UNIVERSITY OF GHANA

COLLEGE OF HUMANITIES

THE CYBERSECURITY INSTRUMENTS AND POLICY FRAMEWORK OF GHANA'S ELECTORAL COMMISSION: A QUALITATIVE LONGITUDINAL STUDY

BY

DATSOMOR JOSEPH KWASHIE ANTHONY

(11366199)

THIS THESIS IS SUBMITTED TO THE UNIVERSITY OF GHANA, LEGON IN PARTIAL FULFILMENT OF THE REQUIREMENT FOR THE AWARD OF MASTER OF PHILOSOPHY IN POLITICAL SCIENCE

OCTOBER, 2025

DECLARATION

I, DATSOMOR JOSEPH KWASHIE ANTHONY, hereby solemnly declare that this thesis is entirely my original work carried out under the supervision of Dr. Nene-Lomotey Kuditchar and Dr. Isaac Owusu-Mensah. This work is unique and has not been submitted in whole or in part for a degree anywhere. All sources and references used in this thesis have been duly acknowledged and cited in the work.

..... 4th December, 2025.

DATSOMOR JOSEPH KWASHIE ANTHONY — DATE

Candidate

1st December 2025

....

DR. NENE-LOMOTEY KUDITCHAR — DATE

Lead supervisor

..... 4th December, 2025

PROF. ISAAC OWUSU-MENSAH — DATE

Co-supervisor

ABSTRACT

This study investigates the Cybersecurity Instruments and Policy Framework of Ghana's Electoral Commission (EC), tracing its evolution from 2012 to 2024. Employing a qualitative longitudinal design, the research explores how the EC has developed, implemented, and adapted cybersecurity measures to safeguard electoral integrity in the digital age. The study draws on in-depth interviews with officials from the EC, Cyber Security Authority (CSA), CERT-GH, civil society organizations, development partners, and election experts. It is guided by Joseph Nye's theory of power diffusion and Bruce Schneier's surveillance and trust framework, both of which illuminate how authority, control, and legitimacy operate within cyberspace and democratic institutions.

Findings reveal that Ghana's EC has moved progressively from ad hoc and reactive cybersecurity practices, seen during the 2012 and 2016 election cycles, to more structured and proactive frameworks by 2024, particularly after the passage of the Cybersecurity Act, 2020 (Act 1038). Despite significant improvements, including the introduction of biometric verification, encrypted data transmission, and inter-agency collaboration with CSA and CERT-GH, the study identifies gaps such as the EC's non-designation as a Critical Information Infrastructure (CII), limited independent audits, and insufficient year-round cyber readiness.

The research concludes that Ghana's electoral cybersecurity landscape remains dynamic, requiring continuous investment in technical tools, institutional coordination, and human capacity development. It recommends establishing a permanent Election Cybersecurity Unit, strengthening compliance with Act 1038, conducting regular penetration tests, and aligning EC practices with international standards such as ISO 27001. The study contributes to scholarship by providing the first longitudinal analysis of Ghana's electoral cybersecurity evolution and its implications for digital governance and democratic resilience.

DEDICATION

This work is dedicated first to the Almighty God, whose grace and mercy have sustained me throughout this academic journey.

To my parents, whose love, prayers, and sacrifices have shaped my life, especially to my late father, Mr. Anthony Kwashie Datsomor, whose memory continues to inspire me, and to my mother, Mrs. Vicentia Adzo Datsomor, for her unwavering support and encouragement.

The Xhosa/Zulu aphorism *umuntu ngumuntu ngabantu* (a person is a person through other people) beautifully reflects the spirit of gratitude and interconnectedness that I wish to honor here.

This achievement is as much yours as it is mine.

ACKNOWLEDGEMENT

"For I know the plans I have for you," declares the Lord, "plans to prosper you and not to harm you, plans to give you hope and a future." — Jeremiah 29:11

"Weeping may endure for a night, but joy comes in the morning." — Psalm 30:5

"Let us not become weary in doing good, for at the proper time we will reap a harvest if we do not give up." — Galatians 6:9

These verses have guided me through moments of uncertainty and perseverance, constantly reminding me that resilience, faith, and patience yield divine reward.

I express my deepest gratitude to my Principal Supervisor, Dr. Nene-Lomotey Kuditchar, who has been not only an exceptional academic guide but also a true mentor. His commitment, wisdom, and mentorship have gone far beyond scholarly supervision, shaping my professional, intellectual, and personal growth. I am sincerely grateful for his continued encouragement and belief in my abilities. My heartfelt appreciation also goes to my Co-Supervisor, Prof. Isaac Owusu-Mensah, for his invaluable insights, constructive feedback, and consistent guidance throughout this research journey.

I extend special thanks to Konrad Adenauer Stiftung (KAS) Ghana, Prof. Seidu Alidu Mahama, Prof Samuel K. Bonsu, Mr. Frederick Odartei Lamptey, Dr. Williams Kudzi, Grace Esinam Kpesese, Francis Kwesi Addo, Micheal Anyetei Ajei, Enoch Hudu, Nadia Gaddafi, Thompson Osei Akoto Addo, Sandra Senanu Adjetey, Anthony Grace, and Anthony William for their support, motivation, and contributions at different stages of my work.

To my dear friends, Amstrong Mubarack, Ramlah Arhinful, Isaac Kwartei Quartey, Bema Debora, Alex Quao, Akoto Michael, Bright Oduro, Darlington Rex Tettey, Judith Amoah-Mensah, and Nelson Quame, thank you for your companionship, intellectual exchanges, and unwavering support. You each played a vital role in making this journey fulfilling.

Finally, I thank the Almighty God once again for granting me strength, wisdom, and perseverance. May His name be forever praised.

LIST OF ABBREVIATIONS

BVR	Biometric Voter Registration
BVD	Biometric Verification Device
CERT-GH	Computer Emergency Response Team – Ghana
CII	Critical Information Infrastructure
CSA	Cyber Security Authority
EC	Electoral Commission
EU	European Union
ICT	Information and Communication Technology
IDS	Intrusion Detection System
ISO	International Organization for Standardization
MFA	Multi-Factor Authentication
NCA	National Communications Authority
NIST	National Institute of Standards and Technology
NIS	Network and Information Security
UNDP	United Nations Development Programme
USAID	United States Agency for International Development

TABLE OF CONTENTS

DECLARATION **1**

ABSTRACT **1**

DEDICATION **1**

ACKNOWLEDGEMENT **1**

LIST OF ABBREVIATIONS **1**

CHAPTER ONE: INTRODUCTION **1**

1.1 Background to the Study 1

1.2 Problem Statement 5

1.3 Research Objectives 8

1.4 Research Questions 9

1.5 Significance of the Study 9

1.6 Scope of the Study 12

1.7 Justification of the Study 14

1.8 Limitations of the Study 15

1.9 Organization of the Study 17

CHAPTER TWO: LITERATURE REVIEW **20**

2.1 Introduction 20

2.2 Conceptual and Theoretical Framework 21

2.2.1 Key Concepts.....21

2.2.2 Theoretical Lens and Foundation 24

2.3 Cybersecurity in Elections.....28

2.3.1 Increasing Vulnerabilities of Electoral Systems.....28

2.3.2 Adoption of Election Technology and Its Benefits 30

2.3.3 Unintended Consequences and Risks of Election Technology 32

2.3.4 Biometric Technology in Elections: Promise and Perils 34

2.3.4.1 Rationale for Biometric Systems in Elections 35

2.3.4.2 Challenges and Failures of Biometric Systems 36

2.3.5 Cybersecurity Vulnerabilities Across the Electoral Cycle 40

2.3.6 Threats to Electoral Integrity.....44

2.3.7 Global Trends and Lessons for Ghana 45

2.4 Cybersecurity Instruments and Tools.....47

2.4.1 Application of Cybersecurity Instruments in Elections.....51

2.4.2 Technical Tools and Policy Instruments of Ghana's EC.....54

2.4.3 Frameworks and Best Practices for Securing Elections 57

2.5 Ghana's Legal and Institutional Framework for Cybersecurity 65

2.5.1 Cybersecurity Act, 2020 (Act 1038) and the Cyber Security Authority (CSA).....66

2.5.2 Data Protection Act, 2012 (Act 843) and Personal Data Protection 68

2.5.3 Other Relevant Legislation and Institutions 69

2.6 Longitudinal Analysis of Ghana's EC 74

2.6.1 Why Longitudinal? 75

2.6.2 Methodological Insights 76

2.7 Gaps in the Literature 78

2.7.1 Instrument-Policy Disconnect 79

2.7.2 Longitudinal Blindspots 80

2.7.3 Stakeholder Dynamics and Institutional Roles 81

2.8 Summary 82

CHAPTER THREE: METHODOLOGY 83

3.1 Introduction 83

3.2 Research Philosophy and Approach 84

3.3 Research Design: Qualitative Longitudinal Study 85

3.4 Data Collection Methods 86

3.5 Data Analysis 87

3.6 Trustworthiness and Rigor 89

3.7 Ethical Considerations 90

3.8 Limitations of the Methodology 91

3.9 Summary 93

CHAPTER FOUR: FINDINGS, DISCUSSION, AND ANALYSIS 94

4.1 Introduction to Findings and Thematic Overview 94

4.2 Evolution of EC Cybersecurity Practices Across Electoral Cycles (2012–2024).....94

4.2.1 2012: Nascent Use of Technology and Minimal Cybersecurity Focus 94

4.2.2 2016: Wake-Up Call – Cyber Incident and Reactive Measures.....95

4.2.3 2020: Institutionalization – Legal Reforms and System Upgrades 97

4.2.4 2024: Consolidation of Practices and New Threat Landscapes 99

4.3 Thematic Analysis of Ghana's Electoral Cybersecurity Posture 102

4.3.1 Cybersecurity Tools, Measures, and Practices Implemented.....102

4.3.2 Gaps and Ongoing Challenges in the EC's Cybersecurity Posture 105

4.3.3 Incident Response, Inter-Agency Collaboration, and Proactive vs. Reactive Approaches 111

4.3.4 Insider Threats and Internal Security Culture 115

4.3.5 Misinformation, Public Trust, and the Human Factor in Cybersecurity 118

4.4 Theoretical Reflections: Power Diffusion and Trust in Ghana's Electoral Cybersecurity 121

4.5 Preliminary Policy Insights and Conclusion of Findings.....131

CHAPTER FIVE: SUMMARY OF FINDINGS, CONCLUSIONS AND RECOMMENDATIONS.....135

5.1 Reiterating the Research Problem and Key Insights.....135

5.2 Contributions of the Study 136

5.3 Technical Recommendations 138

5.4 Policy Recommendations 141

5.5 Capacity-Building and Organizational Recommendations 146

5.6 Alignment with International Standards and Best Practices 150

5.7 Limitations of the Study 152

5.8 Suggestions for Future Research 154

5.9 Conclusion 156

REFERENCES **158**

APPENDICES **170**

CHAPTER ONE

INTRODUCTION

In today's digital age, the integrity of electoral processes is increasingly intertwined with cybersecurity resilience. Election management bodies globally are facing increasing levels of cyber threats, from voter database hacking attempts to disinformation campaigns, which can erode public trust and undermine democratic stability. Ghana's Electoral Commission (EC) is no different. The EC in the last decade has adopted technological innovations (including the biometric voter registration and electronic result transmission) to enhance the credibility of elections. But such technologies also open the voting process to fresh vulnerabilities that adversaries could exploit. During Nigeria's 2023 general elections, for example, nearly 13 million cyberattacks targeted at government systems, with threat traffic reaching 6.9 million attacks on the presidential election day alone (Izuaka, 2023). Although the Nigerian authorities were able to foil those attacks, this case underlines the magnitude of the cyber threats that face West African elections and the increasingly high stakes for Ghana. If a Ghanaian electoral infrastructure faced something similar, could our current cybersecurity framework survive it? The need to critically appraise Ghana's preparedness and to build the EC's guard against such threats is the underlying motivation for this study.

