	10.69	10.69	**v2smprivcon**			
Quarter	499	23.10	33.8	Any Type	6	0.29	0.29
Half	324	15.00	48.8	Most types	363	17.62	17.91
Three Quarter	268	12.41	61.2	Many Types	411	19.95	37.86
Complete	838	38.80	100	Few Types	555	26.94	64.81
Total	2160	100		Only Extraordinary circumstances	725	35.19	100
v2smgovsmmon				Total	2060	100	
Extremely comprehensive	94	4.35	4.35				
Mostly Comprehensive	465	21.53	25.88				
Somewhat Comprehensive	506	23.43	49.31				
Limited	734	33.98	83.29				
Not at all	361	16.71	100				
Total	2160	100					

Source: Author's computation using Stata

The results for the developing countries presented in Table 4.2 above, are interpreted as follows:

Government cyber security capacity (v2smgovcapsec)

In developing countries, 5.14% of governments lack the resources to counter even basic cyber threats, while 33.56% can only address unsophisticated attacks. Approximately 33.33% can combat moderately sophisticated attacks, and 23.61% can combat the majority of sophisticated attacks. Only a small proportion (4.35%) have the resources to combat even the most sophisticated cyberattacks.

These findings indicate that the majority of developing countries are ill-equipped to handle sophisticated cyber-attacks, with only a small proportion possessing the resources to counter the most advanced cyber threats.

Government Internet filtering capacity (v2smgovfilcap)

The majority of developing countries' governments possess some capacity to filter internet content. While 8.24% lack any filtering capacity, over a third (34.95%) have limited capacity to block a few sites. A significant proportion (22.04%) can block most sites, and the largest proportion (34.77%) has complete filtering capacity.

These findings indicate that the majority of developing countries' governments have the capacity to filter internet content, with a significant proportion having complete control over what websites their citizens can access.

Government Internet filtering in practice (v2smgovfilprc)

Although many developing countries have the capacity to censor the Internet, the largest proportion (34.21%) never or rarely actually censor the Internet. However, 8.61% engage in extreme censorship, regularly removing online political content except for pro-government sites. An additional 13.70% censor online political content frequently, and 17.27% censor critical political content occasionally.

These findings suggest that Internet freedom in developing countries varies, with the majority rarely engaging in censorship and a significant minority actively censoring online political content.

Government Internet shut down capacity (v2smgovshutcap)

The majority of developing countries' governments have some capacity to shut down domestic Internet access. While 10.69% lack this capacity, a substantial proportion can shut down varying amounts of domestic Internet access: 23.10% can shut down a quarter, 15% can shut down half, and 12.41% can shut down three-quarters. Notably, 38.80% have the capacity for a near-total shutdown.

These findings suggest that the majority of developing countries' governments have the capacity to shut down domestic internet access, with a significant proportion capable of a near-total shutdown of the domestic Internet.

Government social media monitoring (v2smgovsmmon)

A small proportion (4.35%) of developing countries' governments surveil virtually all content on social media, while 21.53% surveil most content and key political issues. Nearly a quarter (23.43%) monitor key issues about half the time, and a third (33.98%) have limited social media monitoring. A sizable minority (16.71%) do not surveil political content at all.

These findings indicate that developing countries conduct government social media monitoring to varying degrees.

Government capacity to regulate online content (v2smregcap)

A small proportion of developing countries' governments (4.91%) lack any capacity to regulate online content, and over a third (35.42%) have extremely limited resources to do so. About 28.84% can regulate some online content, while almost a quarter (24.21%) have robust but incomplete capacity to regulate all content. Only 6.62% of developing countries have sufficient resources to regulate all online content.

These findings suggest that the capacity for online content regulation varies considerably in developing countries, with a majority facing limitations in their ability to regulate online content effectively.

Government online content regulation approach (v2smregapp)

While 21.06% of developing countries' governments rely entirely on state regulation, a similar proportion (21.02%) involves private actors in a limited way. A significant

proportion (43.29%) share responsibility with private actors, and 13.52% delegate the majority of regulation to private actors. Only 1.11% completely delegate regulation to private actors.

These findings indicate the majority of developing countries' governments involve private actors in online content regulation to some degree.

Internet legal regulation content (v2smregcon)

In 12.41% of developing countries, the state can remove any content at will, and in another 12.31%, it can remove most content with limited speech protections. The laws of a significant proportion of developing countries (23.33%) are ambiguous, allowing the state to remove politically sensitive content while protecting other content. Meanwhile, 15.79% of developing countries safeguard most speech, with exceptions for controversial content. The largest proportion of developing countries (36.16%) provide robust legal protections for political speech.

These findings suggest that frameworks for Internet regulation vary considerably in developing countries, with a significant proportion offering strong protections for political speech.

Privacy protection by law content (v2smprivcon)

A very small minority of developing countries (0.29%) have no legal restrictions on their governments accessing online personal data. A further 17.62% of these countries allow their governments to access most types of online personal data, while 19.95% of developing countries allow their governments to access many types of personal data online. 26.94% of them allow their governments to access a few types of online personal data. The largest proportion of developing countries (35.19%) allow the government to access online personal data only in extraordinary circumstances.

These findings suggest that while a considerable proportion of developing countries have laws to protect online privacy, a majority still permit varying degrees of government access to personal data, raising concerns about data privacy rights and surveillance.

4.2 Ordinal logistic regression results

4.2.1 African countries

Table 4.3: Ordinal regression results for Model 1 (African Countries)

(v2smgovcapsec)	Coef.	Std. Err.	t-value	p-value	Sig
v2smgovfilcap					
Limited Capacity	-9.5966891	2.391945	-4.01	.0000602	***
Adequate Capacity	-8.2937993	3.3738977	-2.46	.0139626	**
Complete Capacity	-3.938893	2.8841979	-1.37	.1720392	
v2smgovfilprc					
Often	-15.870675	4.1892732	-3.79	.0001516	***
Sometimes	-17.372486	4.1875691	-4.15	.0000335	***
Rarely	-12.465814	4.3783668	-2.85	.0044114	***
Never	-12.587	4.4634525	-2.82	.0048021	***
Number of observations	1200				

*** $p<.01$, ** $p<.05$, * $p<.1$

Source: Author's computation using Stata

The results of Table 4.3 above are interpreted as follows:

Government Internet filtering capacity (v2smgovfilcap)

For African governments with limited capacity to block websites (v2smgovfilcap= "Limited Capacity"), the study rejects the null hypothesis at a 1% significance level. This suggests that there is a statistically significant negative relationship between limited internet filtering capacity and government cybersecurity capacity.

For African governments with sufficient capacity to block websites (v2smgovfilcap= "Adequate Capacity"), the study rejects the null hypothesis at a 5% significance level. This suggests that there is a statistically significant negative relationship between adequate internet filtering capacity and government cybersecurity capacity.

For African governments that can block any websites (v2smgovfilcap="Complete Capacity"), the study fails to reject the null hypothesis at a 10% significance level. This suggests that there is no statistically significant relationship between complete filtering

capacity and government cybersecurity capacity. This indicates that having the capacity to block any websites might not influence government cybersecurity capacity in African countries.

In African countries, the study found a complex relationship between a government's capacity to filter internet content and its cybersecurity capacity. While having some filtering capability (either limited or adequate) has a significant negative relationship with government cybersecurity capacity, having complete filtering capacity did not demonstrate a significant effect on government cybersecurity capacity. This suggests that a moderate approach to internet filtering, rather than full control, may be more conducive to improving government cybersecurity capacity in African countries.

Government Internet filtering in practice (v2smgovfilprc)

For African governments that commonly remove online political content (v2smgovfilprc="Often"), the study rejects the null hypothesis at a 1% significance level. This suggests that there is a statistically significant negative relationship between commonly removing online political content and government cybersecurity capacity.

For African governments that successfully remove about half of the critical online political content (v2smgovfilprc="Sometimes"), the study also rejects the null hypothesis at a 1% significance level. This suggests that there is a statistically significant negative relationship between sometimes removing online political content and government cybersecurity capacity.

For African governments that rarely remove online political content (v2smgovfilprc= "Rarely"), the study also rejects the null hypothesis at a 1% significance level. This suggests that there is a statistically significant negative relationship between rarely removing online political content and government cybersecurity capacity.

For African governments that never or almost never remove online political content (v2smgovfilprc= "Never"), the study also rejects the null hypothesis at a 1% significance level. This suggests that there is a statistically significant negative relationship between never, or almost never, removing online political content and government cybersecurity capacity.

In African countries, both overly restrictive and unregulated approaches seem to have a significant negative relationship with government cybersecurity capacity.

Table 4.4: Ordinal regression results for Model 2 (African Countries)

(v2smgovcapsec)	Coef.	Std. Err.	t-value	p-value	Sig
v2smgovshutcap					
Quarter	35.728542	3.3105119	10.79	0	***
Half	51.526935	2.2162687	23.25	0	***
Three Quarter	53.19134	3.8107486	13.96	0	***
Complete	53.834309	3.0862761	17.44	0	***
Number of observations	1200				

*** $p<.01$, ** $p<.05$, * $p<.1$

Source: Author's computation using Stata

The results of Table 4.4 above are interpreted as follows:

Government Internet shut down capacity (v2smgovshutcap)

For African governments with the capacity to shut down a quarter of domestic internet access (v2smgovshutcap="Quarter"), the study rejects the null hypothesis at a 1% significance level. This suggests that there is a statistically significant positive relationship between the capacity to shut down a quarter of domestic internet access and government cybersecurity capacity.

For African governments with the capacity to shut down half of domestic internet access (v2smgovshutcap="Half"), the study also rejects the null hypothesis at a 1% significance level. This suggests that there is a statistically significant positive relationship between the capacity to shut down half of domestic internet access and government cybersecurity capacity.

For African governments with the capacity to shut down three-quarters of domestic internet access (v2smgovshutcap="Three Quarter"), the study also rejects the null hypothesis at a 1% significance level. This suggests that there is a statistically significant positive relationship between the capacity to shut down three-quarters of domestic internet access and government cybersecurity capacity.

For African governments with the capacity to shut down all or almost all domestic internet access (v2smgovshutcap="Complete"), the study also rejects the null hypothesis at a 1% significance level. This suggests that there is a statistically significant positive relationship between the capacity to shut down all or almost all of domestic internet access and government cybersecurity capacity.

In African countries, the government's capacity to shut down domestic internet access, regardless of its extent, appears to have a significantly positive relationship with government cybersecurity capacity. This suggests that the capacity to control internet access, even partially, could be a statistically significant factor.

Table 4.5: Ordinal regression results for Model 3 (African Countries)

(v2smgovcapsec)	Coef.	Std. Err.	t-value	p-value	Sig
v2smgovsmmon					
Mostly Comprehensive	1.679	3.046	0.55	.582	
Somewhat Comprehensive	-3.538	3.102	-1.14	.254	
Limited	-2.256	4.433	-0.51	.611	
Not at all	-.841	6.217	-0.14	.892	
v2smregcon					
Remove Most Content	-6.474	3.049	-2.12	.034	**
Ambiguous Framework	-2.347	3.255	-0.72	.471	
Remove Controversial Content	-3.403	2.89	-1.18	.239	
Remove if violate legal criteria	-.114	3.112	-0.04	.971	
Number of observations	1200				

*** p<.01, ** p<.05, * p<.1

Source: Author's computation using Stata

The results of Table 4.5 above are interpreted as follows:

Government social media monitoring (v2smgovsmmon)

For all the levels of government social media monitoring in African countries, the study fails to reject the null hypothesis at a 10% significance level. This suggests that government social media monitoring does not have a significant relationship with government cybersecurity capacity in African countries.

Internet legal regulation content (v2smregcon)

For African governments that can remove most online content, with legal protections for speech limited to uncontroversial contexts (v2smregcon= "Remove Most Content"), the study rejects the null hypothesis at a 5% significance level. This suggests that there is a statistically significant negative relationship between removing most online content (with limited legal protections for political speech) and government cybersecurity capacity.

For all the other levels of Internet legal regulation content in African countries, the study fails to reject the null hypothesis at a 10% significance level. This suggests that there is no statistically significant relationship between the other levels of internet legal regulation regarding content removal, ranging from removing some politically sensitive content to removing only content that violates established legal criteria, and government cybersecurity capacity. These varying levels of internet legal regulation content do not seem to have a statistically significant effect on government cybersecurity capacity in African countries.

In African countries, a restrictive legal framework for internet content regulation seems to be negatively related with government cybersecurity capacity. Other levels of internet legal regulation, ranging from allowing the removal of some politically sensitive content to only removing content that violates established legal criteria, do not seem to have a statistically significant effect on cybersecurity capacity.

Table 4.6: Ordinal regression results for Model 4 (African Countries)					
(v2smgovcapsec)	Coef.	Std. Err.	t-value	p-value	Sig
v2smprivcon					
Most types	-67.9	15.154	-4.48	0	***
Many Types	-5.902	3.795	-1.56	.12	
Few Types	-3.523	8.691	-0.41	.685	
Only Extraordinary circumstances	-6.174	8.956	-0.69	.491	
v2smregcap					
Not Really	.274	2.112	0.13	.897	
Somewhat	-1	2.628	-0.38	.704	
Mostly	.447	4.781	0.09	.925	
v2smregapp					
Most Content	-1.15	1.271	-0.90	.366	
Some Content	13.678	5.273	2.59	.009	***
Little Content	15.902	4.945	3.22	.001	***
Number of observations	1161				

*** $p<.01$, ** $p<.05$, * $p<.1$

Source: Author's computation using Stata

The results of Table 4.6 above are interpreted as follows:

Privacy protection by law content (v2smprivcon)

For African governments, where the legal framework allows access to most types of online personal data (v2smprivcon="Most Types"), the study rejects the null hypothesis at a 1% significance level. This suggests that there is a statistically significant negative relationship between privacy protection by law content and government cybersecurity capacity.

For African governments where the legal framework allows access to online personal data in varying degrees (many, few, or only in extraordinary circumstances), the study fails to reject the null hypothesis at a 10% significance level. This suggests that there is no statistically significant relationship between these levels of privacy protection by law content and government cybersecurity capacity.