Ghana's national context presents a dual narrative of progress and persisting challenges in cybersecurity. On one hand, Ghana has emerged as a regional leader in cyber policy and capacity-building. The country climbed from 89th to 43rd globally in the International Telecommunication Union's Global Cybersecurity Index within three years, becoming one of only seven African nations in the top 50 (Africa Center for Strategic Studies, 2022). Ghana's government has enacted a comprehensive Cybersecurity Act (Act 1038 of 2020) and established a dedicated Cyber Security

Authority (CSA) to oversee critical information infrastructure protection, incident response (CERT-GH), and public awareness programs (Africa Center for Strategic Studies, 2022; Media Foundation for West Africa, 2022). These efforts indicate high-level recognition of cybersecurity as pivotal to national security and digital development.

On the other hand, there are still significant vulnerabilities. Ghanaian institutions are not immune to internal threats, capacity challenges, and poor policy enforcement. The vulnerability of the internal staff and personnel of a country's EC was illustrated by a recent breach from the EC itself: a staff member illegally moved the voter records, challenging access controls and resulting in the staff member's termination (Owusu-Darko, 2024). Not only did this compromise sensitive details about voters, it also served to erode public trust in the EC's digital systems – a demonstration of what a once-trusted insider with privileged access can do to undermine technical defences. Together, these illustrative incidents, from Nigeria's foiled cyber-attacks to the EC's internal breach, underscore the twin challenges of external threats and insider vulnerabilities, and they have been integrated here to strengthen the analytical argument rather than serve as stand-alone anecdotes.

These risks are heightened by a more general lack of capacity, with Ghana suffering a lack of dedicated staff and general resources that are common in many developing countries (E-Governance Knowledge Hub, 2023). In addition, weak enforcement of existing regulations can undermine the effectiveness of Ghana's cybersecurity framework. For instance, in spite of the passage of Act 1038, very little prosecution has occurred under this law, indicating disparity between law on paper and implementation practice (Media Foundation for West Africa, 2022). Where critical institutions are not submitting fully to security mandates, as seen in the EC's

hesitation to classify its system as Critical Information Infrastructure for independent audits (Owusu-Darko, 2024), vulnerabilities may persist unchecked.

From a theoretical standpoint, these are not isolated issues: they intersect with wider themes of cybersecurity, surveillance, and power. Bruce Schneier (2015) argues that we now "live in the golden age of surveillance", wherein governments and corporations possess unprecedented capabilities to monitor and collect data (Schneier, 2015). This mass surveillance ecosystem presents a complex trade-off between security and civil liberties, as those who control data gain significant power over society's safety and privacy. In the election domain, public institutions like the EC that facilitate surveillance and data collection must strike a balance on the use of surveillance and data collection (e.g., voter databases, biometric information) for security purposes with the protection of citizens' rights and trust. Excessive surveillance, or a data breach, could destroy public trust as much as inadequate security would. Meanwhile, Joseph Nye (2011) introduces the concept of cyber power – the ability of an actor to achieve preferred outcomes through the use of cyberspace – explaining how cyberspace has lowered the barrier of entry for a much broader group of actors to project power (Nye, 2011). In traditional domains, power belonged to nation-states, but in cyberspace, a single hacker or small band can shape national affairs. This diffusion of power also means that Ghana's electoral systems may come into the crosshairs not just of rival states or criminal organizations, but independent hacktivists or disgruntled insiders with the know-how to cause damage. Under Nye's paradigm, even a relatively small actor may use cyber tools to trouble a larger institution; thus, the EC's cyber posture is key to deterring and also mitigating asymmetric threats. The following theoretical considerations make it clear that a comprehensive cybersecurity framework for Ghana's EC is not only a technical

necessity but it is also a crucial matter of safeguarding democratic power and sovereignty in the information age.

Elections are the cornerstone of Ghana's democratic stability, and any breach of electoral IT systems – such as hacking of results transmission, tampering with the voter register, or hacking ransomware on the EC's databases – would have significant impacts. It could erode confidence in the outcomes of an election, foment political unrest, or destabilize the hard-earned democratic institutions on which this country is based. Notwithstanding the high stakes, there is limited academic study focusing on Ghana's electoral cybersecurity framework over time. Many studies and reports on cybersecurity in African elections are cross-sectional, with some others presenting Nigeria as a more acute case study (Izuaka, 2023; E-Governance Knowledge Hub, 2023). Ghana-specific literature often highlights general cybercrime trends or national strategy developments (Africa Center for Strategic Studies, 2022; Media Foundation for West Africa, 2022), but what remains underexplored is the scope of change within the EC's own policy and securitization practices over time, and to what extent these have changed in unison with contemporary threats. In other words, we know that threats are increasing and that Ghana has enacted laws and created agencies, but it is not well documented how these translate into improved security for the electoral commission in practice. Fundamental issues remain: Are the EC's cybersecurity policies proactive or merely reactive? Have past incidents or near-misses prompted meaningful policy changes? Is there an effective enforcement mechanism to ensure compliance with cybersecurity standards within the EC? Without answers to these questions, policymakers and stakeholders lack a clear understanding of the EC's preparedness and what additional tools or reforms might be needed.

This thesis addresses this gap by conducting a qualitative longitudinal research on the cybersecurity tools and policy framework of Ghana's Electoral Commission. Through an analysis

covering the introduction of major IT initiatives in the electoral process (biometric registration in 2012, electronic result transmission pilots, etc.) to the present day, the study will examine how the EC's cybersecurity posture has changed over time, identify the drivers of those changes (such as incidents, shifts in the threat environment, legal and institutional reforms), and evaluate the effectiveness of current measures in mitigating risks. In adopting a longitudinal perspective, the study reaches beyond the snapshot to reveal trends, patterns, and lessons that can be learned across several election cycles. The result will not only serve as a diagnosis of the present state of strengths and weaknesses of the EC's cybersecurity framework, but also as a set of recommendations (benchmarked against global best practice) based on evidence that the EC should implement in order to secure Ghana's electoral systems into the future. At bottom, the research provides a problem-solution map: it recites the cybersecurity challenges faced by Ghana's EC, explains why those challenges are problematic and what has been done to date, and suggests how the deficiencies identified could be remedied through policy and institutional changes.

1.2 Problem Statement

The introduction of digital technologies into democratic systems has significantly enhanced the efficiency and trustworthiness of the electoral processes. However, it has raised concerns about cybersecurity vulnerabilities that could imperil the integrity of elections. Around the world, voter systems are increasingly the targets of cyberattacks, including data breaches, ransomware, disinformation campaigns, and efforts to sabotage infrastructure. Unmitigated, these cyber threats could compromise confidence in the veracity of an election's outcome, delegitimize democratic institutions, and compromise national security (Brown et al., 2020; Bund, 2016; Garnett & James, 2020). Within this narrative, Ghana's EC, the institution responsible for conducting and

supervising elections, is caught at the heart of a looming cybersecurity conundrum: with the EC increasingly relying on digital technology for voter register management, voter verification, and results transmission, it is increasingly exposed to cyber risks that demand an adequate and tailored cybersecurity response. Yet, a major gap remains in our understanding; no comprehensive longitudinal analysis has yet examined how Ghana's EC has adapted its cybersecurity measures over successive election cycles. This study is motivated by the gap.

Despite significant efforts to bolster its national cybersecurity system (in particular, the Cybersecurity Act (2020) and the Cyber Security Authority (CSA)), this capacity has not been fully absorbed into the operational architecture of the EC. A significant divide can still be observed in national cybersecurity guidelines and the translation of the same into practice in the Commission's election systems. This discrepancy is evidenced by a number of issues, including a lack of in-house technical expertise in the EC, a lack of cybersecurity training for staff, uneven policy enforcement, and no formal designation of the EC's digital assets as critical national infrastructure. These weaknesses had been demonstrated in events such as the insider access to the voter register (Owusu-Darko, 2024), which revealed weaknesses in internal access controls and data protection protocols. These aren't just alarming in the way they expose sensitive voter information, but also in that they highlight the bigger questions around the EC's capacity to safeguard it against more advanced, external cyber threats. It should be noted that the scope of this study is focused on the EC's policy evolution and institutional practices in cybersecurity, rather than on technical penetration systems or other purely technical audits; in other words, the research concentrates on organizational and policy dimensions of cybersecurity and explicitly leaves detailed system security testing outside its purview.

The use of biometric technologies in Ghana's electoral processes further complicates this issue. Biometric voting systems have immensely enhanced the integrity of elections since they were introduced due to their capabilities of accurately identifying voters and minimising multiple voting and impersonation (Dorpenyo, 2020). However, despite the agreement over the operational advantages of BVR systems, academic and policy literature has paid little attention to the essential cybersecurity risks involved in storing, communicating, and securing biometric information. For instance, research by Jacobsen (2020), Debrah et al. (2019), and Wolf et al. (2017) assesses the effectiveness and limitations of biometric technologies in elections but gives little consideration to the threats of cyber attacks and hacking, data theft, and technological sabotage. The omission of cybersecurity as part of discussions around the biometric systems is a dangerous blind spot, particularly as Ghana increasingly depends more on digital electoral infrastructure.

Broader international studies and cybersecurity guidelines do not address the unique Ghanaian context. While frameworks provided by institutions such as the National Institute of Standards and Technology (NIST, 2021), USAID (2019), and Van der Staak and Wolf (2019) emphasize best practices for securing electoral technologies, they tend to focus on generalized approaches or case studies from countries with different political, technological, and institutional conditions. As a result, there is scant scholarly information on how such frameworks can be customized to suit the peculiarities of Ghana, particularly in the case of biometric systems, and on the capacity of the EC to effectively put into action these structures.

Against this backdrop, a critical gap exists in the academic and policy literature concerning how the EC's cybersecurity instruments and policies have metamorphosed over the course of time in reaction to Ghana's dynamic cyber threat environment. Cyber-threats continue to evolve, with a growing number of attacks being perpetrated against electoral systems in West Africa and around

the world; it is imperative that the cybersecurity response is dynamic. However, little is known about the pathway of Ghana's efforts in cybersecurity, especially in the area of the electoral process, how far the instruments of the efforts are currently in place, and what the constraints are to their full implementation.

This study seeks to address this knowledge gap by conducting a comprehensive, longitudinal analysis of the cybersecurity instruments and policy frameworks adopted by Ghana's Electoral Commission. It will analyse the development of such measures in the face of new threats, their effectiveness in securing biometric and other digital electoral technologies, and the institutional and operational obstacles that mitigate against their successful implementation. In so doing, the study seeks to add to the growing literature on electoral cybersecurity in young democracies, with a view to generating lessons to underpin policy reform and institutional capacity building toward safeguarding the integrity of Ghana's democratic processes in the digital age.

1.3 Research Objectives

1. To analyze the evolution of the Electoral Commission's cybersecurity framework in response to emerging digital threats across key electoral cycles (2012-2024) and the drivers of policy change in the EC's cybersecurity framework, determining why and how changes were made.

2. To evaluate the effectiveness of cybersecurity policies and instruments implemented by the Electoral Commission in safeguarding electoral integrity.

3. To identify gaps, challenges, and areas for improvement in the EC's cybersecurity framework and to formulate actionable recommendations or best practices to address these gaps.

1.4 Research Questions

1. How has the Electoral Commission's cybersecurity framework adapted to emerging threats over time (2012-2024), and what factors have driven these changes or updates in the EC's cybersecurity framework?

2. What specific cybersecurity policies and instruments has the Electoral Commission employed to mitigate risks, and how effective have they been in ensuring electoral security?

3. What gaps or weaknesses remain in the EC's cybersecurity framework, and what best practices or recommendations can address these gaps to enhance election security in Ghana?

1.5 Significance of the Study

This research is significant at several levels: national, regional, and global. It addresses the national security of Ghana's electoral process, which is key to the democratic stability of the country. Ghana has developed a reputation for being one of Africa's most stable democracies and has frequently overseen peaceful transfers of power and maintained civil liberties. Accordingly, election integrity isn't simply a technical challenge; it's a foundational aspect of sustaining public confidence in governance. A successful cyberattack on election infrastructure has the potential to undo years of democratic consolidation. Through pointing out the deficiencies and suggesting enhancements, this study adds to the strengthening of an essential building block of the Ghanaian democracy. It offers evidence-based insights that can inform policymakers (at the EC, CSA, and beyond) as they develop strategies to prevent election disruptions. The study also holds the EC

accountable to its mandate of delivering free and fair elections in the modern era, where "free and fair" implicitly requires secure digital systems. In practical terms, if the recommendations made in this thesis are adopted, then key events such as unauthorized access to the voter register and vote result tampering (an event that has untold but grave political and social effects) could be averted.

On the regional level, Ghana has taken a proactive position on safeguarding cybersecurity in West Africa, and its posture is thus frequently seen as an example by other states in the neighborhood (Africa Center for Strategic Studies, 2022). West Africa's security and political stability are interconnected; challenges in one country can spill over to others. Not only can Ghana set a good example for how to secure elections through best practice, but it can also help the region to learn from its successes and mistakes through mechanisms and organizations such as ECOWAS and the African Union. For instance, the Ghana model of creating a Cyber Security Authority and domesticating international cybercrime conventions (in Budapest and Malabo) (Africa Center for Strategic Studies, 2022) has become a model for emulation by other countries. By focusing on the electoral sphere, this study addresses a particularly sensitive and high-impact domain of cybersecurity. The results could help shape not just Ghana's domestic policy, but also regional election missions as well as the electoral-support efforts that increasingly incorporate a cybersecurity component. Furthermore, the insights gained from Ghana's achievements or failings can help countries like Liberia, Sierra Leone, or Nigeria as they seek to invest in safeguarding their election technologies. In an era where cyber threats cut across national borders, strengthening Ghana's defenses does not simply make the cyber ecosystem more secure for Ghana — it makes it more secure regionally, as adversaries commonly target more than one state in the same fashion.

At the global level, this study contributes to a burgeoning literature on election cybersecurity and governance in new democracies. Most of the literature about election cybersecurity thus far has

focused on developed countries or high-profile events (like Russian meddling in the 2016 U.S. elections or the hacking of European election systems). By focusing on Ghana, which is a low-middle-income country with a good democratic reputation, the paper offers a view from the Global South, which is less represented in the academic output. It shows the unique challenges developing democracies face – including resource limitations, balancing foreign aid with local ownership, and incorporating cybersecurity in institutions that may be reforming or professionalizing – building a more diverse global knowledge about how to secure elections. The merging of theoretical insights from Schneier and Nye also infers a degree of theoretical independent contribution, showing what surveillance and cyber power theories look like when they play out on the ground. For example, the situation in Ghana may illustrate how power in cyberspace is not only about offensive capabilities but also about resilience – the ability of a state to withstand and recover from cyberattacks can be seen as a form of defensive power crucial for sovereignty. Lastly, the study's research-based recommendations (including better insider threat management, capacity building programmes, multi-agency cooperation, and more) could be used as a best practice case for international organisations and election support NGOs running on cybersecurity. Organizations that commonly play a role in supporting election processes around the world, such as the International Foundation for Electoral Systems (IFES) and the United Nations Development Programme (UNDP), among others, might consider learning from these findings to help design better interventions in countries like Ghana. Put simply, the implications of this study go beyond the academic research and have real-world implications for election security, regional policy harmonisation in cybersecurity, and global conversations about how to safeguard democracy in a digital age.

1.6 Scope of the Study

This research is focused on the cybersecurity instruments and policy framework of Ghana's Electoral Commission, with an emphasis on a longitudinal analysis covering approximately the last decade (2012–2024). The scope is delineated as follows:

Institutional Focus: The primary focus is on the Ghana Electoral Commission as an institution. This includes the EC's internal policies (such as security protocols, strategic plans, and standard operating procedures for IT systems), its technology infrastructure related to elections (voter registration systems, biometric verification devices, results transmission systems, databases and networks used by the EC), and its interactions with other national cybersecurity bodies (notably the Cyber Security Authority, National Cyber Security Centre/CERT, and security agencies). The study does not directly assess other institutions, except in how they interface with or support the EC (for instance, the role of the CSA in auditing EC systems, or the Ministry of Communications in policy formulation).

Thematic Coverage: The research encompasses cybersecurity measures in a broad sense – including technical, administrative, legal, and human resource aspects. For example, technical instruments might involve firewalls, encryption, intrusion detection systems used by the EC; administrative measures might include policies for user access control, incident reporting procedures, and data backup protocols; legal/policy instruments cover relevant laws (e.g., Act 1038, Data Protection Act 2012) and official guidelines that govern the EC's cybersecurity; and human factors include training programs for EC staff, awareness of cybersecurity among election officials, and vetting of personnel to prevent insider threats. While the study will touch on cyber threats and incidents (malware, hacking, disinformation, etc.), it will do so in service of evaluating

the EC's preparedness and response – a detailed technical forensic analysis of any particular attack is outside the scope.

Geographic and Comparative Scope: Geographically, the study is centered on Ghana. Comparisons with other countries (such as Nigeria's cyberattack figures or best practices in advanced democracies) will be included to contextualize Ghana's situation and to benchmark performance, but they are not the primary object of analysis. The study does not, for instance, provide a full comparative case study of another country's electoral cybersecurity; rather, it selectively uses external reference points to assess what Ghana is doing well or could improve. The regional and global comparisons serve as a backdrop to highlight Ghana's unique challenges (like resource constraints) and opportunities (like regional leadership in cybersecurity).

Temporal Scope: The term "longitudinal" signifies that the research will examine changes over time rather than a single moment. The starting point of 2012 is chosen because it marks the introduction of biometric voter registration and verification in Ghana's elections – a major technological shift that brought cybersecurity to the fore of election management. From 2012 onward, Ghana has held multiple general elections (2012, 2016, 2020) and other polls, providing several points in time to observe developments. The study will track the timeline of policy rollouts and incidents through these election cycles up to the present day (2024). However, it is not a month-by-month chronicle; rather, it will focus on key milestones (for instance, the adoption of a new election management system, the passage of key legislation, notable cyber incidents around election periods, etc.). The cutoff for analysis will be mid-2024, aligning with the most recent data and developments available at the time of writing.

Limitations of Scope: It is important to note what the study does not cover. Content moderation and online misinformation on social media, while related to election cybersecurity, are not a

primary focus here except insofar as the EC has specific policies on them. The study remains centered on the security of the EC's own systems and data, rather than the broader information ecosystem (which might involve social media companies, media houses, etc.). Additionally, physical security of election materials (like ballot papers or voting machines) is outside the cyber scope except where a clear cyber-physical link exists (e.g., tampering with a biometric device's software). Finally, while the research will inevitably discuss cyberattacks and threat actors, it will not delve into intelligence attributions or detailed hacker profiles; those are beyond the scope and often classified. Instead, the emphasis is on whether the EC's instruments are robust against generic categories of threats (insider, outsider, malware, etc.) that we know from global trends.

1.7 Justification of the Study

Ghana has long been regarded as a beacon of democratic stability in West Africa, with a history of peaceful elections and constitutional governance. Yet that reputation is being challenged, as other malicious actors become more sophisticated and brazen in their attacks on election systems across the globe. Biometric verification systems implemented by the EC have increased electoral transparency and decreased electoral fraud (Brown et al., 2020; Bund, 2016; Garnett & James, 2020), but have also made the system more vulnerable in a cybersecurity context. With digital infrastructure playing a central role in the electoral process, the protection of this infrastructure is important not only for the credibility of the democratic process in Ghana but also for stability in a sub-region with a history of political instability.