In African countries, a legal framework allowing the government access to most types of personal data has a statistically significant negative relationship with government

cybersecurity capacity. However, where the legal framework allows access to personal data on the Internet in varying degrees (many, few, or only in extraordinary circumstances), it does not seem to have a statistically significant relationship with government cybersecurity capacity in African countries.

Government capacity to regulate online content (v2smregcap)

For all the levels of government capacity to regulate online content in African countries, the study fails to reject the null hypothesis at a 10% significance level. This suggests that in African countries, government capacity to regulate online content does not seem to have a statistically significant relationship with government cybersecurity capacity.

Government online content regulation approach (v2smregapp)

For African countries where the state shares responsibility for monitoring and regulation with private actors, either doing some content regulation (v2smregapp="Some Content") or little content regulation (v2smregapp="Little Content"), the study rejects the null hypothesis at a 1% significance level. This suggests that there is a statistically significant positive relationship between sharing responsibility for online content regulation with private actors and government cybersecurity capacity.

For African countries where the state does most online content monitoring and regulation but involves private actors in a limited capacity, the study fails to reject the null hypothesis at a 10% significance level. This suggests that there is no statistically significant relationship between African governments that do most of their own online content monitoring and cybersecurity capacity.

Overall, these results suggest that involving private actors in online content regulation, particularly when the state takes a less active role, has a statistically significant positive relationship with government cybersecurity capacity in African countries. Other approaches to content regulation, including the limited involvement of private actors, do not seem to have a statistically significant relationship with government cybersecurity capacity.

4.2.2 Developing Countries

Table 4.7: Ordinal regression results for Model 1 (Developing Countries)

(v2smgovcapsec)	Coef.	Std. Err.	t-value	p-value	Sig
v2smgovfilcap					
Limited Capacity	1.2079645	1.9702677	0.61	.5398125	
Adequate Capacity	2.6989233	1.8554673	1.45	.1457859	
Complete Capacity	4.2344587	2.277394	1.86	.0629784	*
v2smgovfilprc					
Often	.4269883	.9506315	0.45	.6533142	
Sometimes	.9614785	1.3755645	0.70	.4845707	
Rare	1.1884222	2.1939119	0.54	.5880314	
Never	.305724	2.2321415	0.14	.8910589	
Number of observations	2160				

**** p<.01, ** p<.05, * p<.1*

Source: Author's computation using Stata

The results of Table 4.7 above are interpreted as follows:

Government Internet filtering capacity (v2smgovfilcap)

The study rejects the null hypothesis at the 10% significance level for governments in developing countries that have the capacity to block any website (v2smgovilcap="Complete Capacity"). This suggests that there is a statistically significant positive relationship between complete Internet filtering capacity and government cybersecurity capacity.

The study fails to reject the null hypothesis at a 10% significance level for governments in developing countries that have limited or adequate internet filtering capacity. This suggests that there is no statistically significant relationship between these levels of government Internet filtering capacity and cybersecurity capacity.

These findings suggest that only complete government Internet filtering capacity is positively correlated with government cybersecurity capacity.

Government Internet filtering in practice (v2smgovfilprc)

For all levels of government internet filtering in practice in developing countries, the study fails to reject the null hypothesis a 10% significance level. This suggests that there is no statistically significant relationship between government internet filtering in practice and government cybersecurity capacity in developing countries.

Table 4.8: Ordinal regression results for Model 2 (Developing Countries)

(v2smgovcapsec)	Coef.	Std. Err.	t-value	p-value	Sig
v2smgovshutcap					
Quarter	-.701	1.216	-0.58	.565	
Half	.175	1.319	0.13	.894	
Three Quarter	2.781	1.61	1.73	.084	*
Complete	2.202	1.922	1.15	.252	
Number of observations	2160				

**** p<.01, ** p<.05, * p<.1*

Source: Author's computation using Stata

The results of Table 4.8 above are interpreted as follows:

Government Internet shut down capacity (v2smgovshutcap)

For developing countries with the capacity to shut down roughly three-quarters of domestic internet access (v2smgovshutcap="Three Quarter"), the study rejects the null hypothesis at a 10% significance level. This suggests that there is a statistically significant positive relationship between having the ability to shut down roughly three-quarters of the internet and government cybersecurity capacity.

For all the other levels of government internet shut down capacity in developing countries, the study fails to reject the null hypothesis at a 10% significance level. This suggests that for all other levels of internet shutdown capacity (one-quarter, half, and almost all/all), there is no statistically significant relationship with government cybersecurity capacity.

In developing countries, only the capacity to shut down a significant proportion (three-quarters) of domestic internet access seems to be correlated with government cybersecurity capacity. The capacity to shut down smaller portions of the Internet does not seem to be correlated with government cybersecurity capacity.

Table 4.9: Ordinal regression results for Model 3 (Developing Countries)					
(v2smgovcapsec)	Coef.	Std. Err.	t-value	p-value	Sig
v2smgovsmmon					
Mostly Comprehensive	-3.188	1.417	-2.25	.024	**
Somewhat Comprehensive	-3.424	1.487	-2.30	.021	**
Limited	-5.383	1.931	-2.79	.005	***
Not at all	-4.507	2.01	-2.24	.025	**
v2smregcon					
Remove Most Content	1.023	1.377	0.74	.457	
Ambiguous Framework	1.466	2.14	0.69	.493	
Remove Controversial Content	.702	2.885	0.24	.808	
Remove if violate legal criteria	.592	3.009	0.20	.844	
Number of observations	2160				

*** $p<.01$, ** $p<.05$, * $p<.1$

Source: Author's computation using Stata

The results of Table 4.9 above are interpreted as follows:

Government social media monitoring (v2smgovsmmon)

For developing countries where the government engages in comprehensive social media surveillance, either by monitoring most key political issues (v2smgovsmmon= "Mostly Comprehensive") or selectively targeting key political issues (v2smgovsmmon= "Somewhat Comprehensive"), the study rejects the null hypothesis at a 5% significance level. This suggests that there is a statistically significant negative relationship between mostly comprehensive or somewhat comprehensive social media surveillance and government cybersecurity capacity.

Similarly, for developing countries where the government limits its surveillance to political content (v2smgovsmmon="Limited") or does not surveil political content at all (v2smgovsmmon="Not at all"), the study rejects the null hypothesis at a 1% significance level. This suggests that there is a statistically significant negative relationship between limited or no social media surveillance and government cybersecurity capacity.

Overall, the results suggest that in developing countries, government surveillance of social media, whether comprehensive or limited, is negatively correlated with government cybersecurity capacity.

Internet legal regulation content (v2smregcon)

For all levels of Internet legal regulation content in developing countries, the study fails to reject the null hypothesis at a 10% significance level. This suggests that in developing countries, Internet legal regulation content is not correlated with government cybersecurity capacity.

Table 4.10: Ordinal regression results for Model 4 (Developing Countries)

(v2smgovcapsec)	Coef.	Std. Err.	t-value	p-value	Sig
v2smprivcon					
Most types	.572	3.623	0.16	.875	
Many Types	3.558	3.214	1.11	.268	
Few Types	2.869	3.263	0.88	.379	
Only Extraordinary circumstances	4.476	3.521	1.27	.204	
v2smregcap					
Not Really	2.536	.992	2.56	.011	**
Somewhat	5.474	1.508	3.63	0	***
Mostly	9.279	1.902	4.88	0	***
All	13.543	2.3	5.89	0	***
v2smregapp					
Most Content	.437	.812	0.54	.59	
Some Content	-.582	1.236	-0.47	.638	
Little Content	-2.503	1.568	-1.60	.11	
All Content	-6.79	1.682	-4.04	0	***
Number of observations	2060				

**** p<.01, ** p<.05, * p<.1*

Source: Author's computation using Stata

The results of Table 4.10 above are interpreted as follows:

Privacy protection by law (v2smprivcon)

For all levels of privacy protection by law in developing countries, the study fails to reject the null hypothesis at a 10% significance level. This suggests that in developing countries, privacy protection by law is not correlated with government cybersecurity capacity.

Government capacity to regulate online content (v2smregcap)

For developing countries that have extremely limited resources to regulate online content (v2smregcap="Not Really"), the study rejects the null hypothesis at a 5% significance level. This suggests that there is a statistically significant positive relationship between limited online content regulation capacity and government cybersecurity capacity

For developing countries with the capacity to regulate only some online content or portions of the law (v2smregcap="Somewhat"), the study rejects the null hypothesis at a 1% significance level. This suggests that there is a statistically significant positive relationship between partial online content regulation capacity and government cybersecurity capacity.

For developing countries with robust capacity to regulate online content but not enough to regulate all content and all portions of the law (v2smregcap = "Mostly"), the study rejects the null hypothesis at a 1% significance level. This suggests that there is a statistically significant positive relationship between mostly robust online content regulation capacity and government cybersecurity capacity.

For developing countries with sufficient capacity to regulate all online content (v2smregcap="All"), the study rejects the null hypothesis at a 1% significance level. This suggests that there is a statistically significant positive relationship between full online content regulation capacity and government cybersecurity capacity.

These findings suggest that in developing countries, government capacity to regulate online content, even if limited, is positively correlated with government cybersecurity capacity.

Government online content regulation approach (v2smregapp)

For developing countries that rely entirely on private actors to monitor and regulate online content (v2smregapp = "All Content"), the study rejects the null hypothesis at a 1% significance level. This suggests that there is a statistically significant negative relationship between this approach and government cybersecurity capacity.

However, for all other levels of online content regulation and monitoring, the study fails to reject the null hypothesis at the 10% significance level. This suggests that there is

no statistically significant relationship between government cybersecurity capacity and these online regulation and monitoring approaches (where the government either handles all regulation, shares some responsibility with private actors, or does little regulation).

These findings suggest that in developing countries, relying entirely on private actors to regulate online content is negatively correlated with government cybersecurity capacity, while other approaches to online content regulation do not show a statistically significant relationship with government cybersecurity capacity.

This chapter's Results section presented the detailed statistical findings of the study. The following section will synthesise these results, offering a concise overview of the factors that influence government cybersecurity capacity in African and developing countries.

4.3 Summary of Key Statistical Results

This study sought to determine the factors that influence government cybersecurity capacity in African and developing countries. The quantitative analysis revealed contrasting findings between African and developing countries regarding the relationship between digital media freedom and state Internet control measures with government cybersecurity capacity. Table 4.11 below summarises the key statistical results of the study.

Table 4.11: Summary of Key Statistical Results

Independent Variable	African Countries	Developing Countries
Government Internet filtering capacity	Significant negative relationship at moderate levels (i.e., limited and adequate) with government cybersecurity capacity.	Significant positive relationship (i.e., only at complete level) with government cybersecurity capacity.
Government Internet shut down capacity	Significant positive relationship (i.e., at all levels) with government cybersecurity capacity.	Significant positive relationship (i.e., only for near-total shutdowns) with government cybersecurity capacity.
Government Internet filtering in practice	Significant negative relationship (i.e., at all levels) with government cybersecurity capacity.	No significant relationship with government cybersecurity capacity.
Government social media monitoring	No significant relationship with government cybersecurity capacity.	Significant negative relationship (i.e., at all levels) with government cybersecurity capacity.

Internet legal regulation content	Significant negative relationship when state can remove most content (i.e., with law protecting speech only in specific and politically uncontroversial contexts) with government cybersecurity capacity.	No significant relationship with government cybersecurity capacity.
Privacy protection by law content	Significant negative relationship (i.e., when government has access to most types of online personal data) with government cybersecurity capacity.	No significant relationship with government cybersecurity capacity.
Government capacity to regulate online content	No significant relationship with government cybersecurity capacity.	Significant positive relationship (i.e., at all levels) with government cybersecurity capacity.
Government online content regulation approach	Significant positive relationship (i.e., when the state takes a less active role in online content regulation) with government cybersecurity capacity.	Significant negative relationship (i.e., when the state completely relies on private actors for online content regulation) with government cybersecurity capacity.

The above summary of the key statistical results highlight the relationships between digital media freedom, state Internet regulation, and government cybersecurity capacity. While some state Internet control measures improve government cybersecurity capacity, their effectiveness and broader implications vary across African and developing countries. The following discussion will explore these findings in more detail.

4.4 Discussion of Findings

This study sought to identify the determinants of government cybersecurity capacity in African and developing countries by the integrating perspectives from CSS and Oxford's GCSCC CMM. The findings reveals that the influence of digital control mechanisms is neither uniform nor straightforward, being fundamentally influenced by regional contexts and the specific characteristics of the control measures. CSS provides a theoretical framework to understand these varied outcomes as results of distinct securitisation processes and power dynamics (Ramich & Piskunov, 2022), while the CMM provides a conceptual framework to assess how these processes impact measurable capacity across various cyber dimensions (Global Cyber Security Capacity Centre, 2021).

Contrary to the study's first hypothesis, which predicted a positive correlation between more stringent Internet control measures (such as Internet filtering and shutdown

capacities and practices) and government cybersecurity capacity in African and developing nations, the results reveal that state Internet control measures have a complex and often contradictory relationship with government cybersecurity capacity. Partially supporting the study's second hypothesis, which predicted that active government monitoring of social media would positively correlate with government cybersecurity capacity in African and developing countries, social media monitoring presents a distinct trade-off, negatively affecting government cybersecurity capacity in developing nations. The study's third hypothesis, which predicted that a robust legal and regulatory framework (including data privacy protection and laws safeguarding online political speech) would positively correlate with government cybersecurity capacity in African and developing countries, found limited support, underscoring the gap between formal legislation and effective implementation.

4.4.1 Internet Control Mechanisms and Cybersecurity Capacity: Divergent Pathways

The relationship between state internet control and cybersecurity capacity is contextual, reflecting what CSS scholars describe as diverse securitisation patterns across different political and developmental landscapes (Cavelty, 2024).

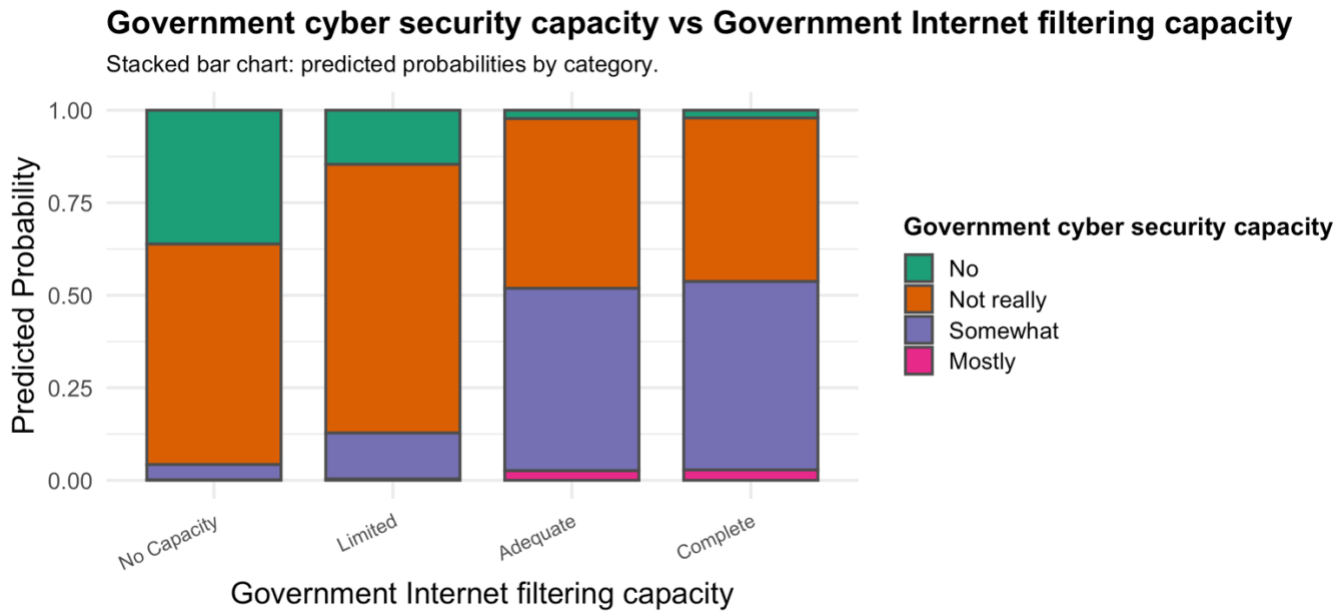
Internet Filtering and Shutdown Capacity: A Question of Degree and Context

The study highlights a crucial difference in how Internet filtering capacity impacts cybersecurity outcomes. In African countries, a moderate level of Internet filtering capacity, characterised by limited and adequate levels, demonstrates a statistically significant negative correlation with governmental cybersecurity capacity. From a CSS viewpoint, this implies that efforts to enhance security through Internet filtering, without the institutional capability for full control, might be counterproductive, potentially hindering innovation and misallocating resources without improving cybersecurity (Turianskyi & Wekesa, 2021; Ifeanyi-Ajufo, 2023).

Figure 4.1 below, a stacked bar chart depicting the predicted probabilities of government cybersecurity capacity in relation to government Internet filtering capacity across 50 African countries, indicates that African governments with limited Internet filtering capacity are most likely equipped to combat only unsophisticated cyber-attacks. Conversely, African governments with adequate Internet filtering capacity are

nearly evenly divided between being most likely equipped to combat only unsophisticated cyber-attacks and moderately sophisticated cyber-attacks.

Figure 4.1: Government cyber security capacity vs Government Internet filtering capacity in 50 African countries

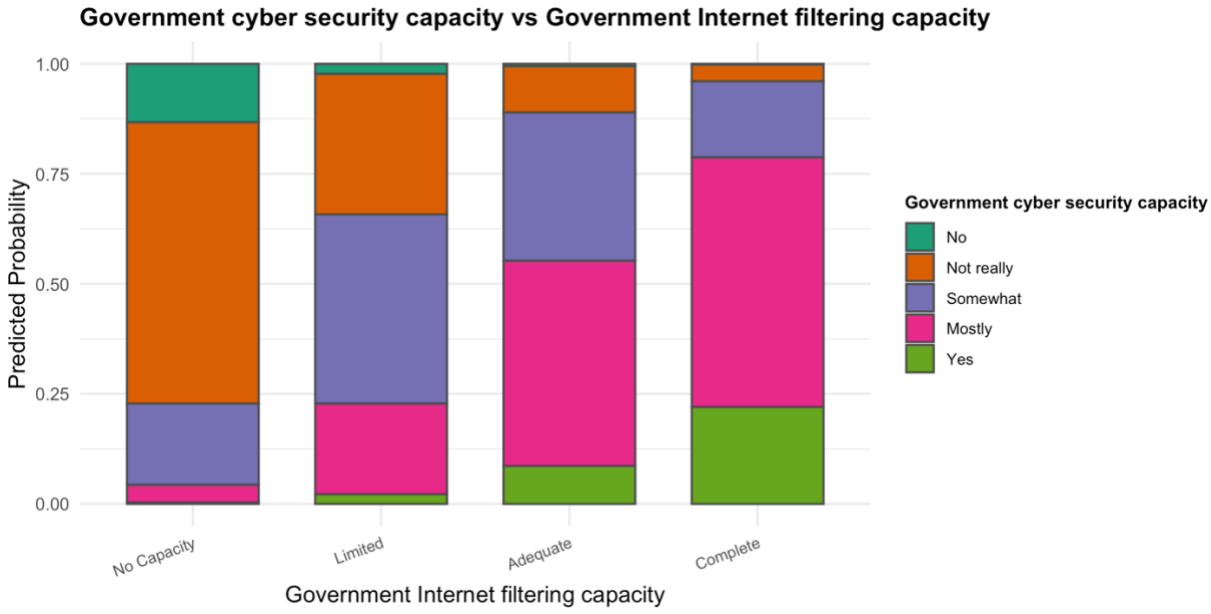


Source: Author's computation using R

In developing countries, a statistically significant positive correlation with government cybersecurity capacity is observed only when there is complete Internet filtering capacity. This finding corresponds with a more authoritarian control model, which, as cautioned by the CDI report, can stifle innovation and possibly weaken long-term cybersecurity readiness (O'Brien, 2022).

Figure 4.2 below, a stacked bar chart depicting the predicted probabilities of government cybersecurity capacity in relation to government Internet filtering capacity across 90 developing countries, indicates that governments of developing countries with complete Internet filtering capacity are most likely equipped to combat most sophisticated cyber-attacks.

Figure 4.2: Government cyber security capacity vs Government Internet filtering capacity in 90 developing countries

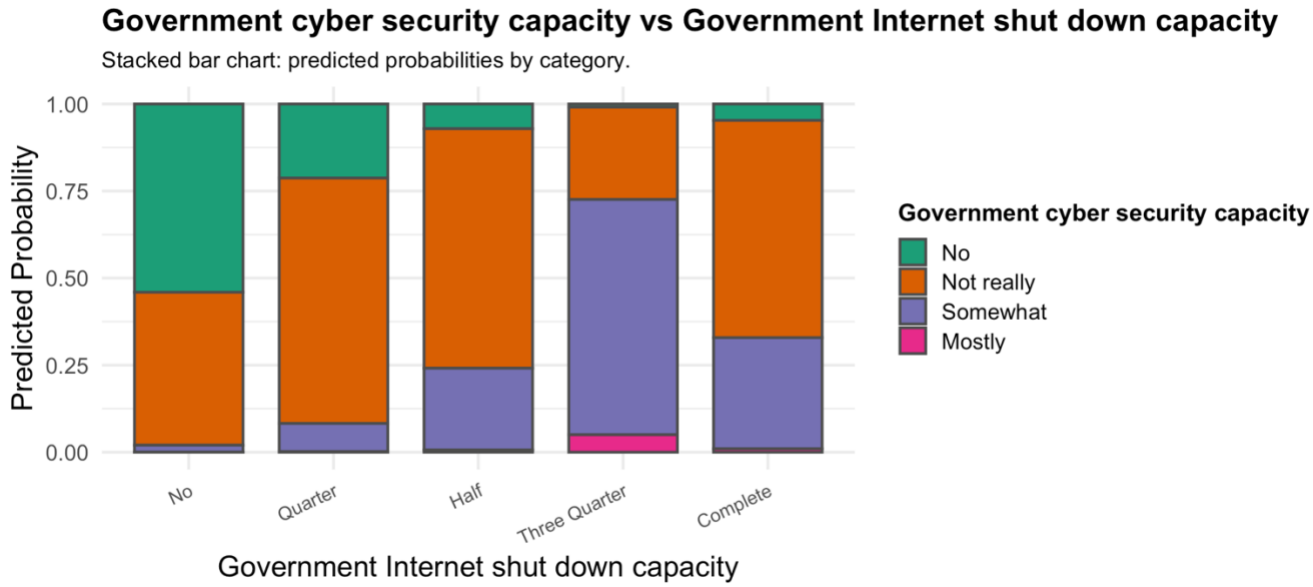


Source: Author's computation using R

Similarly, the capacity to shut down the Internet reveals varying thresholds. In African countries, even partial government Internet shutdown capacity is positively correlated with government cybersecurity capacity, indicating that the mere technical ability for digital control is integrated into the state's security framework. However, in developing countries, this relationship is evident only with near-total Internet shut down capacity, suggesting a higher threshold for this measure to be related with broader cybersecurity capacity, possibly reflecting more advanced digital infrastructure (Portulans Institute, 2023b).

Figure 4.3 below presents a stacked bar chart depicting the predicted probabilities of government cybersecurity capacity in relation to government Internet shutdown capacity across 50 African countries. The analysis shows that African countries that lack any shutdown capacity are most likely to also lack capacity to combat even unsophisticated cyber-attacks, those with partial shutdown capacities (one quarter or half) are most likely able to combat only unsophisticated cyber-attacks, those with three-quarters shutdown capacity are more likely equipped for moderately sophisticated cyber-attacks, and African countries with full shutdown capacity generally still face limitations in tackling more advanced cyber-attacks.

Figure 4.3: Government cyber security capacity vs Government Internet shut down capacity in 50 African countries



Source: Author's computation using R

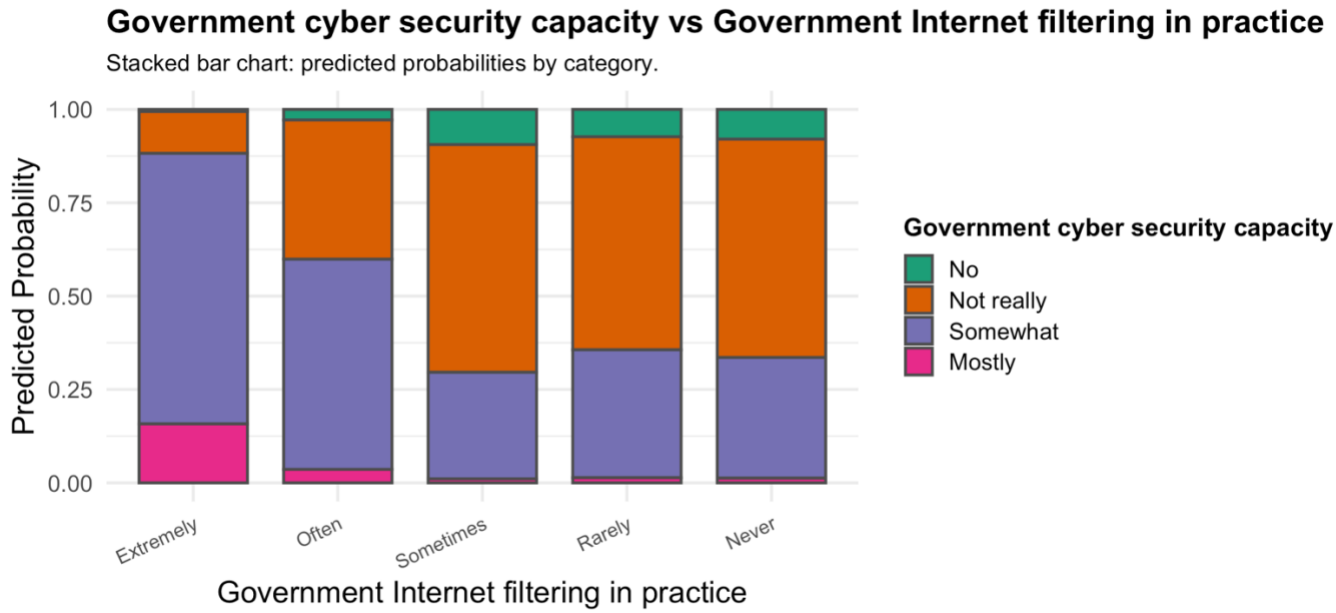
Internet Filtering in Practice: The Implementation Gap in African Countries

The analysis reveals a significant negative relationship between active Internet filtering practices and government cybersecurity capacity in African countries. This underscores a critical gap between securitisation rhetoric—the speech acts that declare certain online content a threat (Buzan et al., 1998)—and institutional capacity. Several mechanisms, informed by the Oxford GCSCC CMM framework, can explain this negative relationship. Firstly, active filtering requires scarce technical and financial resources that could otherwise be allocated to proactive measures within the Policy and Strategy dimension, such as vulnerability management (Kayode-Ajala, 2023). Secondly, it erodes public trust, a foundation of the Cybersecurity Culture and Society dimension, thereby hindering collaborative cyber threat reporting (Onumo et al., 2017; Turianskyi & Wekesa, 2021). In developing countries, the absence of a statistically significant relationship suggests greater diversity in Internet filtering implementation, ranging from targeted technical measures to indiscriminate political control (Karlekar & Dunham, 2014).

Figure 4.4 below presents a stacked bar chart depicting predicted probabilities of government cybersecurity capacity in relation to government Internet filtering practices across 50 African countries. The analysis shows that African countries that often or

extremely often remove critical online political content (primarily allowing online content supportive of the government) are most likely equipped to counter moderately sophisticated cyber-attacks, while those that sometimes, rarely, or never remove such online content are predominantly equipped only to address unsophisticated cyber-attacks.