This research is justified for numerous reasons. Firstly, it fills a notable gap in the academic literature by moving away from the electoral technologies' operational performance to the specific

cybersecurity policies and instruments that govern their use. Secondly, Ghana presents a compelling case study due to its dual identity as both a democratic frontrunner and a digitalizing electoral environment in a region experiencing increased cyber-insecurity and authoritarian pushback. Thirdly, the study is in line with international and national policy directions, such as Ghana's Cybersecurity Act (2020), which aims to provide a holistic approach for the protection of national digital assets, including those accessed for elections.

Moreover, given Ghana's influence on regional political trends, the efficacy—or failure—of its electoral cybersecurity measures could have a spillover effect across West Africa. With other ECOWAS states beginning to adopt electronic electoral technologies for elections, Ghana's experience could be emulated (or repudiated) by those who follow suit. The findings from this qualitative longitudinal study will, therefore, not only be useful for policy making in Ghana but also perhaps for a larger knowledge base related to electoral cybersecurity policy in emerging democracies. By mapping systemic strengths and institutional weaknesses and capacity-building needs, this study will inform practical, policy-relevant recommendations to those stakeholders interested in ensuring future electoral integrity.

1.8 Limitations of the Study

Although this research seeks to contribute to an in-depth understanding of the electoral cybersecurity profile of Ghana, it comes with some limitations. First, sensitive or confidential information with respect to the EC's cybersecurity infrastructure may be limited on the basis of national security directives and institutional secrecy. This has the potential to limit the depth of analysis in regions where transparency is limited.

Second, the rising threat landscape and fast pace of technology changes impose a methodological constraint. Some implications, especially those involving threat typologies and policy responses, could be outdated soon with the appearance of other risks and mitigation strategies. While the longitudinal approach is beneficial for trend analysis, the constantly moving inches landscape presents a risk to up-to-the-moment relevance.

Third, because of lack of human resources and time, primary data collection may have been insufficiently extensive. Individual interviews, focus group discussions, and institutional visits could be constrained by respondent availability, institutional red tape, and logistical barriers. These limitations may influence the quality of qualitative data elicited during the fieldwork stage.

In addition, while ethical protocols will be strictly followed—including informed consent, data anonymization, and secure handling of interview transcripts—the study must also grapple with the ethical complexity of dealing with potentially sensitive information. There is a risk of inadvertently disclosing vulnerabilities or institutional weaknesses that could be exploited if not handled with discretion. Thus, extra caution will be taken in data presentation and interpretation to ensure the security of institutional data and the protection of participants.

Lastly, the focus of this study on the isolated case of Ghana may constrain broader generalizations to other countries with varying political, technological, and institutional dynamics. While the study will incorporate comparative references, its primary contribution lies in deepening the understanding of Ghana's unique electoral cybersecurity ecosystem.

1.9 Organization of the Study

This thesis is arranged into five major chapters, covering step by step the essential elements related directly to the research questions, building a coherent narrative from the identification of the problem to the proposed solution.

Chapter One: Introduction

This chapter outlines the research area, including the context of the study, presents a detailed contextual background on the current challenges to cybersecurity faced by the Electoral Commission of Ghana, and highlights the gaps in existing literature. It explicates the research problem and question, presents the aims and objectives of the study, provides justification for the study, and delimits the scope and theoretical focus of the investigation. In this way, the first chapter provides a frame in regard to which this study can be understood, and what it will explore and why.

Chapter Two: Literature Review

This chapter reviews relevant literature to understand the cybersecurity measures, as well as policy and regulatory frameworks of the Ghanaian EC from the 2012 to 2024 election cycles. The literature review is systematically organized according to the research aims: the conceptual and theoretical foundation of the study, international and national threats to electoral cybersecurity, technical and policy responses, national and EC-level frameworks, and the importance of a longitudinal perspective. This chapter ends by considering the research gap and situating the research within the wider field of today's research culture.

Chapter Three: Research Methodology

This chapter describes the approach used to study the development of cybersecurity tools and legislative policies in the context of the Ghanaian Electoral Commission (EC). The study employs a qualitative longitudinal approach to understand the reactions of EC to new forms of cyber threats and how the EC has altered its institutional practices across four pivotal election cycles: 2012, 2016, 2020, and 2024. The chapter presents the philosophical stance, research design, research approach, data collection modes, data analysis methods, strategies applied to ensure confidentiality and anonymity, and the limitations of the method, which all contributed to the trustworthiness of the study. Issues of validity, reliability, and ethics are also confronted in this chapter.

Chapter 4: Findings, Discussion, and Analysis

In this chapter, the empirical findings of the study are reported with the Research Questions, and may be presented either chronologically or thematically. It could start with the level of cybersecurity when biometric elections were introduced in 2012 and follow through the 2016 and 2020 elections to the present (2024). This chapter evaluates cybersecurity practices and tools in place and areas of greatest variance and best practice. It then critically discusses these findings in light of relevant theories, such as Nye's power diffusion and Schneier's trust and oversight, and analyses in which ways Ghana's EC adheres to, or diverges from them. The discussion also considers the implications of insider threats, reactive versus proactive policy approaches, and preparedness for the 2024 general elections. Practical, prioritized policy recommendations are introduced, including proposals such as establishing a permanent EC cybersecurity unit or a multi-agency Election Cybersecurity Task Force.

Chapter Five: Conclusion and Recommendations

This final chapter synthesizes the entire study, reiterating the research problem and summarizing key findings and their implications. It emphasises the contribution that the study makes to scholarly understanding and the conduct of elections in Ghana. Recommendations are outlined in a structured manner — technical, policy, and capacity building. Items such as regular penetration testing of our EC systems, updating EC's cybersecurity policy to incorporate the provisions of Act 1038, and the implementation of cybersecurity training and crisis table top exercises. To the extent possible, recommendations refer to international standards and best practice guidelines such as ISO 27001. The chapter also highlights the limitations of the research (that is, lack of access to highly sensitive material, dynamic cyber threat environment) and future research directions. These might involve comparative analysis, mathematical modeling of electoral security risks, or examination of public trust and perception in electoral cybersecurity. In summary, the thesis underlines that election cybersecurity is a dynamic endeavour that demands persistent attention, innovation, and partnership.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

This chapter reviews relevant literature to understand the cybersecurity measures, as well as policy and regulatory frameworks of the Ghanaian EC from the 2012 to 2024 election cycles. The literature review is organized based on the study's aims, including the conceptual and theoretical foundation, threats to electoral cybersecurity, technical and policy responses, and institutional frameworks at national and EC levels.

The chapter begins by outlining fundamental ideas and theoretical frameworks, then moves on to analyze global and national cybersecurity threats to elections, technical and policy responses, and Ghana's institutional cybersecurity frameworks. Key cybersecurity threats to electoral processes – from hacking of systems to disinformation campaigns – are outlined, drawing on both international cases and the Ghanaian context.

The chapter then explores established frameworks and best practices for securing election infrastructure, including risk management approaches and interagency collaboration models. Special attention is given to biometric voter registration and verification systems, as these have been central to recent elections in Ghana and other countries. Ghana's legal and institutional measures for cybersecurity, such as the Cybersecurity Act 2020 and the role of the Cyber Security Authority, are analyzed to understand the national readiness to protect electoral processes. Throughout the chapter, technical terms are explained for clarity. Each section is linked back to the research questions and methodology – highlighting how existing studies inform the current

research and where gaps remain. This approach ensures that the literature review not only summarizes prior work but also establishes the relevance and foundation for the present study's goals.

This chapter concludes by emphasizing the relevance of a longitudinal perspective in studying cybersecurity changes across numerous electoral cycles, as well as identifying research gaps and positioning the research within the larger field of current academic discourse.

By the end of the chapter, the reader will have a comprehensive understanding of the opportunities and threats of election technology, the cybersecurity challenges in safeguarding electoral integrity, and the specific context of Ghana's efforts and experiences. This sets the stage for identifying how this research will build upon and contribute to the existing knowledge.

2.2 Conceptual and Theoretical Framework

2.2.1 Key Concepts

Cybersecurity

Cybersecurity encompasses a wide range of technical, organizational, and governance challenges that must be addressed to safeguard an information system from both unintentional and deliberate assaults. It goes far beyond the specifics of firewalls, anti-virus software, and other technological security measures (Brown et al., 2020). Cybersecurity, in essence, strives to ensure that information systems maintain their integrity, confidentiality, and availability against both intentional attacks and unintentional failures. Cybersecurity focuses on protecting digital infrastructure, public trust in democratic processes, and data integrity in the context of elections.

The International Telecommunication Union (ITU) frequently used definition captures this breadth by noting that cybersecurity encompasses not only technical solutions but also training, best practices, and risk management actions to secure connected devices, personnel, and information in cyberspace (Brown et al., 2020).

Cybersecurity Instruments

Cybersecurity Instruments are the administrative systems and technical tools to prevent, identify, and respond to cyber threats. These consist of policy frameworks and concrete technologies. For instance, in election contexts, they include formal regulatory measures, incident response mechanisms, biometric voter registration (BVR) systems, encryption techniques, intrusion detection systems, and firewalls (Mohan et al., 2023; IFES, 2023c; Nobles, 2024; IFES, 2023a; IFES, 2023b). Such tools and procedures together enable election management bodies to strengthen their systems against attacks and to react swiftly when incidents occur.

Electoral Cybersecurity

Electoral Cybersecurity refers to protecting the digital systems and data involved specifically in electoral processes, such as voter registration databases, voting machines or software, results transmission networks, and public communication channels. This subfield is particularly concerned with protecting the digital systems and data involved in electoral processes, including voter registration, election results transmission, and public communication. In Ghana, this includes specific efforts to protect the biometric voter registration data, to preserve the credibility of the electronic result transmission system, and to prevent online disinformation campaigns that would jeopardize public trust (Amoah, 2020; Dorpenyo, 2019; Gadasu, 2023). Electoral cybersecurity,

by focusing on election-specific weaknesses, aims to secure the operational aspects of voting and the legitimacy of the electoral outcomes.

Policy Frameworks

Policy frameworks refer to the laws, institutional protocols, and international principles that govern cybersecurity practices. These are frameworks defined with a set of standards, roles, and responsibilities for ensuring cyber-resilience on a national and organizational level. The Ghanaian cybersecurity policy framework, as follows, comprises the Cybersecurity Act, 2020, the National Cybersecurity Policy and Strategy (NCPS), and the Electoral Commission's internal guidelines and standard operating procedures for secure elections (Government of Ghana, 2020). They offer an organizational blueprint within which the EC can work, with the advantage that cyber protections are bound to national laws and international best practices.