Figure 4.4: Government cyber security capacity vs Government Internet filtering in practice in 50 African countries



Source: Author's computation using R

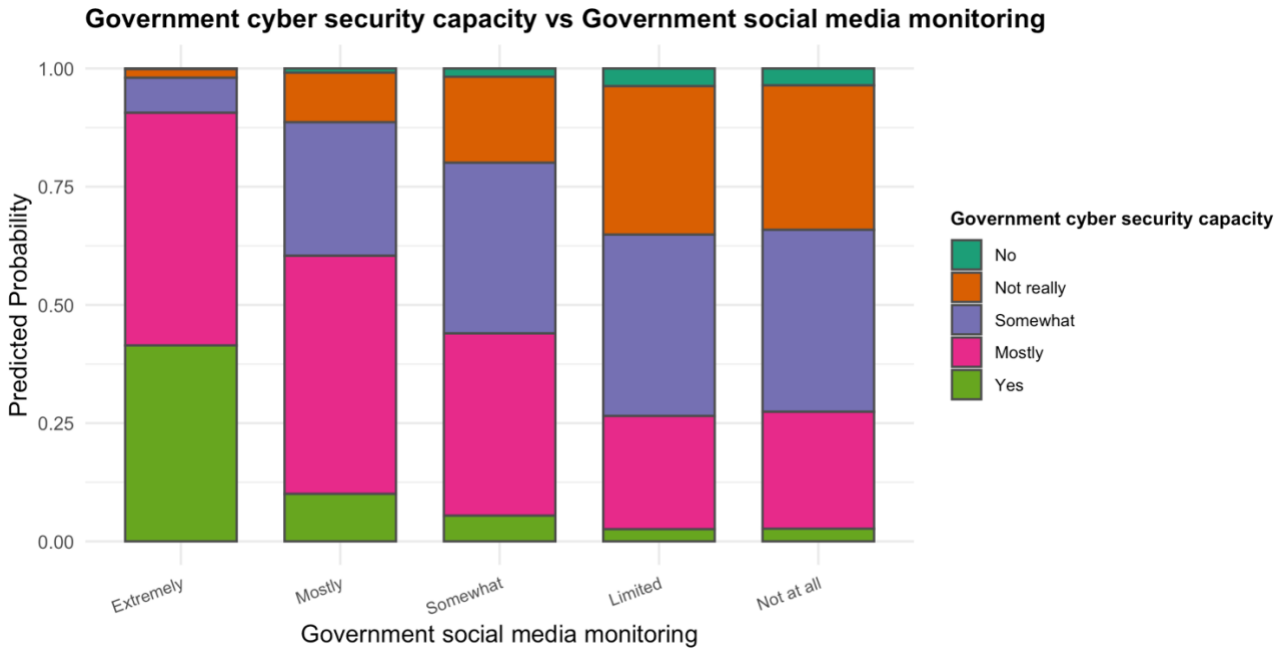
4.4.2 Social Media Surveillance: The Erosion of Trust and Capacity

The findings partially support the second hypothesis, revealing a clear trade-off in developing countries, where all levels of social media monitoring (i.e., not at all to extremely comprehensive social media monitoring) demonstrate a significant negative relationship with government cybersecurity capacity. From a CSS perspective, this represents a counterproductive securitisation of the digital public sphere, which undermines the trust and collaboration that are essential for effective cybersecurity (Ramich & Piskunov, 2022). This observation aligns with the Oxford GCSCC CMM's Culture and Society dimension, which identifies trust as a critical factor in building cybersecurity capacity (Global Cyber Security Capacity Centre, 2021). The negative relationship likely arises from the misallocation of limited resources away from technical cybersecurity infrastructure and towards surveillance apparatuses

(Calderaro & Craig, 2020), and the creation of a climate of fear that discourages public cooperation in reporting cyber threats. In African countries, the absence of a significant relationship suggests that social media monitoring may be less systematic or resourced, thus not yet showing a measurable impact on cybersecurity capacity.

Figure 4.5 below presents a stacked bar chart depicting the predicted probabilities of government cybersecurity capacity in relation to government social media monitoring in 90 developing countries. The analysis indicates that developing countries engaging in comprehensive or near-comprehensive surveillance of social media content are most likely to possess the capacity to combat most sophisticated cyber-attacks. Developing countries that intermittently monitor key political issues on social media tend to be equipped for both moderately sophisticated and sophisticated cyber-attacks. Additionally, developing countries that conduct only limited surveillance of political content, or do not engage in political surveillance at all, are generally also most likely to possess capacity for combatting most sophisticated cyber-attacks.

Figure 4.5: Government cyber security capacity vs Government social media in 90 developing countries



Source: Author's computation using R

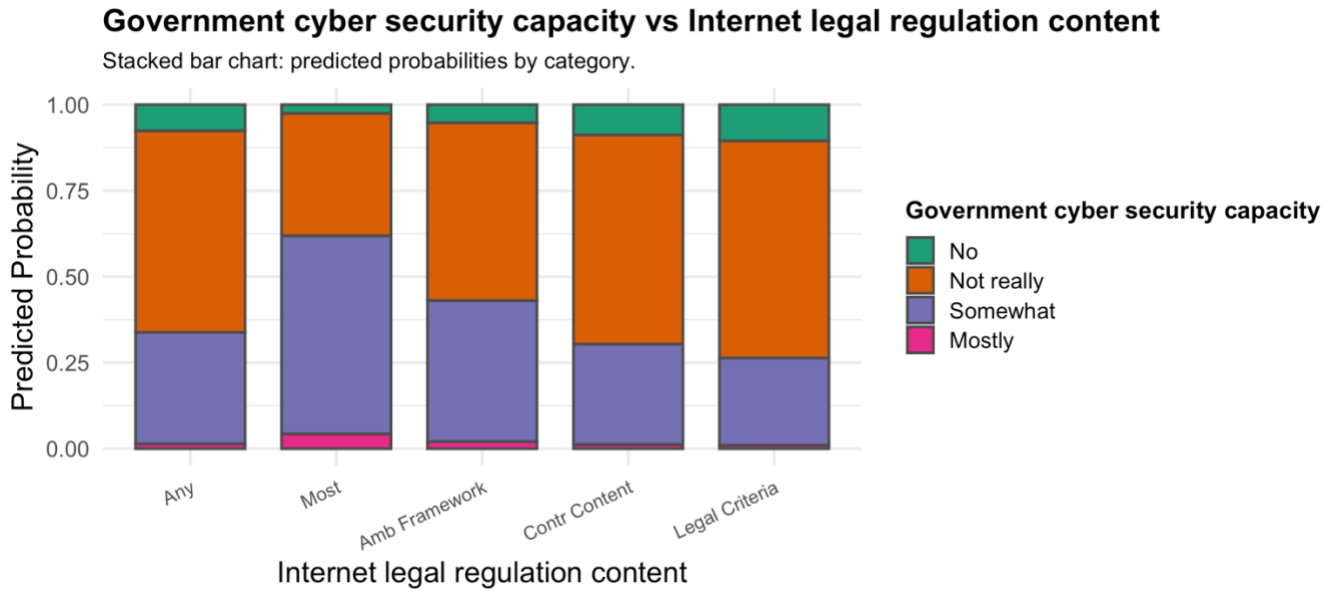
4.4.3 Legal and Regulatory Frameworks: The Form versus Function Dilemma

The study's third hypothesis, which predicted a positive relationship between legal and regulatory frameworks and government cybersecurity capacity, was not supported, revealing a widespread implementation gap. In developing countries, no statistically significant relationships were found between the measured legal variables and government cybersecurity capacity. This finding underscores that merely having laws, without effective enforcement and alignment with technical needs, is inadequate (Creese et al., 2021).

In African countries, the findings are more notable. Legal frameworks that are highly restrictive—permitting the state to remove most online content, and the law protects speech in only specific, and politically uncontroversial contexts—exhibit a significant negative relationship with government cybersecurity capacity. Within the CSS framework, these laws represent the formalisation and institutionalisation of securitisation, embedding extraordinary control into the legal structure (Bigo, 2002; Thumfart, 2024). However, this formalisation seems to prioritise political control over the development of robust technical capabilities, ultimately weakening cybersecurity capacity. The slow ratification of the Malabo Convention across Africa countries exemplifies the institutional and bureaucratic challenges that hinder the development of effective, coordinated legal frameworks (Chatham House, 2024).

Figure 4.6 below presents a stacked bar chart depicting the predicted probabilities of government cybersecurity capacity in relation to Internet legal regulation content across 50 African countries. The analysis indicates that African countries possessing the authority to remove most online content—where legal frameworks protect freedom of expression only in limited, politically neutral contexts—are most likely to be equipped to combat moderately sophisticated cyber-attacks.

Figure 4.6: Government cyber security capacity vs Internet legal regulation content in 50 African countries



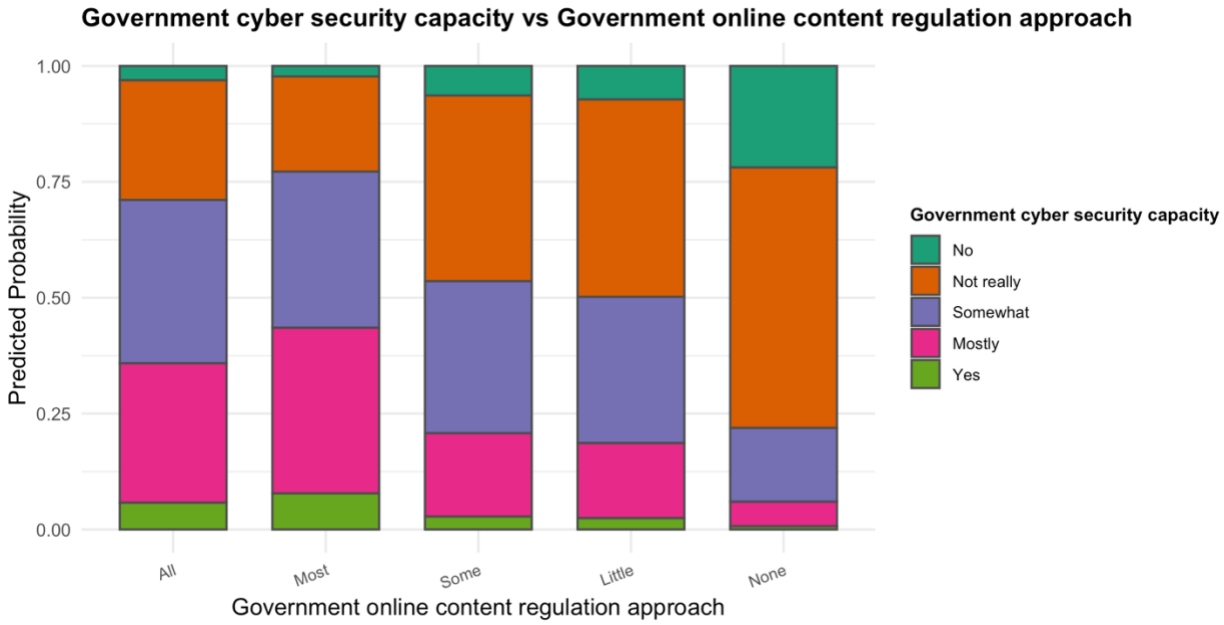
Source: Author's computation using R

4.4.4 The Role of Private Actors in Online Content Monitoring and Regulation

The involvement of private actors in monitoring and regulating online content highlights a notable disparity. In developing countries, a total dependence on private actors for this regulation is significantly negatively correlated with government cybersecurity capacity. This finding indicates that when governments fully relinquish their involvement in regulating online content, it can disrupt national strategies and expose fundamental institutional weaknesses (Kayode-Ajala, 2023).

Figure 4.7 below presents a stacked bar chart depicting the predicted probabilities of government cybersecurity capacity in relation to government online content regulation approach in 90 developing countries. The analysis indicates that developing countries that off-load all online content monitoring and regulation to private actors are most likely to be equipped to combat only unsophisticated cyber-attacks.

Figure 4.7: Government cyber security capacity vs Government online content regulation approach in 90 developing countries

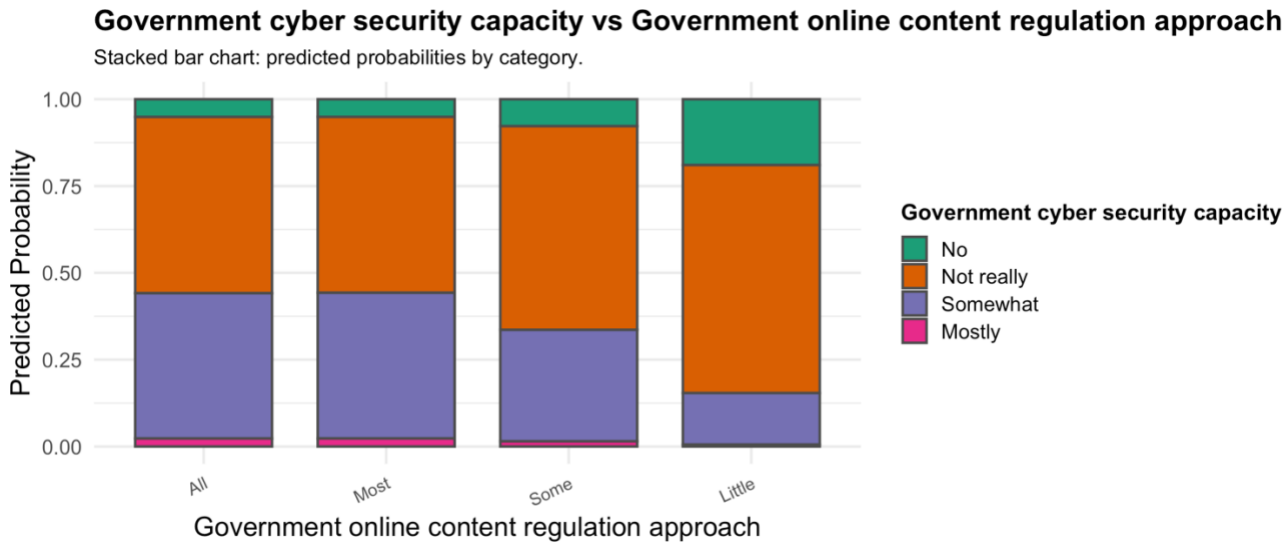


Source: Author's computation using R

Conversely, in African countries, a significant positive correlation emerges when the government adopts a less active role and engages private actors to regulate online content. This finding supports the multi-stakeholder approach promoted in recent cybersecurity agendas (Chatham House, 2024) and aligns with the CMM's focus on collaboration (Global Cyber Security Capacity Centre, 2021). In situations where state capacity is limited, utilising the expertise and resources of the private sector can effectively enhance cybersecurity efforts, as long as these public-private partnerships are transparent and accountable.

Figure 4.8 presents a stacked bar chart depicting the predicted probabilities of government cybersecurity capacity in relation to government online content regulation approach across 50 African countries. The analysis indicates that African countries engaging in some degree of online content monitoring and regulation, while also involving private actors in these processes, are most likely to be equipped to combat only unsophisticated cyber-attacks. Similarly, African countries that conduct minimal state monitoring and regulation—delegating the majority of responsibility to private actors—are most likely equipped to combat only unsophisticated cyber-attacks.

Figure 4.8: Government cyber security capacity vs Government online content regulation approach in 50 African countries



Source: Author's computation using R

4.4.5 Integration of the CSS and Oxford GCSCC CMM Frameworks

The study's findings collectively illustrate how CSS and the Oxford GCSCC CMM frameworks clarifies the determination of cybersecurity capacity. CSS emphasises that cybersecurity capacity extends beyond technical skills, encompassing socially constructed processes where governments securitise digital phenomena and institutionalise extraordinary government measures (Ramich & Piskunov, 2022). The Oxford GCSCC CMM underscores that sustainable cybersecurity capacity involves the integration of policy and strategy, cultural and societal aspects, and legal and regulatory frameworks.

A critical aspect for both groups of countries is the trade-offs involved in social media monitoring and legal framework approaches. In developing countries, government social media monitoring potentially undermines government cybersecurity capacity by diverting resources and eroding trust. In both groups, legal frameworks alone—without implementation, enforcement, and cultural acceptance—fail to enhance government cybersecurity capacity. The Oxford GCSCC CMM's emphasis on multidimensional capacity building is reinforced by these findings: formal institutions, laws, and surveillance mechanisms require complementary cultural, technical, and collaborative elements to effectively translate into effective national cybersecurity capacity.

4.4.7 Emerging Questions for Complementary Qualitative Research

While this quantitative study has identified statistically significant relationships between digital governance variables and government cybersecurity capacity across African and developing countries, the use of ordinal logistic regression reveals relationships rather than causal mechanisms. These results raise several important questions that call for additional qualitative research to offer deeper explanations, contextual insights, and a better understanding of the processes behind the statistical results.

Causal Mechanisms and Decision-Making Processes

The quantitative results indicate that in African countries, a moderate level of Internet filtering capacity seems to be negatively correlated with government cybersecurity capacity, and in developing countries, a complete filtering capacity level is positively correlated with government cybersecurity capacity. However, the regression analysis does not shed light on the decision-making processes, institutional thinking, or political considerations that drive governments to implement Internet filtering strategies. Qualitative research questions emerging from this finding include:

- What institutional and political factors lead African governments to adopt moderate Internet filtering strategies rather than comprehensive approaches or minimal intervention? Case studies focusing on specific African countries could delve into cabinet-level decision-making, inter-ministerial discussions, and the influence of international donor pressures in shaping Internet filtering policy decisions.
- How do government officials in developing countries with complete filtering capacity justify and implement these measures within broader cybersecurity frameworks? Interviews with senior policymakers, cybersecurity experts, and telecommunications regulators could help explain whether comprehensive Internet filtering results from deliberate strategic planning or gradual policy evolution.
- What trade-offs do government decision-makers perceive between internet control and developing cybersecurity capacity, and how do resource constraints affect these perceptions? Qualitative interviews could investigate budget allocation processes and competing priorities within ministries responsible for both digital regulation and cybersecurity.

Implementation Gaps and Institutional Practices

The observed negative correlation between the practical application of Internet filtering and government cybersecurity capacity in African countries—despite their theoretical ability to filter—highlights a significant gap between formal capabilities and actual implementation. While the quantitative analysis identifies this negative relationship, it does not explain the mechanisms responsible for this disconnect. Emerging research questions include:

- What institutional barriers prevent African governments from converting their regulatory capacity into effective cybersecurity implementation? Ethnographic studies within government cybersecurity agencies could explore issues such as bureaucratic division, challenges in inter-agency collaboration, shortages in skilled personnel, and resource allocation practices.
- How do telecommunications regulators, ISPs, and cybersecurity professional deal with and manage the conflicts between political mandates for Internet content filtering and their technical cybersecurity objectives? Conducting qualitative interviews with technical personnel can uncover informal solutions, professional grievances, and hidden organisational dynamics that are not evident in aggregated statistical data.
- In what ways do external entities, such as international technology companies, bilateral donors, and regional organisations, play a role in enhancing the relationship between Internet filtering techniques and cybersecurity capacity within national contexts? Case studies conducted across multiple sites can examine how external factors either facilitate or hinder the development of government cybersecurity strategies.

The Social Media Surveillance Paradox

In developing countries, government social media surveillance (i.e., at all levels) has a negative correlation with government cybersecurity capacity, indicating trade-offs in resource allocation and a decline in trust. However, quantitative analysis fails to capture the subjective experiences, organisational cultures, or public perceptions that underlie this finding. Emerging research questions include:

- What are the perceptions of citizens in developing countries with extensive social media monitoring regarding government cybersecurity efforts, and does such surveillance discourage them from engaging in joint cyber threat

reporting? Surveys and focus groups aimed at internet users could investigate the dynamics of trust, tendencies toward self-censorship, and opinions on cybersecurity initiatives led by the government.

- What organisational priorities and resource allocation strategies lead government agencies to focus more on social media monitoring than on investing in cybersecurity infrastructure? Case studies focusing on organisations within security agencies could examine the cultures of these organisations, the frameworks they use to perceive threats, and how they make decisions regarding budgets.
- How do cybersecurity experts employed by surveillance-focused governments manage the ethical dilemmas that arise between the demands for monitoring and their professional duty to create secure digital systems? Conducting in-depths interviews could reveal tensions in their professional identity and the strategies that they use to manage these issues.

Legal Framework Paradoxes

The finding that restrictive legal frameworks in African countries seem to negatively correlate with government cybersecurity capacity challenges the assumption that strong legal structures improve cybersecurity outcomes. Qualitative research is essential to understand why formal legal frameworks do not translate into effective cybersecurity capacity. Emerging research questions include:

- What factors contribute to the persistent disparity between legal frameworks established on paper and the actual enforcement capacity in African countries? By conducting comparative case studies of countries with similar legal structures but differing cybersecurity outcomes, it is possible to identify important implementation factors such as judicial capacity, political will, and the effectiveness of institutional coordination.
- What is the relationship between restrictive legal frameworks that allow for extensive state intervention in content removal and data access, and the technical priorities and ethical obligations of cybersecurity professionals? Conducting interviews with legal experts, cybersecurity analysts, and civil society representatives could uncover conflicts between legal authority and security operations.

- What factors have led to the Malabo Convention's limited success in ratification and implementation, despite its establishment of comprehensive regional cybersecurity standards? A qualitative policy analysis focusing on the ratification discussions within individual AU member states could help explain the political, institutional, and resource-related challenges involved.

Public-Private Partnerships and Governance Configurations

The differing outcomes related to the involvement of private actors in regulating online content—negative in developing countries that fully depend on private actors, yet positive in African countries with increased participation by private actors—indicate that the structure of governance is more significant than the mere division between public and private sectors. Qualitative research can investigate the organisational and relational dynamics that contribute to effective public-private partnerships. Emerging research questions include:

- What characteristics set apart successful public-private cybersecurity partnerships from those that weaken national capabilities? By examining comparative case studies of both effective and ineffective partnerships, one could pinpoint essential success elements such as transparency measures, accountability frameworks, shared threat intelligence systems, and governance structures.
- What are the views of private technology firms operating in African and developing countries on their roles and duties in enhancing national cybersecurity capabilities? Interviews with company leaders, corporate social responsibility representatives, and government relations officers could uncover the private sector's insights on potential partnerships and their limitations.
- How do power dynamics, information asymmetries, and reliance on resources influence the relationships between public and private sectors in contexts with limited resources? Ethnographic studies of partnership initiatives could explore the processes of negotiation, methods of knowledge exchange, and informal channels of influence.

Regional and Contextual Variations

The varying results observed between African and developing nations across several factors indicate that the regional context plays a crucial role in determining the

relationship between digital governance systems and government cybersecurity capabilities. However, aggregate statistical analyses fail to account for the historical, cultural, political, and institutional factors that lead to these regional disparities. Emerging research questions include:

- How do historical legacies, such as colonial governance structures, post-independence state-building paths, and experiences with regional conflicts, impact current strategies for digital governance and cybersecurity in certain African countries? Historical case studies could explore the origins of surveillance practices, the setup of institutions, and perceptions of threats.
- In what ways do regional cybersecurity norms, the spread of ideas, and peer influences affect national decisions on Internet regulation and cybersecurity investment? Qualitative research on policy diffusion, focusing on regional bodies such as the African Union, ECOWAS, and SADC, could reveal how norms are transmitted and policies are learned.
- What cultural and social factors shape public attitudes towards government Internet control, surveillance, and cybersecurity efforts in specific national contexts? Anthropological and sociological research could explore how cultural values regarding privacy, authority, community, and technology influence the relationship between governance and capacity.

The Complementary Value of Mixed Methods

These qualitative research questions collectively underscore the explanatory limitations of quantitative analysis when examining complex socio-technical phenomena such as government cybersecurity capacity. While ordinal logistic regression identifies statistically significant relationships across the two groups of countries, it falls short in uncovering the decision-making processes, organisational practices, cultural meanings, power dynamics, and implementation challenges that shape these relationships. To gain a comprehensive understanding, complementary qualitative research using case studies, elite interviews, ethnographic observation, process-tracing, and comparative historical analysis is needed to understand the causal mechanisms and contextual nuances.

Future research should therefore employ mixed methods designs that combine quantitative identification of statistical relationships with qualitative exploration of

specific cases. This approach would enable scholars to progress from mere correlation to causal explanation. Such integration would enhance both theoretical understanding—by refining CSS and CMM frameworks through empirically grounded insights—and practical policy guidance for governments, international organisations, and civil society actors working to improve cybersecurity capacity in African and developing countries.

4.5 Summary

This study examined the determinants of government cybersecurity capacity in African and developing countries through ordinal logistic regression analysis of the DSP dataset (2000–2023). The analysis revealed divergence in how digital media freedom and state Internet regulation controls relate to cybersecurity capacity development in African and developing countries, highlighting the importance of context-specific governance approaches in the Global South.

Table 4.12: Comparative Analysis of Key Findings

Regulatory Mechanism	African Countries	Developing Countries	Critical Distinction
Internet Filtering Capacity	Significant negative relationship at moderate levels (limited and adequate capacity); complete capacity shows no significant effect	Significant positive relationship only at complete capacity level	Moderate filtering capacity undermines cybersecurity capacity in African countries, whereas comprehensive capacity serves as a functional proxy for infrastructure development in developing countries
Internet Shutdowns	Significant positive relationship at all levels of shutdown capacity	Significant positive relationship only for near-total shutdown capacity	African governments demonstrate correlation between shutdown capability and cybersecurity infrastructure at all Internet shutdown levels; developing countries show this relationship only at extreme capacity levels
Internet Filtering in Practice	Significant negative relationship across all implementation frequencies (often, sometimes, rarely, never)	No significant relationship	Active filtering practices consistently undermine cybersecurity capacity in African countries regardless of frequency; regulatory practice is operationally decoupled from cybersecurity outcomes in developing countries

Government Social Media Monitoring	No significant relationship	Significant negative relationship across all social media monitoring levels	Social media surveillance mechanisms pose measurable cybersecurity capacity risks exclusively in developing countries
Legal Framework for Content Removal	Significant negative relationship when state removes most content (protecting speech only in politically uncontroversial contexts)	No significant relationship	Restrictive legal frameworks that privilege state speech control directly undermine African cybersecurity capacity; legal frameworks show no correlation with capacity in developing countries
Privacy Protection by Law Content	Significant negative relationship when government has broad access to personal data	No significant relationship	Privacy law framework functions as a cybersecurity capacity determinant in African countries; privacy law frameworks remain operationally independent from cybersecurity outcomes in developing countries
Government Capacity to Regulate Online Content	No significant relationship	Significant positive relationship at all regulatory capacity levels (limited, moderate, extensive)	Regulatory capacity measures demonstrate no cybersecurity correlation in African countries; regulatory infrastructure represents a foundational cybersecurity capacity enabler in developing countries
Government Content Regulation Approach	No significant relationship across all levels	Significant negative relationship when state delegates entirely to private actors; no relationship for other approaches	Governance delegation models show no capacity effects in African countries; exclusive private-sector regulation compromises cybersecurity outcomes in developing countries

Interpretation of Comparative Findings

The comparative analysis reveals divergent relationships between digital governance mechanisms and cybersecurity capacity across African and other developing country contexts. In African countries, the findings demonstrate a paradoxical pattern wherein governmental deployment of digital control and surveillance mechanisms—including active Internet filtering practices, restrictive legal frameworks for content removal, and expansive state access to personal data—exhibits consistent negative relationships with government cybersecurity capacity. This negative relationship suggests that the operationalisation of digital control measures may divert governmental resources, technical expertise, and institutional focus away from foundational cybersecurity

infrastructure development. The notable exception to this pattern emerges in Internet shutdown capacity, which demonstrates positive correlations with cybersecurity capacity across all levels, potentially reflecting the technical infrastructure investments required to maintain network control capabilities.

In contrast, developing countries exhibit a markedly different governance-capacity nexus characterised by positive associations between institutional regulatory capacity and cybersecurity development. Governmental capacity to regulate online content—encompassing the technical, legal, and administrative infrastructure enabling digital oversight—correlates positively with cybersecurity capacity at all measured levels (limited, moderate, and extensive). However, this relationship notably does not extend to the operational implementation of such regulatory powers. Active filtering practices and social media monitoring demonstrate either negative associations or no significant relationship with cybersecurity capacity, revealing a critical disjuncture between regulatory capacity-building and regulatory practice. This divergence suggests that the institutional and technical investments establishing regulatory capability may strengthen broader cybersecurity infrastructure, whilst the active exercise of surveillance and content control mechanisms potentially undermines capacity through resource diversion or operational priorities that deprioritise comprehensive security architecture.

These contrasting regional patterns underscore distinct developmental trajectories in cybersecurity governance, wherein African contexts demonstrate detrimental effects from operational securitisation of digital spaces, whilst other developing regions benefit from regulatory infrastructure investments that remain separated from intensive surveillance practices.