Qualitative Longitudinal Research

Qualitative longitudinal (QL) research is an approach to studying the dynamic nature of people's lives through marrying qualitative enquiry with longitudinal inquiry. As Neale (2019) describes, QL research tracks individuals or small collectives in "real time" to document change and continuity as they unfold. It possesses the capacity to delve into dynamic social processes at the qualitative level, to learn how people frame and construct their ongoing experiences.

One of the strengths of QL research is not only its use of time as a methodological tool but also the engagement with time as a theoretical construct. QL research "looks beyond static representations of social life" by focusing on "thinking dynamically" about paths into and through social experiences, according to Neale (Neale, 2019). This approach enables researchers to analyze

how agency and structure interweave over time, providing a greater sense of lived experience than conventional cross-sectional studies.

Moreover, unlike quantitative longitudinal studies, QL research is more focused and emphasizes depth instead of breadth. Whereas large-scale quantitative studies can map wide social patterns, QL research takes a more multi-faceted view by exploring how individuals make sense of and manage change (Neale, 2019). It is often generated through recursive interviewing and/or extended fieldwork and/or longitudinal ethnographic methods to get at the complexity of social life in motion over time.

QL is now a well-established methodological framework for the study of social change, life-course processes, and policy impacts. Thus, with its interplay of temporal and qualitative dimensions, it offers a novel means of examining how lives are influenced by wider societal currents as well as by individual decision-making (Neale, 2019). A qualitative longitudinal methodology is used in this thesis to map the changing cybersecurity posture of the EC in electoral cycles from 2012 to 2024, thereby capturing changes in policies, practices, and perceptions over an extended period.

2.2.2 Theoretical Lens and Foundation

Three primary theoretical perspectives have informed this research: Institutional Theory, Street-Level Bureaucracy, and the Confidentiality, Integrity, and Availability (CIA) Triad. Each theory provides a different, but complementary, lens through which to appreciate how Ghana's EC enacts, implements, and adapts its cybersecurity policy and tools over time.

Institutional Theory

Institutional theory is used to examine how the EC has responded to national and international cybersecurity norms over time. The adoption of cybersecurity policies can be better understood by looking at the EC's organizational culture, routines, and norms through the eyes of institutional theory. Further, institutional theory draws attention to the way historical trajectories and external pressures shape organizational response. The institutional perspective in this analysis helps to understand how EC's past decisions lead to path dependencies and how norms from the wider environment (national laws, international best practices) exert pressure through institutional isomorphism. This perspective is employed to determine the extent to which the EC has adjusted its cybersecurity practices in response to changing national and international expectations over time (Adu-Amanfoh & Allen, 2023; Hsu, Lee, & Straub, 2012; Kolog & Tijani, 2023). Through appreciating these institutional pressures, insights are gained into how some cybersecurity practices are adopted or neglected within the EC's operations. This theory lends direct support to Research Objective 1 (RO1), which examines the evolution and dynamics of change of the EC's cybersecurity framework between 2012 and 2024.

The Theory of Street-Level Bureaucracy

The theory of Street-Level Bureaucracy (Lipsky, 1980) will be utilized to make sense of how frontline implementers within the EC interpret and enact cybersecurity policy. The theory of street-level bureaucracy centers on the judgment and discretion of public servants who carry out policy implementation. By using this lens, it becomes easier to understand the decisions and actions made by the EC's election officers and IT personnel daily as they operationalize cybersecurity tools and procedures. These people frequently have to make snap decisions that have a big impact on cybersecurity results while interpreting high-level regulations under practical constraints. By

utilizing Lipsky's approach, the study can investigate how resource constraints, subjective assessments, and interactions at the "street-level" of the EC affect the efficacy of cybersecurity measures. Research Objective 2, which assesses the effectiveness of cybersecurity tools from the perspective of individuals who use them directly, is especially pertinent to this theory.

The Confidentiality, Integrity, and Availability (CIA) Triad

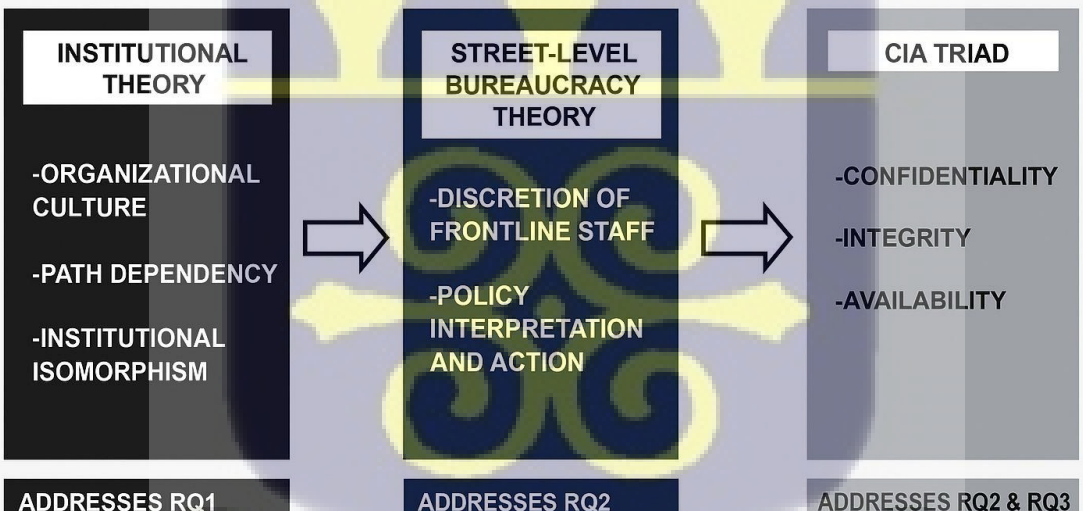
The CIA model provides a structured approach to assessing how the EC safeguards voter data, ensures accurate results transmission, and maintains system availability during elections. It is a fundamental model in the field of cybersecurity that offers a technical framework for assessing the security of election systems. This framework is implemented in the context of the Ghanaian election to guarantee a well-organized analysis of EC's cybersecurity position. Confidentiality encompasses securing sensitive election data (such as biometric voter information) from leaks or unauthorized access; integrity encompasses securing the accuracy and trustworthiness of election results transmission and verification processes; and availability involves the protection and availability of critical election systems (voter registration databases, result transmission networks and so on) remain functional and accessible when required, predominantly during the election day (Effah & Debrah, 2018; Owusu-Oware & Effah, 2022). By looking at measures in such dimensions, the CIA triad addresses core objectives of electoral cybersecurity: confidentiality, integrity, and availability. This framework, therefore, supplements the institutional and behavioral theories by concentrating on the technical requirements for a secure election process.

Each theory offers an individual yet complementary perspective to understand how Ghana's EC engages, enacts, implements, and evolves its cybersecurity policy and tools over time. Combining these three theoretical approaches guides the analysis of the Ghanaian EC in this study. They enable a multi-level approach to the problem: institutional theory offers a macro-level view of

norms and structures, street-level bureaucracy provides a micro-level view of the implementation, and the CIA triad offers a technical criterion-based view of security. This triangulated theoretical foundation is innovative and comprehensive, covering both socio-institutional dynamics and technical security principles. The relationship among these theories is explained in the text and illustrated in a conceptual diagram (Figure 2.1). For clarity, the CIA triad is being used as an evaluative tool for assessing technical security aspects (confidentiality, integrity, availability), rather than as a standalone social theory.

(To illustrate their inter-relationship in a conceptual diagram, refer to Figure 2.1, visualizing how the three structures guide the research.)

FIGURE 2.1



2.3 Cybersecurity in Elections

The increasing digitalization of electoral processes has introduced new vulnerabilities, particularly in regions with emerging cybersecurity frameworks like Ghana. As elections introduce digital technologies into their composition, these systems demand a solid cybersecurity infrastructure to maintain the integrity of elections. Technologies such as biometric verification and electronic transmission are now common but come with the risks of hacking, data breaches, and misinformation. Like the Philippines and Canada, Ghana faces similar risks, including data breaches and misinformation campaigns, but with unique institutional and contextual challenges.

2.3.1 Increasing Vulnerabilities of Electoral Systems

The growing dependence on digital technologies for conducting elections around the world has created significant vulnerabilities that could be leveraged to undermine the electoral process (Brown et al., 2020). In 2016, for instance, the Philippines' Commission on Elections had a big data breach that put the personal information of more than 55 million registered voters at risk (McDermott, 2017). Also, from 2015 to 2018, Canada's Communications Security Establishment observed more than twice as many digital attacks on democratic processes globally and a threefold rise in Organisation for Economic Co-operation and Development (OECD) nations. Sophisticated state intelligence organizations, "hackers for hire," and crime gangs aiming for ransoms have all perpetrated these attacks on companies (as experienced by one Caribbean EMB, which had to pay a bitcoin ransom to recover access to its data) (Brown et al., 2020).

According to Cheng et al. (2018), the global practice of election interference has emerged, whereby foreign and domestic actors exploit the same cyber vulnerabilities to manipulate public discourse

and interfere with electoral processes. The tampering of election infrastructure has manifested in multiple high-profile countries (especially the United States, France, and Ukraine) with attempts to hack into voter registration databases, adjust vote-tallying systems, or leak sensitive political information (Cheng et al., 2018).

While these global trends highlight the growing threat of cyberattacks, African countries like Ghana face additional challenges due to limited technical infrastructure and institutional capacity. Most African countries are adopting the biometric system for voter registration to curb the problem of electoral fraud. For example, over 25% of African nations have already implemented Biometric Voter Registration (BVR) systems, which typically use unique physical features, such as fingerprints and facial patterns, to verify the identity of voters (IFES, 2023c; Dorpenyo, 2019). These practices have been employed in a number of African countries in order to improve the accuracy of voter registries and to address challenges such as double registration and multiple voting (Dorpenyo, 2019).

While the situation has improved, biometric voting technology has significant challenges (IFES, 2021). Studies posit that their effectiveness can be affected by environmental conditions; for instance, heat could reduce the ability for biometric machines to effectively read fingerprints and thus deny eligible voters the ability to cast their votes if the biometric data is unreadable, as seen in elections in Ghana (Dorpenyo, 2019). Moreover, systems can have trouble correctly reading the fingerprints of manual laborers whose prints may be faded or damaged, as well as older people (Brown et al., 2020).