Chapter 5: Conclusion and Recommendations

The increasing digitalisation of government operations and services globally has highlighted the importance of effective cybersecurity in safeguarding national security, economic stability, and citizen data. The absence of a clear international consensus on best practices for cybersecurity capacity building, particularly within African and developing countries, underscores the need for a more comprehensive understanding of the factors that shape government cybersecurity capacity in these two groups of countries.

This study examined how state Internet control measures and digital media freedom relate to government cybersecurity capacity in African and developing countries. The quantitative analysis of the DSP dataset covered two groups of countries. This concluding chapter summarises the key findings, discusses their significance and limitations, identifies emerging questions that require further investigation, and outlines directions for future research to build upon this study.

5.1 Summary of Findings

This study investigated the determinants of government cybersecurity capacity in African and developing countries through quantitative analysis of the Digital Society Project (DSP) dataset. The analysis examined longitudinal data from 2000 to 2023 across 50 African and 90 developing countries, using ordinal logistic regression models to examine the relationships between digital media freedom, state Internet regulation, and government cybersecurity capacity.

The findings reveal distinct patterns in how digital governance mechanisms relate to cybersecurity capacity across the two regional contexts. In African countries, moderate government Internet filtering capacity demonstrated a positive relationship with government cybersecurity capacity, whilst complete capacity did not. Internet shutdown capacity demonstrated a positive correlation with cybersecurity capacity at all escalation levels. However, active Internet filtering practices and restrictive legal frameworks for content removal both showed negative relationships with government cybersecurity capacity. Government social media monitoring showed no significant relationship with government cybersecurity capacity in African countries. The

involvement of private actors in content regulation, particularly when the state assumes a less active role, seemed to be positively correlated with cybersecurity capacity.

In developing countries, the pattern differs considerably. Government capacity to regulate online content showed a positive relationship with government cybersecurity capacity across all measured levels. Internet shutdown capacity exhibited a positive relationship only at near-total capacity levels. Government social media monitoring demonstrated a negative relationship with cybersecurity capacity. Legal and regulatory frameworks showed no significant relationship with cybersecurity capacity, and complete reliance on private actors for content regulation showed a negative relationship.

The study did not support the initial hypotheses that stronger Internet control measures or robust legal frameworks would automatically enhance cybersecurity capacity. Instead, the findings demonstrate that the relationship between digital governance mechanisms and cybersecurity capacity is complex and context dependent. The effectiveness of these measures varies significantly between African and developing country contexts, challenging one-size-fits-all approaches to cybersecurity governance.

5.2 Key Insights and Emerging Questions

The divergent findings between African and developing countries raise important questions about the nature of cybersecurity capacity building in different developmental contexts. Several emerging questions require further investigation:
First, why does regulatory capacity correlate with cybersecurity capacity in developing countries but not in African countries? This distinction suggests that the relationship between institutional infrastructure and cybersecurity capacity may depend on broader governance contexts, implementation capacity, or the effectiveness of existing institutions. Understanding these contextual factors requires investigation beyond the aggregate regional level.

Second, why do active surveillance and filtering practices appear to undermine cybersecurity capacity in African countries whilst regulatory capacity shows no such

negative effect? This paradox suggests a potential disconnection between the formal capacity to regulate digital content and the actual practice of surveillance. The distinction raises questions about whether intensive surveillance practices may divert resources or institutional focus away from foundational cybersecurity infrastructure, or whether they reflect governance priorities that differ from cybersecurity development.

Third, the findings reveal an interesting dynamic regarding private actor involvement in content regulation. In African countries, greater private sector involvement appears associated with higher cybersecurity capacity, whilst the opposite is true in developing countries. This contradiction warrants investigation into the nature of public-private partnerships in cybersecurity governance, the capacity and accountability of private actors in different contexts, and how public-private partnerships shape cybersecurity outcomes.

Fourth, the weak or absent relationships between legal frameworks and cybersecurity capacity in both regions challenge assumptions about the importance of formal regulatory frameworks. This raises questions about whether cybersecurity capacity development requires different institutional foundations than those provided by content regulation frameworks, or whether legal frameworks matter differently depending on how they are implemented and enforced.

5.3 Limitations and Implications for Future Research

The quantitative approach employed in this study has provided broad regional patterns and statistical relationships, but it cannot explain the reasons, contexts, and motivations behind these findings. Several specific limitations point towards important avenues for future research.

The study's reliance on ordinal variables and aggregate regional analysis masks important variations within countries and between different types of states. Future research should employ sub-national analysis to examine how cybersecurity capacity differs across regions, provinces, or states within African and developing countries. This approach could reveal whether findings hold consistently across different administrative levels or whether significant disparities exist that reflect local contexts and governance structures.

The potential subjectivity of expert assessments in the DSP dataset, whilst ensuring contextual knowledge, may not capture all dimensions of government cybersecurity capacity or may reflect perspectives on what constitutes effective cybersecurity governance. Qualitative research methods could complement this study by providing direct evidence of government cybersecurity capacity through examination of actual policies, institutional structures, and implementation practices. Qualitative case studies of countries in both groups could offer rich understanding of how cybersecurity capacity develops in practice, examining factors such as institutional arrangements, resource allocation, technical expertise, and political will.

The quantitative approach also limits understanding of how and why certain relationships exist. Policy ethnographies—detailed examinations of how cybersecurity policies are developed, negotiated, and implemented within specific government settings—could reveal the processes through which Internet regulation and digital governance mechanisms influence cybersecurity capacity. This approach would be particularly valuable for understanding the disconnection between regulatory capacity and active surveillance practices observed in the findings.

Additionally, network analysis represents a complementary methodological approach that could enhance understanding of cybersecurity governance. Examining networks of cybersecurity actors (government agencies, private sector partners, international organisations, civil society), their interconnection, and their influence could reveal how cybersecurity capacity develops through relationships and coordination rather than through isolated policy measures. This approach might explain variations between countries and show how different network structures affect cybersecurity capacity outcomes.

5.3 Directions for Future Research

Several specific research directions emerge from the gaps and questions identified in this study.

Comparative analysis between African and developing countries could investigate whether the distinctions observed reflect fundamental differences in governance

models, institutional capacity, economic resources, or external influences such as international cybersecurity norms and donor priorities. This analysis would benefit from mixed-methods approaches combining quantitative comparison with qualitative investigation of country-specific contexts.

Sub-national studies within both African and developing countries would reveal whether the regional patterns identified hold consistently across different administrative levels, or whether significant variations exist. Such studies could examine how local governance structures, resource availability, technical expertise, and security challenges affect cybersecurity capacity at provincial, state, or municipal levels.

In-depth qualitative case studies of specific countries experiencing different trajectories of cybersecurity capacity development would provide detailed understanding of how and why digital governance policies influence cybersecurity outcomes. These cases could examine how governments prioritise competing demands between surveillance, content regulation, and cybersecurity infrastructure investment.

Longitudinal qualitative research tracking changes in cybersecurity capacity over time within selected countries could help explain the processes through which capacity develops or declines. This approach could examine how policy shifts, institutional changes, technological developments, and external pressures influence cybersecurity capacity trajectories.

Research investigating the actual functioning and effectiveness of public-private partnerships in cybersecurity governance could explain why private actor involvement shows different effects across regions. This research could examine partnership structures, resource allocation, accountability mechanisms, and capacity distribution between state and private actors.

Studies examining the implementation and enforcement of legal and regulatory frameworks for content regulation could reveal why formal legal frameworks show limited relationship with cybersecurity capacity. This research might clarify whether

cybersecurity capacity development requires different institutional foundations than those provided by content regulation frameworks.

Finally, international and comparative research examining how different national contexts interpret and implement international cybersecurity norms and standards could illuminate whether global cybersecurity governance frameworks are appropriately adapted to African and developing country contexts, or whether they reflect assumptions better suited to more developed governance systems.

5.5 Conclusion

This study has advanced understanding of the complex and context-dependent relationships between digital governance, Internet regulation and monitoring, and government cybersecurity capacity in African and developing countries. By revealing that these relationships differ significantly between these two groups of countries, the research challenges assumptions that universal approaches to cybersecurity governance will be equally effective across different contexts. The distinct patterns observed suggest that cybersecurity capacity building requires careful attention to regional governance contexts, institutional structures, and the specific ways in which different regulatory mechanisms operate within political and economic environments.

However, the quantitative findings represent only one dimension of understanding these complex relationships. The emerging questions identified—particularly regarding the disconnection between formal regulatory capacity and active surveillance practices, the effects of private actor involvement, and the weak role of legal frameworks—require investigation through complementary research methods. Qualitative case studies, policy ethnographies, network analysis, and sub-national research will provide the detailed understanding and explanations necessary to show how and why these patterns emerge and how they operate in practice.

Future research in cybersecurity capacity should engage these different approaches to build on the foundation established by this study, moving from identifying statistical relationships to understanding the processes, contexts, and reasons that shape cybersecurity capacity development in African and developing countries.

Reference List

Afiyah, S. (2024). The Impact of E-Government Services, Citizen Participation, and Transparency on Public Trust in Government. *Global International Journal of Innovative Research*, *2*(6), 1246–1261. https://doi.org/10.59613/global.v2i6.200

Allen, N. (2021, January 19). *Africa's Evolving Cyber Threats*. Africa Center for Strategic Studies. https://africacenter.org/spotlight/africa-evolving-cyber-threats/

Amnesty International UK. (2025, April 1). *Why we're taking the UK government to court over mass spying*. Mass Surveillance. https://www.amnesty.org.uk/why-taking-government-court-mass-spying-gchq-nsa-tempora-prism-edward-snowden

Annarelli, A., Nonino, F., & Palombi, G. (2020). Understanding the management of cyber resilient systems. *Computers & Industrial Engineering*, *149*, 106829. https://doi.org/10.1016/j.cie.2020.106829

Arslan, A. S. (2023). Neorealist Analysis of Security Dilemma in Cyberspace; A Quantitative Study. *APSA Preprints*. https://doi.org/10.33774/apsa-2023-wvw2z-v6

Ayalew, Y. E. (2019). The Internet shutdown muzzle(s) freedom of expression in Ethiopia: Competing narratives. *Information & Communications Technology Law*, *28*(2), 208–224. https://doi.org/10.1080/13600834.2019.1619906

Bánhidi, Z., & Dobos, I. (2024). Measuring digital development: Ranking using data envelopment analysis (DEA) and network readiness index (NRI). *Central European Journal of Operations Research*, *32*, 1089–1108. https://doi.org/10.1007/s10100-024-00919-y

Ben Naseir, M., Dogan, H., Apeh, E., & Ali, R. (2020). National Cybersecurity Capacity Building Framework for Countries in a Transitional Phase. *Proceedings of the 22nd International Conference on Enterprise Information Systems*, 841–849. https://doi.org/10.5220/0009576708410849

Bennett, P., & Naim, M. (2015, January 5). *21st-century censorship*. Columbia Journalism Review. https://www.cjr.org/cover_story/21st_century_censorship.php

Bigo, D. (2002). Security and Immigration: Toward a Critique of the Governmentality of Unease. *Alternatives: Global, Local, Political*, *27*(1_suppl), 63–92. https://doi.org/10.1177/03043754020270S105

Bruggemann, R., Koppatz, P., Scholl, M., & Schuktomow, R. (2022). Global Cybersecurity Index (GCI) and the Role of its 5 Pillars. *Social Indicators Research*, *159*(1), 125–143. https://doi.org/10.1007/s11205-021-02739-y

Buzan, B., Waever, O., & Wilde, J. de. (1998). *Security: A New Framework for Analysis*. Lynne Rienner Publishers.

Calderaro, A., & Craig, A. J. S. (2020). Transnational governance of cybersecurity: Policy challenges and global inequalities in cyber capacity building. *Third World Quarterly*, *41*(6), 917–938. https://doi.org/10.1080/01436597.2020.1729729

Caprioli, M. (2004). Democracy and Human Rights Versus Women's Security: A Contradiction? *Security Dialogue*, *35*(4), 411–428. https://doi.org/10.1177/0967010604049520

Cavelty, M. D. (2024). *The Politics of Cyber-Security* (1st edn). Routledge.