Moreover, social media has also been the tool used for disinformation campaigns to influence voter opinions and undermine the credibility of election results (Cheng et al., 2018). Research by Jonathan, Sanusi, Akinbola, and Nwankwo (2024) revealed that in Ghana's electoral system, the

rate of misinformation increased drastically between 2020 and 2024. The most prevalent forms of misinformation are out-of-context claims (28%), inter-party misinformation (25%), and AI-generated content (20.8%). Social media platforms such as Facebook, WhatsApp, and Twitter have been increasingly used as weapons by political candidates, political parties, and voters to spread fake news. Newly registered voters who made up 41.8% of those surveyed could be more vulnerable due to over-reliance on digital platforms and limited, reliable information in resource-poor contexts. The fight against lies is equally difficult for journalists because of political pressure and a gross lack of fact-checking training (Jonathan, Sanusi, Akinbola, & Nwankwo, 2024).

Collectively, these cyber trends- technical compromises and information operations- are moulding EC Ghana's security posture in cyberspace, pressing the need to harden BVR, secure the transmission of results, and counter coordinated online manipulation

2.3.2 Adoption of Election Technology and Its Benefits

To improve elections, several democracies have made investments in online result management systems, electronic voter identification devices, and electronic voting and counting systems. Estonia's nationwide internet voting, which was introduced in 2005 and proved that safe online voting at scale was possible and could improve voter convenience, is a noteworthy success story that is frequently mentioned (Ehin et al., 2022). Similar to this, India, the biggest democracy in the world, has been using electronic voting machines for decades in order to speed up vote tallying and eliminate invalid ballots (Election Commission of India, 2020). The commonwealth guide on cybersecurity for elections notes that when properly implemented, technology can "secure [votes]

until official counting begins" and help polling officials verify voter identity efficiently, thus enhancing the integrity of the process (Brown et al., 2020).

Biometric technologies in particular have been promoted as game-changers in contexts with a history of voter fraud. Studies report that biometric voter ID systems have deterred traditional fraud tactics like ballot-box stuffing or ghost voting by tying each vote to a unique physical identity (Effah & Debrah, 2018). In Ghana and Nigeria, the deployment of fingerprint verification at polling stations was lauded as a means to ensure "one person, one vote" by catching impostors and those attempting to vote multiple times (ibid). Indeed, International IDEA's report on introducing biometric technology in elections highlights that biometrics can "provide immediate proof of registration" and serve as a robust authentication method on Election Day (Wolf et al., 2017).

By demonstrating why EMBs, like as Ghana's EC, have adopted technology to increase credibility and trust in results, these advantages correspond with the research goals. They also highlight the first section of my methodology justification, which is comprehending institutional incentives for implementing security innovations in elections, which are frequently normative and coercive pressures in terms of institutional theory.

Scholars warn that technology is not a panacea despite these benefits. Any election technology's efficacy is contingent upon user proficiency, backup procedures, and the larger electoral context. According to Wolf et al. (2017), digitizing electoral processes alone won't fix any flaws in the underlying systems, such as incomplete voter lists or a lack of transparency. As Wolf et al. (2017) bluntly note, "biometric technology alone does not guarantee comprehensive or inclusive voter registration"– citizens still need to be aware of and able to access the registration process.

This highlights that while technology can enhance democracy by addressing certain problems, it must be integrated carefully into the social and institutional fabric, a point the study keeps in focus when evaluating Ghana's approach.

2.3.3 Unintended Consequences and Risks of Election Technology

For all its promise, the introduction of technology in elections has also generated new challenges and vulnerabilities. An emerging body of literature discusses the "digital dilemmas" of election technology – essentially the unintended consequences that may undermine the very integrity such tech was meant to ensure (Cheeseman, Lynch & Willis, 2018). The possibility that technical malfunctions would interfere with the voting process is a crucial concern. There is a limited margin for mistakes because elections are high-stakes affairs that usually take place on a single day; if any equipment or processes malfunction, the effects are instantaneous and extensive.

One example is Ghana's 2012 introduction of biometric verification, which at first increased confidence but caused confusion and delays on election day due to electronic verification device malfunctions, even forcing some polling places to extend voting until a second day (Debrah et al., 2019). These glitches, combined with human errors and ad-hoc policy decisions by polling officials, "neutralised the efficacy of the biometric technology" in guaranteeing a smooth and trusted outcome. In fact, the aftermath of the 2012 election saw the legitimacy of results being challenged in court, partly on grounds that breakdowns in the biometric system might have allowed irregularities (Debrah et al., 2019).

This illustrates a classic unintended consequence: a tool introduced to strengthen integrity inadvertently became a source of dispute due to implementation problems. The lesson – reflected

in Dorpenyo's analysis of Ghana's experience – is that local context and "street-level" adaptations matter greatly. Polling staff, as street-level bureaucrats (Lipsky, 1980), had to improvise when devices failed (e.g., using manual checks), and those decisions, though practical, opened the door for losing parties to allege manipulation. In line with the methodology's emphasis on qualitative insights from implementers, these instances highlight why the research examines not only the existence of security systems but also their actual management.

Another risk of election tech is increased complexity, which can reduce transparency for stakeholders. Traditional paper-based processes, while slow, are visible and understandable to party agents and observers. When results are transmitted electronically or aggregated by software, it may be harder for observers to verify each step, unless special measures are in place. Amoah (2020) argues that "whoever controls the computation [of results] exercises a right to take advantage and win", suggesting that hacking or manipulating digital result systems has become a new avenue for would-be election riggers (Amoah, 2020).

In Africa, this has become a "new battleground" – there is growing concern that tech-savvy incumbents or external actors might compromise result transmission or databases to tilt outcomes (Amoah, 2020). Thus, EMBs face a dual challenge: they must secure their IT systems against intrusions and also convince candidates and voters that those systems are secure. A failure on either front can undermine trust. According to Norris (2019), there is a negative correlation between public trust in elections and perceived concerns about electoral integrity, such as worries about digital manipulation.

This is highly pertinent to Ghana's case: for example, ahead of the 2020 elections, opposition voices raised suspicions about the new biometric voter register and result management system, reflecting a trust deficit that can exist even absence of any proven cyber attack (IMANI Africa,

2021). The study, therefore, treats technology-related perceptions as important as technical facts, examining how Ghana's authorities address public confidence issues – an aspect linking to our research goal about strengthening electoral trust.

Finally, cybersecurity vulnerabilities are a significant unintended consequence of digital elections – a theme so important that we devote the next section entirely to it. This highlights that while election technologies offer improvements (addressing certain research questions about benefits), they also introduce new risks and require robust management.

The literature clearly reveals a gap in documenting how countries like Ghana navigate these trade-offs over time. The research aims to fill part of that gap by analyzing Ghana's experience across multiple election cycles, employing a longitudinal case study approach (Yin, 2018; Pettigrew, 1990) to capture how solutions and problems evolved. This approach aligns with Mahoney & Rueschemeyer's (2003) advocacy for historical analysis in understanding institutional change – here, the changing approach to election tech and cybersecurity in Ghana.

2.3.4 Biometric Technology in Elections: Promise and Perils

Biometric technologies, such as fingerprint, facial, and iris recognition, are increasingly used in elections to improve voter list accuracy and prevent fraud. EMBs promote Biometric Voter Registration (BVR) and verification as tools to deter impersonation and ensure "one person, one vote" (Debrah et al., 2019; Wolf et al., 2017). These solutions do, however, have drawbacks, such as high expenses, technological malfunctions, and threats to privacy and data security (Dorpenyo, 2019; Cheeseman, Lynch & Willis, 2018). Ghana's experience since implementing BVR in 2012

demonstrates both advantages and disadvantages: although biometric verification has decreased multiple registrations, frequent equipment failures and register disputes have eroded trust.

Accordingly, this section reviews the rationale for biometric adoption and the challenges and failures encountered in practice. In doing so, it connects the literature on biometric systems to broader concerns about cybersecurity, data protection, and institutional resilience in Ghana's electoral governance.

2.3.4.1 Rationale for Biometric Systems in Elections

In order to address persistent problems like multiple voting and ghost voters (dead or fictional registrants), biometric voter registration was frequently implemented in developing democracies as part of both domestic reform initiatives and international democracy support. According to Jacobsen (2020), biometric voter registration is a "new modality of democracy assistance" that is frequently supported or promoted by foreign donors who present it as a way to strengthen electoral integrity. Each voter is given a unique biometric identity, which allows the system to de-duplicate the voter roll. This means that duplicates can be removed if the same fingerprint or iris is used twice (Wolf et al., 2017). This was especially alluring in situations where manual voter lists were thought to be inaccurate or inflated.

In Ghana before 2012, opposition parties frequently alleged that voter registers contained duplicates and unauthorized entries. The adoption of BVR in 2012 thus had a strong justification: to create a new, clean register and give every voter a biometric ID to prevent impersonation. Indeed, as noted earlier, Debrah et al. (2019) found that the biometric system initially "served as a forensic measure against election fraud" by blocking multiple registrations/votes, and it

"stimulated confidence" among voters that the election would be fair. Voters could see their fingerprint being verified, which added a sense of transparency and personal validation of the process.

Other benefits of biometrics include reducing identity disputes – e.g., in the past, if someone showed up to vote and their name was already checked off (due to an imposter voting earlier), it would be a word-against-word situation. With biometrics, only the legitimate person's fingerprint should authenticate, thereby precluding impostors. Some countries have also integrated biometric voter IDs into broader national ID systems, streamlining identification across services (though this raises broader privacy issues beyond the election itself, as discussed later). Additionally, biometric voter cards can double as general ID cards, as was the case in Nigeria with its 2015 introduction of biometric Permanent Voter Cards that also carried chips with personal data (Wolf et al., 2017).

From a cybersecurity angle, biometric systems shift some authentication burden from something one has (like an ID card) to something one is (fingerprint, etc.), which, in theory, is harder to steal or forge. However, it also introduces sensitive personal data into the system, which then must be protected. The research considers whether Ghana's investment in biometrics has paid off in terms of trust and reduced fraud, and how the associated data is being secured.

2.3.4.2 Challenges and Failures of Biometric Systems

While conceptually strong, biometric systems have encountered practical problems that the literature documents extensively. Failure rates are a known issue – fingerprints can be worn out (common among manual laborers or the elderly), equipment can malfunction, or software can have bugs. International IDEA's guide explicitly warns that assuming biometrics "always work

correctly and without failure" is unrealistic; in reality, "biometric technologies and related matching" do have error rates and can fail due to various factors (Wolf et al., 2017). For example, in Zambia's biometric voter registration, mentioned in the IDEA report, issues arose in de-duplicating a large dataset within a short time, overwhelming the system.

In Ghana in 2012, the electronic verification devices (used to scan fingerprints at polling stations) had notable failure rates in certain areas – whether due to battery issues, network issues (some were supposed to network to a central system), or reader failures. Dorpenyo (2019) recounts that Ghanaian voters and officials had to "localize" the technology by finding workarounds – such as using manual tick sheets as a fallback, or in some cases allowing voting without verification when devices failed (a controversial move) – illustrating a local user adaptation in the face of technological breakdown.

A critical challenge is the dependency on technology. If the entire voting process hinges on successful biometric verification, then any systemic failure can derail the election. That is why many experts recommend having a clear backup plan (e.g., manual verification using photo ID) and even considering what threshold of failure triggers a fallback. In Kenya's 2013 elections, for instance, widespread failure of biometric kits forced a reversion to manual voter lookup, which the opposition later cited as a cause for suspicion of fraud (Kersting, 2019). Ghana similarly had to extend voting to a second day in some polling stations in 2012 because of biometric failures, an unprecedented step that again became fuel for disputes. Debrah et al. (2019) conclude that these issues "put the legitimacy of the election outcome in jeopardy" despite the good intentions of deploying biometrics. In 2016 and 2020, Ghana upgraded its biometric devices (the EC procured new kits and software), but even new systems can falter, particularly if not fully tested under field conditions or if poll workers are not adequately trained in their use and troubleshooting.

Cost and logistics present another set of problems. The kits, servers, software licenses, maintenance, and training for biometric systems are costly; these expenses can reach tens of millions of dollars. Some critics contend that investing these monies in fundamental infrastructure or voter education may have a more positive impact. Moreover, these systems often depend on external vendors (as domestic capacity to build them is usually lacking), raising concerns about vendor lock-in and sovereignty (Amoah, 2020; Wolf et al., 2017). The sustainability of maintaining biometric databases (continuous updates, replacing lost biometric voter cards, etc.) can strain EMB resources.

For Ghana, the initial BVR in 2012 was funded and executed with significant external help; by 2020, the EC opted to compile an entirely new biometric register, a decision that was controversial partly because of the cost and the implication that the previous system's data could not simply be updated. Civil society groups like IMANI Africa questioned the necessity of a new register, suspecting political motives, and warned about the time constraints and possible technical hiccups in rolling out new biometrics (IMANI, 2021).

This points to a recurring theme: technology decisions in elections are not purely technical; they are intertwined with politics and trust. The literature review finds that technology can become a proxy battle for political actors – if one side believes a system is being introduced to disadvantage them (e.g., via disenfranchisement or manipulation potential), they may resist it regardless of its security merits (Cheeseman et al., 2018).

Finally, data protection and privacy concerns have come to the fore with biometrics. Collecting biometrics means gathering sensitive personal data that, if breached, could put citizens at risk (for example, biometric data could be misused for surveillance or identity theft). McDermott (2017) argues that in the era of big data, we must reconceptualize the right to data protection because

traditional consent-based models struggle when state authorities mandate biometric data collection for voting.

Ghana has a Data Protection Act, 2012 (Act 843), which requires any entity (including the EC) to handle personal data lawfully and securely. One question is how well the EC complies: do they have a Data Protection Officer as required (DLA Piper n.d. notes Ghanaian law mandates many organizations to appoint one), do they conduct privacy impact assessments when introducing new tech, etc.? The Cybersecurity Act, 2020, also indirectly reinforces data protection by classifying personal data systems as potentially critical and requiring breach reporting to the CSA. The Business & Financial Times article (Owusu-Darko, 2024) on the EC's data breach scandal with voter transfers is telling – it explicitly calls for the EC's voter database to be given the highest CII protection and implies that current internal controls were.

Data protection is not just about confidentiality; it's also about citizens' trust that their information (fingerprints, etc.) won't be abused. Thiel (2020) discusses Ghana's "data revolution" and how biometric voter and ID systems feed into larger state data ecosystems, raising questions of oversight and governance. The study touches on this by considering whether Ghana's approach to election cybersecurity also encompasses data privacy measures, an area sometimes neglected in the rush to secure systems against attacks.

In summary, biometric election technologies encapsulate the double-edged nature of tech in elections: they can greatly enhance integrity by eliminating certain fraud and increasing confidence (as initially seen in Ghana), but they also introduce new technical points of failure and new risks (as seen when devices fail or data is mishandled). The literature provides examples from Ghana, Nigeria, Kenya, DRC, and others that reinforce the need for robust planning and backup procedures when using biometrics (Dorpenyo, 2019; Wolf et al., 2017). For the research, this

reinforces why evaluating Ghana's operational preparedness (training, backups, maintenance of devices) is just as important as evaluating high-level policies. The experiences documented also help justify our research scope: Ghana's path with biometrics is a decade old now, providing a rich case to examine longitudinally (Neale's 2019 qualitative longitudinal research approach is apt here), how initial challenges have been addressed or persisted.

2.3.5 Cybersecurity Vulnerabilities Across the Electoral Cycle

Cybersecurity vulnerabilities threaten all aspects of the political process, including the integrity, confidentiality, and availability of election systems and data. The electoral process is now being shaped by digital technologies surging the course of action—from pre-election preparations and election day operation to post-election processes— raising the risk space for adversarial cyber threats (USAID & IFES, 2022a).

Pre-Election

Voter registration databases have remained particularly vulnerable to attacks and hacking attacks ahead of elections. Attacks in 2016, for example, compromised Illinois' voter registration system, therefore revealing information on as many as 200,000 voters (Brown et al., 2020). Similar to the Illinois voter database breach, Ghana's EC has faced concerns over data integrity and unauthorized access to voter registration. In such a situation, cyber attacks could undermine confidence and unbalance voters if documents are altered or destroyed.

Political parties and candidates are vulnerable to spear-phishing, website defacements, and spreading false information during the campaign. For example, the 2017 French presidential elections saw the hacking and online distribution of campaign emails owned by candidate

Emmanuel Macron, a classic case of cyber-enabled information warfare (USAID & IFES, 2022a). Particularly in protecting their internal communications and planning systems, election management bodies (EMBs) also have major challenges. A breach in these systems could cause operational problems and strategic exposure.

Fears of data integrity and even potential unauthorized access to Ghana's voter database echo those already seen elsewhere. The EC's use of BVR and vendor-assisted systems highlights the importance of strong access controls, credible procurement, and regular pre-election audits.

Election Day

Risks mostly center on the availability and integrity of election technologies — electronic poll books and result transmission systems — on election day. For example, as seen in Ukraine's 2014 presidential election, when attackers attempted to disrupt the website of the Central Election Commission, Distributed Denial of Service (DDoS) attacks can compromise crucial election infrastructure (USAID & IFES, 2022c). While paper ballots are used in many locations to this day, voting that's conducted electronically is on the rise and requires more robust security solutions, like end-to-end encryption and multi-factor authentication.

Polling stations and collation centers are connected with the EC's results transmission. To prevent delays and conflicts, it is essential to ensure redundancy, tested incident response, and integrity checks (hashing, reconciliation).

Post Elections

Post-election, emphasis is on nothing but result aggregation and avenues for public dissemination. Manipulated result management systems can potentially subvert the integrity of the election. False announcements lodged upon mutilated websites, for example, can mislead the public and ignite

riots (USAID & IFES, 2022d). A lack of post-election audits and the secrecy surrounding how discrepancies are resolved can also undermine the public's confidence. Managing contestation and maintaining trust depend heavily on timely, verified results release and transparent audit trails, including risk-limiting audits where practical, and the EC needs to adopt this.

In line with global challenges on protecting democratic processes, cybersecurity vulnerabilities cut across the entire electoral cycle in Ghana. The biometric voter registration system has become a subject of public scrutiny over data integrity, as well as allegedly unauthorised movement of voter details, especially during the 2020 general elections. These challenges have brought the data management policies of the Election Commission (EC) under scrutiny, raising concerns of insider threat and poor institutional oversight (The Business & Financial Times, 2024). Furthermore, disinformation campaigns were rife through social media platforms in the 2020 elections, leading to prompt responses from civil society-based organisations and fact-checking entities like FactSpace and Dubawa (Ghana Fact-checking Coalition) (El País, 2024). These groups monitored and dispelled misinformation that threatened to undermine public trust in the political process.

One of the gaping vulnerabilities in Ghana's electoral cybersecurity lies right within the bigger information ecosystem, particularly in the circulation of misinformation targeting voters, candidates, and the integrity of the election process. According to Jonathan, Sanusi, Akinbola, and Nwankwo (2024), the most frequent forms of election misinformation included out-of-context claims (27.8%) and inter-party or candidate-based disinformation (25%) between the years 2020-2024. Politically driven people have continuously exploited social media to propagate fake stories like widely shared films claiming President Akufo-Addo took a $40,000 bribe during the 2020 elections. More lately, artificial intelligence-generated false information, including deepfakes, has

surfaced as a major concern, comprising 20.8% of disinformation incidents and suggesting a clever change in strategy (Jonathan, Sanusi, Akinbola, & Nwankwo, 2024).

Insufficient technical infrastructure and lack of strong, real-time threat detection systems, especially during vote tallying and result transmission phases, aggravate these dangers. The effect of false information is also increased by the great reliance on digital media, which 97.2% of voters consider as their main source of election knowledge. First-time voters, who make up more than 41.8% of new registrations and usually lack the verification abilities required to identify bogus material, should be particularly worried about this (Jonathan, Sanusi, Akinbola, & Nwankwo, 2024). Together, these cybersecurity flaws highlight the critical requirement of a thorough and strong system to safeguard Ghana's voting integrity.

Throughout the political cycle, both internationally and in the Ghanaian setting, a thorough cybersecurity risk management strategy is vital. This involves systematically identifying key assets and threats, assessing system vulnerabilities, and implementing layered, context-specific mitigation strategies (USAID & IFES, 2022b). For EMBs, this means not only having solid incident response plans and conducting regular system checks, but it also involves facilitating effective stakeholder communication to enhance institutional resilience.

These policies would need to be adapted to the local context and be smartly adapted within the political architecture of the electoral process in Ghana, where there have been large weaknesses to digital threats, from concerns over data integrity in biometric registration to the spread of disinformation. Others, such as donors and development partners, should prioritize ongoing capacity-building efforts over ad-hoc technological intervention to optimally secure technology and to ensure long-term risk resilience (USAID & IFES, 2022e).

In the end, including cybersecurity in every stage of the electoral process is not only a technical need but also a basic pillar for preserving democratic integrity. Maintaining public confidence and strengthening the legitimacy of elected institutions depend on protecting elections from digital threats.