Chatham House. (2024, February 23). *The AU took important action on cybersecurity at its 2024 summit – but more is needed*. https://www.chathamhouse.org/2024/02/au-took-important-action-cybersecurity-its-2024-summit-more-needed

Conduit, D. (2025). Digital Authoritarianism and the Global Technology Industry: Evidence from Iran. *Government and Opposition*, *60*(3), 751–772. https://doi.org/10.1017/gov.2024.31

Coppedge, M., Gerring, J., Knutsen, C. H., Lindberg, S. I., Teorell, J., Altman, D., Angiolillo, F., Bernhard, M., Borella, C., Cornell, A., Fish, S., Fox, L., Gastaldi, L., Gjerløw, H.,

Glynn, A., God, A. G., Grahn, S., Hicken, A., Kinzelbach, K., … Ziblatt, D. (2024). *V-Dem Codebook*. Varieties of Democracy (V-Dem) Project. https://www.v-dem.net/documents/38/V-Dem_Codebook_v14.pdf

Coppedge, M., Gerring, J., Knutsen, C. H., Lindberg, S. I., Teorell, J., Gastaldi, L., God, A. G., & Grahn, S. (2024). *V-Dem Country Coding Units v14*. Varieties of Democracy (V-Dem) Project. https://www.v-dem.net/documents/40/v-dem_countryunit_v14.pdf

Coppedge, M., Gerring, J., Knutsen, C. H., Lindberg, S. I., Teorell, J., Marquadt, K. L., Medzihorsky, J., Pemstein, D., Fox, L., Gastaldi, L., Pernes, J., Rydén, O., Tzelgov, E., Wang, Y., & Wilson, S. (2024). *V-Dem Methodology v14*. Varieties of Democracy (V-Dem) Project. https://v-dem.net/documents/38/V-Dem_Codebook_v14.pdf

Creese, S., Dutton, W. H., & Esteve-González, P. (2021). The social and cultural shaping of cybersecurity capacity building: A comparative study of nations and regions. *Personal and Ubiquitous Computing*, *25*(5), 941–955. https://doi.org/10.1007/s00779-021-01569-6

Creese, S., Dutton, W. H., Esteve-González, P., & Shillair, R. (2021). Cybersecurity capacity-building: Cross-national benefits and international divides. *Journal of Cyber Policy*, *6*(2), 214–235. https://doi.org/10.1080/23738871.2021.1979617

Cross, C. (2021). Dissent as cybercrime: Social media, security and development in Tanzania. *Journal of Eastern African Studies*, *15*(3), 442–463. https://doi.org/10.1080/17531055.2021.1952797

Cyber Security Intelligence. (2017, May 22). *The Difference Between Cyberspace & The Internet*. https://www.cybersecurityintelligence.com/blog/the-difference-between-cyberspace-and-the-internet-2412.html

Czuba, K. (2025). Government Digital Surveillance in Africa. *Governance*, *38*(4), 1–24. https://doi.org/10.1111/gove.70049

Da Vinha, L. (2024). Smart for Whom? Africa's Smart Cities and Digital Authoritarianism. *International Journal of Intelligence and CounterIntelligence*, *37*(3), 941–959. https://doi.org/10.1080/08850607.2023.2284629

Datta, A. (2024). Towards a Framework for Analysing Complex Interdependence in Digital Espionage Markets. *European Conference on Cyber Warfare and Security*, *23*(1), 679–686. https://doi.org/10.34190/eccws.23.1.2231

De Lanerolle, I. (2016, June 1). *Internet freedom: Why access is becoming a human right*. Stories. https://www.wits.ac.za/future/stories/internet-freedom-why-access-is-becoming-a-human-right.html

DeMaris, A. (1995). A Tutorial in Logistic Regression. *Journal of Marriage and the Family*, *57*(4), 956. https://doi.org/10.2307/353415

Digital Society Project. (2024a). *Expert Survey Data*. https://digitalsocietyproject.org/data/

Digital Society Project. (2024b). *The Project*. https://digitalsocietyproject.org/the-project/

Djuraev, I., Baratov, A., Khujayev, S., Yakubova, I., Rakhmonova, M., Mukumov, B., & Abdurakhmanova, N. (2025). The Impact of Digitization on Legal Systems in Developing Countries. *Qubahan Academic Journal*, *5*(1), 81–117. https://doi.org/10.48161/qaj.v5n1a1246

Dutton, W. H., Creese, S., Shillair, R., & Bada, M. (2019). Cybersecurity Capacity: Does It Matter? *Journal of Information Policy*, *9*, 280–306. https://doi.org/10.5325/jinfopoli.9.2019.0280

Egloff, F. J. (2022). Using a Historical Analogy as a Research Strategy. In F. J. Egloff (Ed.), *Semi-State Actors in Cybersecurity* (pp. 17–38). Oxford University Press. https://doi.org/10.1093/oso/9780197579275.003.0002

E-Governance Academy. (n.d.-a). *Methodology*. Description of Indicators. Retrieved 3 October 2025, from https://ncsi.ega.ee/indicators/

E-Governance Academy. (n.d.-b). *National Cyber Security Index 3.0 Methodology*. E-Governance Academy. Retrieved 20 July 2024, from https://ega.ee/wp-content/uploads/2023/08/NCSI-3.0_Methodology.pdf

e-Governance Academy. (2023). *NCSI 2016-2023*. Archived Data from 01.09.2023. https://ncsi.ega.ee/ncsi-index/?archive=1

Ehimuan, B., Ob, O. C., Onyinyechi Vivian Akagha, Oluwatosin Reis, & Bisola Beatrice Oguejiofor. (2024). Global data privacy laws: A critical review of technology's impact on user rights. *World Journal of Advanced Research and Reviews*, *21*(2), 1058–1070. https://doi.org/10.30574/wjarr.2024.21.2.0369

Fasel, M., & Weerts, S. (2024). Can Facebook's community standards keep up with legal certainty? Content moderation governance under the pressure of the Digital Services Act. *Policy & Internet*, *16*(3), 588–606. https://doi.org/10.1002/poi3.391

Florax, R. J. G. M., & De Graaff, T. (2004). The Performance of Diagnostic Tests for Spatial Dependence in Linear Regression Models: A Meta-Analysis of Simulation Studies. In L. Anselin, R. J. G. M. Florax, & S. J. Rey (Eds), *Advances in Spatial Econometrics* (pp. 29–65). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-662-05617-2_2

Forbes. (2022, August 2). *Africa's Chaotic Legal And Regulatory Cybersecurity Landscape Requires Harmonization*. Innovation. https://www.forbes.com/sites/forbestechcouncil/2022/08/02/africas-chaotic-legal-and-regulatory-cybersecurity-landscape-requires-harmonization/

Freedom House. (2016). *Silencing the Messenger: Communication Apps Under Pressure*. Freedom on the Net 2016. https://freedomhouse.org/report/freedom-net/2016/silencing-messenger-communication-apps-under-pressure

Freuler, J. O. (2023). The weaponization of private corporate infrastructure: Internet fragmentation and coercive diplomacy in the 21st century. *Global Media and China*, *8*(1), 6–23. https://doi.org/10.1177/20594364221139729

Giacalone, M., Panarello, D., & Mattera, R. (2018). Multicollinearity in regression: An efficiency comparison between Lp-norm and least squares estimators. *Quality & Quantity*, *52*(4), 1831–1859. https://doi.org/10.1007/s11135-017-0571-y

Global Cyber Security Capacity Centre. (2021). *Cybersecurity Capacity Maturity Model for Nations (CMM)*. University of Oxford. https://gcscc.ox.ac.uk/files/cmm2021editiondocpdf

Global Cyber Security Capacity Centre, Cybersecurity Capacity Centre for Southern Africa, Oceania Cyber Security Centre, & Oxford Martin School. (2020, April 28). *Cybersecurity Capacity Maturity Model for Nations (CMM): Structure and Deployment Methodology* [Meeting]. https://cybilportal.org/wp-content/uploads/2020/04/GFCE-V-Meeting-Assessments-GCSCC.pdf

Gohdes, A. R. (2024). *Repression in the Digital Age: Surveillance, Censorship, and the Dynamics of State Violence*. Oxford University Press. https://doi.org/10.1093/oso/9780197743577.001.0001

Gomez, J. F., Machado, C., Paes, L. M., & Calmon, F. (2024). Algorithmic Arbitrariness in Content Moderation. *The 2024 ACM Conference on Fairness, Accountability, and Transparency*, 2234–2253. https://doi.org/10.1145/3630106.3659036

Gozgor, G., Lau, C. K., Lin, Z., & Zeng, Y. (2024). The impact of digital governance on tourism development. *Journal of Digital Economy*, *3*, 1–13. https://doi.org/10.1016/j.jdec.2024.05.003

Gravett, W. (2020). Digital neo-colonialism: The Chinese model of internet sovereignty in Africa. *African Human Rights Law Journal*, *20*(1), 1–22. https://doi.org/10.17159/1996-2096/2020/v20n1a5

Grinberg, D. (2017). Chilling Developments: Digital Access, Surveillance, and the Authoritarian Dilemma in Ethiopia. *Surveillance & Society*, *15*(3/4), 432–438. https://doi.org/10.24908/ss.v15i3/4.6623

Gros, V., de Goede, M., & İşleyen, B. (2017). The Snowden Files Made Public: A Material Politics of Contesting Surveillance. *International Political Sociology*, *11*(1), 73–89. https://doi.org/10.1093/ips/olw031

Gutwirth, S., & De Hert, P. (2022). Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power. *Direito Público*, *18*(100). https://doi.org/10.11117/rdp.v18i100.6200

Hosmer, D. W., & Lemeshow, S. (2000). Introduction to the Logistic Regression Model. In *Applied Logistic Regression* (1st edn). Wiley. https://doi.org/10.1002/0471722146

Ifeanyi-Ajufo, N. (2023). Cyber governance in Africa: At the crossroads of politics, sovereignty and cooperation. *Policy Design and Practice*, *6*(2), 146–159. https://doi.org/10.1080/25741292.2023.2199960

International Monetary Fund. (2024, April). *World Economic Outlook Database*. IMF. https://www.imf.org/en/Publications/WEO/weo-database/2024/April/weo-report?c=512,914,612,171,614,311,213,911,314,193,122,912,313,419,513,316,913,124,339,638,514,218,963,616,223,516,918,748,618,624,522,622,156,626,628,228,924,233,632,636,634,238,662,960,423,935,128,611,321,243,248,469,253,642,643,939,734,644,819,172,132,646,648,915,134,652,174,328,258,656,654,336,263,268,532,944,176,534,536,429,433,178,436,136,343,158,439,916,664,826,542,967,443,917,544,941,446,666,668,672,946,137,546,674,676,548,556,678,181,867,682,684,273,868,921,94

8,943,686,688,518,728,836,558,138,196,278,692,694,962,142,449,564,565,283,853,288,293,566,964,182,359,453,968,922,714,862,135,716,456,722,942,718,724,576,936,961,813,726,199,733,184,524,361,362,364,732,366,144,146,463,528,923,738,578,537,742,866,369,744,186,925,869,746,926,466,112,111,298,927,846,299,582,487,474,754,698,&s=PPPPC,&sy=2022&ey=2029&ssm=0&scsm=1&scc=0&ssd=1&ssc=0&sic=0&sort=country&ds=.&br=1

International Telecommunications Union. (2021a). *Global Cybersecurity Index 2020* (No. 4). https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

International Telecommunications Union. (2021b, June 25). *Global Cybersecurity Index 2020 – Frequently Asked Questions*. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv4/GCI-FAQ.pdf

International Telecommunications Union. (2024). *Global Cybersecurity Index 2024* (No. 5). https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf

INTERPOL. (2021). *African Cyberthreat Assessment Report*. https://www.interpol.int/content/download/16759/file/AfricanCyberthreatAssessment_ENGLISH.pdf

Irum, S. A., & Al Sharqi, L. (2015). Media censorship: Freedom versus responsibility. *Journal of Law and Conflict Resolution*, *7*(4), 21–24. https://doi.org/10.5897/JLCR2015.0207

ITU-T. (2008). *Overview of cybersecurity* (No. X.1205; Series X: Data Networks, Open System Communications and Security). https://www.itu.int/rec/T-REC-X.1205-200804-I

Jeffrey, J. (2016, November 17). *Ethiopia's internet crackdown hurts everyone*. Aid and Policy. https://www.thenewhumanitarian.org/analysis/2016/11/17/ethiopia-s-internet-crackdown-hurts-everyone

Jones, R. (2009). Agents of Exception: Border Security and the Marginalization of Muslims in India. *Environment and Planning D: Society and Space*, *27*(5), 879–897. https://doi.org/10.1068/d10108

Judge, M. A., Manzoor, A., Maple, C., Rodrigues, J. J. P. C., & Islam, S. U. (2021). Price-based demand response for household load management with interval uncertainty. *Energy Reports*, *7*, 8493–8504. https://doi.org/10.1016/j.egyr.2021.02.064

Kabanda, S., Tanner, M., & Kent, C. (2018). Exploring SME cybersecurity practices in developing countries. *Journal of Organizational Computing and Electronic Commerce*, *28*(3), 269–282. https://doi.org/10.1080/10919392.2018.1484598

Kalema, N. L. (2024). The 'Digital Transformation for Development' Anti-Politics Machine: A Case Study on Global Digital Development Governance and Public-Sector Digital Transformation in Uganda. *Policy & Internet*, *16*(4), 750–763. https://doi.org/10.1002/poi3.436

Karlekar, K. D., & Dunham, J. (2014). *Media Freedom Hits A Decade Low*. Freedom House. https://freedomhouse.org/report/freedom-press/2014/media-freedom-hits-decade-low

Karpa, D., & Rochlitz, M. (2023, May 21). *Authoritarian Surveillance and Public Support for Digital Governance Solutions*. http://dx.doi.org/10.2139/ssrn.4454627

Kauermann, G. (2000). Modeling Longitudinal Data with Ordinal Response by Varying Coefficients. *Biometrics*, *56*(3), 692–698. https://doi.org/10.1111/j.0006-341X.2000.00692.x

Kayode-Ajala, O. (2023). Establishing Cyber Resilience in Developing Countries: An Exploratory Investigation into Institutional, Legal, Financial, and Social Challenges.

International Journal of Sustainable Infrastructure for Cities and Societies, *8*(9), Article 9.

Khalil, A., Bitar, M., & Anandha Krishna Raj, S. (2024). A New Era of Armed Conflict: The Role of State and Non-State Actors in Cyber Warfare with Special Reference to Russia-Ukraine War. *TalTech Journal of European Studies*, *14*(2), 49–72. https://doi.org/10.2478/bjes-2024-0016

Kondratov, E., & Johansson-Nogués, E. (2023). Russia's Hybrid Interference Campaigns in France, Germany and the UK: A Challenge against Trust in Liberal Democracies? *Geopolitics*, *28*(5), 2169–2199. https://doi.org/10.1080/14650045.2022.2129012

Kumar, S. (2024). China's Digital Expansionism in Africa and the US Counter-Strategies. *Insight on Africa*, *16*(2), 146–165. https://doi.org/10.1177/09750878231217957

Kuzior, A., Tiutiunyk, I., Zielińska, A., & Kelemen, R. (2024). Cybersecurity and cybercrime: Current trends and threats. *JOURNAL OF INTERNATIONAL STUDIES*, *17*(2), 220–239. https://doi.org/10.14254/2071-8330.2024/17-2/12

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

Llansó, E. J. (2020). No amount of "AI" in content moderation will solve filtering's prior-restraint problem. *Big Data & Society*, *7*(1), 205395172092068. https://doi.org/10.1177/2053951720920686

Lyon, D. (2003). *Surveillance After September 11*. Polity Press.

Makulilo, A. B. (2015). Myth and reality of harmonisation of data privacy policies in Africa. *Computer Law & Security Review*, *31*(1), 78–89. https://doi.org/10.1016/j.clsr.2014.11.005

Malaivongs, S., Kiattisin, S., & Chatjuthamard, P. (2022). Cyber Trust Index: A Framework for Rating and Improving Cybersecurity Performance. *Applied Sciences*, *12*(21), 1–27. https://doi.org/10.3390/app122111174

Mark, N. C., & Sul, D. (2003). Cointegration Vector Estimation by Panel DOLS and Long-run Money Demand. *Oxford Bulletin of Economics and Statistics*, *65*(5), 655–680. https://doi.org/10.1111/j.1468-0084.2003.00066.x

Marquadt, K. (2023). *Methodology*. V-Dem Methodology. https://v-dem.net/about/v-dem-project/methodology/

Matfess, H. (2015). Rwanda and Ethiopia: Developmental Authoritarianism and the New Politics of African Strong Men. *African Studies Review*, *58*(2), 181–204. https://doi.org/10.1017/asr.2015.43

McGee, R. (2023). The governance shock doctrine: Civic space in the pandemic. *Development Policy Review*, *41*(S1), 1–21. https://doi.org/10.1111/dpr.12678

Mckinsey & Company. (2020, September 16). *The role of government cybersecurity efforts in combating risks*. Our Insights. https://www.mckinsey.com/industries/public-sector/our-insights/follow-the-leaders-how-governments-can-combat-intensifying-cybersecurity-risks

Mechkova, V., Pemstein, D., Seim, B., & Wilson, S. (2019). *Digital Society Project Working Paper*. *1*. https://digitalsocietyproject.org/wp-content/uploads/2019/05/DSP_WP_01-Introducing-the-Digital-Society-Project.pdf

Mechkova, V., Pemstein, D., Seim, B., & Wilson, Steven. L. (2024). Measuring online political activity: Introducing the digital society project dataset. *Journal of Information Technology & Politics*, 1–17. https://doi.org/10.1080/19331681.2024.2350495

Merhi, M. I., & Bregu, K. (2020). Effective and efficient usage of big data analytics in public sector. *Transforming Government: People, Process and Policy*, *14*(4), 605–622. https://doi.org/10.1108/TG-08-2019-0083

Michaelsen, M. (2018). Transforming Threats to Power: The International Politics of Authoritarian Internet Control in Iran. *International Journal of Communication*, *12*, 3856–3876.

Michaelsen, M., & Ruijgrok, K. (2024). Digital Authoritarianism. In A. Wolf (Ed.), *The Oxford Handbook of Authoritarian Politics*. Oxford University Press. https://doi.org/10.1093/oxfordhb/9780198871996.013.59

Midi, H., Sarkar, S. K., & Rana, S. (2010). Collinearity diagnostics of binary logistic regression model. *Journal of Interdisciplinary Mathematics*, *13*(3), 253–267. https://doi.org/10.1080/09720502.2010.10700699

Monaci, S., & Persico, S. (2025). Regulating Disinformation and Ideological Entrepreneurs: An Exploratory Research on the Digital Services Act Implementation. *Media and Communication*, *13*. https://doi.org/10.17645/mac.9471

Mueller, M. L. (2010). *Networks and States: The Global Politics of Internet Governance*. The MIT Press. https://doi.org/10.7551/mitpress/9780262014595.001.0001

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

Nadella, G. S., Gonaygunta, H., Harish, M., & Whig, P. (2024). Privacy and Security: Safeguarding Personal Data in the AI Era. In P. Bhattacharya, A. Hassan, H. Liu, & B. Bhushan (Eds), *Advances in Human and Social Aspects of Technology* (pp. 157–174). IGI Global. https://doi.org/10.4018/979-8-3693-4147-6.ch007

Newman, E. (2010). Critical human security studies. *Review of International Studies*, *36*(1), 77–94. https://doi.org/10.1017/S0260210509990519

Obia, V. (2023). Regulatory Annexation: Extending Broadcast Media Regulation to Social Media and Internet Content. *Communication Law and Policy*, *28*(2), 99–123. https://doi.org/10.1080/10811680.2023.2206382

Obia, V. (2025). Digital policy and Nigeria's Platform Code of Practice: Towards a radical co-regulatory turn. *Data & Policy*, *7*. https://doi.org/10.1017/dap.2025.1

O'Brien, R. (2022). *The Cyber Defense Index 2022/23*. MIT Technology Review Insights. https://mittrinsights.s3.amazonaws.com/CDIreport.pdf

Odueso, T. (2022, May 6). *Africa is losing $4 billion annually to cybercrime. Can conversations at Cyber Africa Forum help?* TechCabal. https://techcabal.com/2022/05/06/africa-cybercrime-cyber-africa-forum/

OECD. (2024). *New perspectives on measuring cybersecurity* (OECD Digital Economy Papers No. 366; OECD Digital Economy Papers, Vol. 366). https://doi.org/10.1787/b1e31997-en

Onumo, A., Cullen, A., & Ullah-Awan, I. (2017). An Empirical Study of Cultural Dimensions and Cybersecurity Development. *2017 IEEE 5th International Conference on Future Internet of Things and Cloud (FiCloud)*, 70–76. https://doi.org/10.1109/FiCloud.2017.41

Otukoya, T. A. (2024). The securitization theory. *International Journal of Science and Research Archive*, *11*(1), 1747–1755. https://doi.org/10.30574/ijsra.2024.11.1.0225

Padmanabhan, R., Filastò, A., Xynou, M., Raman, R. S., Middleton, K., Zhang, M., Madory, D., Roberts, M., & Dainotti, A. (2021). A multi-perspective view of Internet censorship in Myanmar. *Proceedings of the ACM SIGCOMM 2021 Workshop on*

Free and Open Communications on the Internet, 27–36. https://doi.org/10.1145/3473604.3474562

Pagallo, U. (2015). Cyber Force and the Role of Sovereign States in Informational Warfare. *Philosophy & Technology*, *28*(3), 407–425. https://doi.org/10.1007/s13347-014-0177-4

Park, H., & Lee, T. (David). (2018). Adoption of E-Government Applications for Public Health Risk Communication: Government Trust and Social Media Competence as Primary Drivers. *Journal of Health Communication*, *23*(8), 712–723. https://doi.org/10.1080/10810730.2018.1511013

Pawlak, P., & Barmpaliou, P.-N. (2017). Politics of cybersecurity capacity building: Conundrum and opportunity. *Journal of Cyber Policy*, *2*(1), 123–144. https://doi.org/10.1080/23738871.2017.1294610

Peng, C.-Y. J., Lee, K. L., & Ingersoll, G. M. (2002). An Introduction to Logistic Regression Analysis and Reporting. *The Journal of Educational Research*, *96*(1), 3–14. https://doi.org/10.1080/00220670209598786

Petersen, K. L. (2011). Risk analysis – A field within security studies? *European Journal of International Relations*, *18*(4), 693–717. https://doi.org/10.1177/1354066111409770

Pohle, J., Nanni, R., & Santaniello, M. (2024). Unthinking Digital Sovereignty: A Critical Reflection on Origins, Objectives, and Practices. *Policy & Internet*, *16*(4), 666–671. https://doi.org/10.1002/poi3.437

Pohle, J., & Santaniello, M. (2024). From multistakeholderism to digital sovereignty: Toward a new discursive order in internet governance? *Policy & Internet*, *16*(4), 672–691. https://doi.org/10.1002/poi3.426

Portulans Institute. (2023a). *Countries*. https://networkreadinessindex.org/countries/

Portulans Institute. (2023b). *Network Readiness Index 2023*. https://download.networkreadinessindex.org/reports/nri_2023.pdf

Quintais, J. P., Appelman, N., & Ó Fathaigh, R. (2023). Using Terms and Conditions to apply Fundamental Rights to Content Moderation. *German Law Journal*, *24*(5), 881–911. https://doi.org/10.1017/glj.2023.53

Rami, A. A. M. (2024). Navigating Challenges in Policy Development: Addressing Political, Institutional, and Cultural Challenges. *FMDB Transactions on Sustainable Social Sciences Letters*, *2*(2), 56–69. https://doi.org/10.69888/FTSSSL.2024.000220

Ramich, M. S., & Piskunov, D. A. (2022). The Securitization of Cyberspace: From Rulemaking to Establishing Legal Regimes. *Vestnik RUDN. International Relations*, *22*(2), 238–255. https://doi.org/10.22363/2313-0660-2022-22-2-238-255

Reva, D. (2021, July 29). *Cyber attacks expose the vulnerability of South Africa's ports*. ISS Africa. https://issafrica.org/iss-today/cyber-attacks-expose-the-vulnerability-of-south-africas-ports

Roberts, T. (2021). *Digital Rights in Closing Civic Space: Lessons from Ten African Countries*. Institute of Development Studies. https://doi.org/10.19088/IDS.2021.003

Roberts, T., & Oosterom, M. (2024). Digital authoritarianism: A systematic literature review. *Information Technology for Development*, 1–25. https://doi.org/10.1080/02681102.2024.2425352

Rothschild, V. (2024). Protest and repression in China's digital surveillance state. *Journal of Information Technology & Politics*, 1–16. https://doi.org/10.1080/19331681.2024.2326464

Sarker, I. H. (2021). CyberLearning: Effectiveness analysis of machine learning security modeling to detect cyber-anomalies and multi-attacks. *Internet of Things*, *14*, 100393. https://doi.org/10.1016/j.iot.2021.100393

Schumann, M. P. (2025). Legalizing control: The rise of restrictive internet regulation in sub-Saharan Africa. *Democratization*, 1–26. https://doi.org/10.1080/13510347.2025.2503370

Shabaz, A. (2018). *The Rise of Digital Authoritarianism*. Freedom House. https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism

Shahid, F., & Vashistha, A. (2023). Decolonizing Content Moderation: Does Uniform Global Community Standard Resemble Utopian Equality or Western Power Hegemony? *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, 1–18. https://doi.org/10.1145/3544548.3581538

Shao, D., Ishengoma, F., Nikiforova, A., & Swetu, M. (2025). Comparative analysis of data protection regulations in East African countries. *Digital Policy, Regulation and Governance*, *27*(4), 486–501. https://doi.org/10.1108/DPRG-06-2024-0120

Shrestha, N. (2020). Detecting Multicollinearity in Regression Analysis. *American Journal of Applied Mathematics and Statistics*, *8*(2), 39–42. https://doi.org/10.12691/ajams-8-2-1

Signé, L., & Signé, K. (2021, March 16). *How African states can improve their cybersecurity*. Brookings. https://www.brookings.edu/articles/how-african-states-can-improve-their-cybersecurity/

Solum, L. B. (2009). Models of Internet governance. In L. A. Bygrave & J. Bing (Eds), *Internet Governance: Infrastructure and Institutions* (p. 0). Oxford University Press. https://doi.org/10.1093/acprof:oso/9780199561131.003.0003

Spector, L. (2022). Cyber Offense and a Changing Strategic Paradigm. *The Washington Quarterly*, *45*(1), 38–56. https://doi.org/10.1080/0163660X.2022.2054123

StataCorp. (2024). *Statistical software for data science*. Home. https://www.stata.com/

Statista. (2024, April). *Internet and social media users in the world 2024*. Statista. https://www.statista.com/statistics/617136/digital-population-worldwide/

Stevens, A., Fussey, P., Murray, D., Hove, K., & Saki, O. (2023). 'I started seeing shadows everywhere': The diverse chilling effects of surveillance in Zimbabwe. *Big Data & Society*, *10*(1), 1–14. https://doi.org/10.1177/20539517231158631

Stoltzfus, J. C. (2011). Logistic Regression: A Brief Primer. *Academic Emergency Medicine*, *18*(10), 1099–1104. https://doi.org/10.1111/j.1553-2712.2011.01185.x

Stremlau, N. (2025). Internet Shutdowns, Sovereignty, and the Postcolonial State in Africa. *Global Policy*, *16*(2), 372–379. https://doi.org/10.1111/1758-5899.13483

Stremlau, N., & Dobson, N. (2022). Information Controls and Internet Shutdowns in African Elections. *Journal of African Elections*, *21*(2), 1–22. https://doi.org/10.20940/JAE/2022/v21i2a1

Swamy, A. V., & Fikkert, B. (2002). Estimating the Contributions of Capital and Labor to GDP: An Instrumental Variable Approach. *Economic Development and Cultural Change*, *50*(3), 693–708. https://doi.org/10.1086/342250

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. https://doi.org/10.1016/j.egyr.2021.01.045

The Bloggers Association of Kenya. (2016). *State of the Internet in Kenya 2016*. https://www.yumpu.com/en/document/read/56450478/state-internet

The World Bank. (2016). *World Development Report: Digital Dividends*. https://www.worldbank.org/en/publication/wdr2016

The World Bank. (2024). *World Bank Country and Lending Groups*. https://datahelpdesk.worldbank.org/knowledgebase/articles/906519-world-bank-country-and-lending-groups

Thumfart, J. (2024). Digital Rights and the State of Exception. Internet Shutdowns from the Perspective of Just Securitization Theory. *Journal of Global Security Studies*, *9*(1). https://doi.org/10.1093/jogss/ogad024

Turianskyi, Y., & Wekesa, B. (2021). African digital diplomacy: Emergence, evolution, and the future. *South African Journal of International Affairs*, *28*(3), 341–359. https://doi.org/10.1080/10220461.2021.1954546

United Nations Development Programme. (2024). *Human Development Index (HDI)*. Human Development Reports. https://hdr.undp.org/data-center/human-development-index

Vuori, J. A. (2008). Illocutionary Logic and Strands of Securitization: Applying the Theory of Securitization to the Study of Non-Democratic Political Orders. *European Journal of International Relations*, *14*(1), 65–99. https://doi.org/10.1177/1354066107087767

Vuori, J. A., & Paltemaa, L. (2015). The Lexicon of Fear: Chinese Internet Control Practice in Sina Weibo Microblog Censorship. *Surveillance & Society*, *13*(3/4), 400–421. https://doi.org/10.24908/ss.v13i/4.5404

Wall, M., & Ward, M. (2017, May 18). WannaCry: What can you do to protect your business? *BBC News*. https://www.bbc.com/news/business-39947944

Witzleb, N., & Paterson, M. (2021). Micro-targeting in Political Campaigns: Political Promise and Democratic Risk. In U. Kohl & J. Eisler (Eds), *Data-Driven Personalisation in Markets, Politics and Law* (1st edn, pp. 223–240). Cambridge University Press. https://doi.org/10.1017/9781108891325.017

Zeadally, S. (2014). Special Issue on Cybersecurity, Cybercrime, Cyberwar. *Journal of Homeland Security and Emergency Management*, *11*(4), 459–461. https://doi.org/10.1515/jhsem-2014-1005