2.3.6 Threats to Electoral Integrity

Cybersecurity threats to electoral integrity are surging worldwide as reliance on digital platforms grows. From 2015 to 2018, the number of digital attacks against democratic processes more than doubled, and was sometimes perpetrated by state actors and hired hackers or organized crime and targeted electoral management bodies (Brown et al., 2020). Misinformation campaigns, particularly through social media, erode public trust and influence voters' behaviors (Brown et al., 2020; Jonathan, Sanusi, Akinbola, & Nwankwo, 2024). Similarly, numerous countries, especially from the Global South, are faced with a poorly developed cybersecurity infrastructure; they do not possess the administrative, technological, and human resources required to protect elections (Brown et al., 2020). Moreover, foreign interference, via hacking and disinformation, is a serious threat to the credibility of electoral outcomes (Brown et al., 2020).

Ghana exhibits similar cybersecurity vulnerabilities. E-governance platform weaknesses affect critical data integrity, confidentiality, and service availability, potentially affecting the election process (Botchwey, 2018). Misinformation, including cloning reputable news sources during elections, has misled the public and deemed electoral processes void (Brown et al., 2020; Jonathan, Sanusi, Akinbola, & Nwankwo, 2024). The 2016 election also experienced BVR system breach attempts, and the 2020 and 2024 elections experienced widespread misinformation on leading

social media platforms. Additionally, there is the risk of insider threats to security due to significant unauthorized access to sensitive electoral data (Botchwey, 2018; Brown et al., 2020). The Ghana National Cyber Security Centre helps to combat these threats, though its limited funding and lack of regulatory authority undermine its reach (Brown et al., 2020).

Ghana's dangers are consistent with worldwide trends in all phases, but they are exacerbated by capacity limitations and widespread use of social media. This study looks at how phase-specific threats are addressed by the EC's policies and tools (2012–2024) and where implementation gaps still exist.

2.3.7 Global Trends and Lessons for Ghana

Amid the growing number of cyberattacks against election systems, nations around the world are implementing measures to address the threat before it interferes with the results of an election. Each region offers unique case studies, showcasing the growing nature of these threats and highlighting the necessity for collaboration and response against cyberattacks based on this information.

United States (2016 Presidential Election): Russian-backed hackers attacked voter registration databases, attempted to infiltrate election software vendors, and executed extensive disinformation campaigns (Fidler, 2022; Cheng et al., 2018). These incidents were what led the U.S. Department of Homeland Security to designate election systems as critical infrastructure, which paved the way for extensive reforms. Ghana could adopt a similar approach by designating electoral systems as critical infrastructure and strengthening cross-agency coordination.

France (2017 Presidential Election): Emmanuel Macron's campaign was the target of a cyberattack, dubbed "Macron Leaks," in which internal documents were stolen and released just days before the election. Although the result was not influenced, the attack highlighted the susceptibility of political campaigns to cyber espionage and underscored the need for coordinated responses, including media cooperation (Cheng et al., 2018). Ghana could learn from this by requiring a hardened security baseline for parties or candidates (MFA, phishing-resistant keys) and coordinated media protocols for handling hacked materials.

Kenya (2017 general election): Allegations of hacking into the systems of the Independent Electoral and Boundaries Commission (IEBC) raised concerns that the integrity of electronic vote tallying had been compromised. The election results were invalidated by the Supreme Court based on alleged irregularities, highlighting the dangers of digitized election infrastructure (Cheeseman et al., 2018). Ghana can learn from this by pairing technology with transparent auditability and legal clarity on recounts and dispute resolution.

In the 2014 Ukrainian Presidential election, hacking attempts took place, during which the Central Election Commission's network was compromised and files were deleted and altered. Fortunately, cybersecurity experts intervened just in time, and this compromise did not make its way into the final outcome (Cheng et al. 2018). Ghana can learn from this by investing in real-time monitoring, pre-planned incident response playbooks, and technical surge capacity.

International electoral commission lessons show the importance of cybersecurity frameworks. As an example, the Indian EC employs firewalls of various layers to secure BVR and voting technologies (Brown et al., 2020), presenting a model that the Ghanaian could emulate for enhanced resilience. Estonia has put audit trails and transparency measures in place so that both

public trust and technological accountability are institutionalized (Brown et al., 2020). Ghana can learn from these by combining layered technical controls with public transparency to sustain trust.

These global cases underscore the importance of proactive cybersecurity strategies, institutional coordination, and transparency—areas where Ghana's EC can improve.

2.4 Cybersecurity Instruments and Tools

Amid an increasingly digital world, cybersecurity tools and methodologies are vital to protect the confidentiality, integrity, and availability of the voting process. EMBs need to rely on different combinations of technical and procedural approaches according to their own set of risks and resources and the environment in which they operate (USAID & IFES, 2022a). These tools include data encryption protocols, secure software development methods, multi-factor authentication (MFA), firewalls, and intrusion detection systems (IDS). Encryption is an important tool, for example, to secure the transmission of election results from the polling stations to the central tally centers, particularly end-to-end encryption (USAID& IFES, 2022d).

Another important tool that stops malware and unauthorized access within the election infrastructure is network segmentation. Network segmentation limits lateral movement by isolating critical assets and applying least-privilege access. When combined with access control systems, such segmentation guarantees that users only engage with data and systems required for their duties, hence lowering insider threats (USAID & IFES, 2022b). Firewalls and antivirus software are the first lines of defense against malware and phishing attacks, which are getting smarter and more often are designed to target political players and EMBs.

Additionally, log monitoring and Security Information and Event Management (SIEM) tools are essential for the real-time generation of alerts and the detection of anomalies. These solutions allow EMBs to respond quickly to potential violations, thereby minimizing the time window of exposure and potential harm (USAID & IFES, 2022b). Fast incident response based on monitoring tools provided the Central Election Commission with the ability to thwart a major cyberattack on its results transmission system during Ukraine's elections in 2014 (USAID & IFES, 2022d).

Equally important are cyber hygiene tools and practices, which include frequent software patching, password management, and cybersecurity awareness training. Especially in resource-limited settings, these simple instruments may reflect the most affordable way to lower risk (USAID & IFES, 2022a). Routine audits and penetration testing, for instance, enable EMBs to find and fix weaknesses before they may be used (USAID & IFES, 2022c).

These tools must be provided to EMBs by donor agencies and partners, who also help to guarantee their sustainable application. Development efforts should emphasize capacity building, knowledge transfer, and policy alignment with worldwide best practices rather than providing one-off technology (USAID & IFES, 2022e). A whole approach, including people, procedures, and technology, guarantees that cybersecurity technologies are not only implemented but also properly integrated into electoral systems.

Cybersecurity tools fall into two broad categories: technical and administrative. These complementary instruments are key pillars in the layered defence that is needed for managing cyber risks in contemporary elections.

Technical tools are digital or system-based mechanisms that are used to detect, prevent, and respond to cyber incidents. Examples of these can include firewalls, encryption technologies, intrusion detection and prevention systems (IDPS), virtual private networks (VPNs), endpoint protection software, and multi-factor authentication protocols. Hardware and software assets are at risk from unauthorized use and exploitation, so tools to protect them are designed (Brady et al., 2024; P3 Risk Management, 2023). For example, firewalls are utilized to filter digital traffic in and out of electoral data centers, and encryption is used to protect sensitive voter and election data during transmission and when it is stored. These tools protect hardware and software assets from unauthorized access and exploitation (Brady et al., 2024; P3 Risk Management, 2023).

Administrative measures are non-technical and encompass practices like cybersecurity policies, training personnel, conducting periodic audits, planning for incident responses, and setting up governance frameworks for the organization. These interventions ensure the consolidation of technological deployments through human and institutional aspects, and are fundamental to promoting a culture that fosters cybersecurity awareness (NIS Cooperation Group, 2018; Brady et al., 2024). Risk management policies enable the larger strategic and operational imperatives of electoral bodies to be satisfied through frameworks like the NIST Cybersecurity Framework and ISO/IEC 27001.

One practical example is penetration testing, which requires both a technical execution part and an administrative oversight part. It entails the simulation of cyber-attacks—whether through social engineering, the probing of a network, or the testing of internal access— to unearth vulnerabilities and assess the preparedness for response (P3 Risk Management, 2023). These kinds of tests are increasingly included in election preparedness plans around the world.

(As summarized in Table 2.1 below, cybersecurity instruments span both technical and administrative measures. The effectiveness of electoral protection depends not only on deploying technical tools but also on institutionalizing supportive policies and practices.)

Table 2.1: Cybersecurity Instruments and Tools

Category	Example Tools/Measures	Purpose/Function	Relevance to Elections
Technical Tools	Firewalls, IDS/IPS, SEIM, VPN, Endpoint Protection, Encryption, MFA	Protect data, detect intrusions, prevent unauthorized access	Secure voter registers, protect results transmission, detect anomalies
Administrative Tools	Cybersecurity policies, audits, procurement guidelines, training incident response plans	Ensure governance, accountability, preparedness	Promote compliance, staff awareness, sustainable protection
Hybrid Tools (tech + admin)	ERM frameworks, risk assessments	Combine technical execution with oversight and evaluation	Identify vulnerabilities and test election system resilience

ERM: Electoral Risk Management

IDS: Intrusion Detection System

IPS: Intrusion Prevention System

VPN: Virtual Private Network

SEIM: Security Information and Event Management

MFA: Multi-factor Authentication

As summarized in Table 2.1, electoral cybersecurity relies on both technical and administrative measures. However, the literature also stresses that tools alone are insufficient; their effectiveness depends on integration into broader governance and institutional practices. This observation directly connects to our research objective of evaluating not just the presence of cybersecurity instruments in Ghana's EC, but also the frameworks and practices that sustain them

2.4.1 Application of Cybersecurity Instruments in Elections

From pre-election preparations to post-election activities, cybersecurity technologies and instruments are very necessary for risk mitigation across the political cycle. EMBs have to use strong cybersecurity policies, including technical tools and procedural safeguards, as electoral processes get increasingly digital (USAID & IFES, 2022a).

Pre-Election

The pre-election phase, particularly voter registration, is susceptible to cyber threats, including data intrusions, unauthorized access, and ransomware attacks. Essential tools for safeguarding

voter registration databases are encryption protocols, IDS, and firewalls (USAID & IFES, 2022c). Hacking into Illinois' voter registration system in 2016 compromised the records of about 200,000 voters, an event that highlighted the necessity for proactive protection (USAID & IFES, 2022c).

Additionally, authentication tools like multi-factor authentication (MFA) are very important for keeping hackers out of voting systems. Cybersecurity tools also aid political parties and candidates in warding off disinformation and spear phishing attacks throughout the campaign time. Among the most affordable countermeasures EMBs can adopt are cyber hygiene activities such as regular patching, user awareness training, and endpoint protection software (USAID & IFES, 2022a). In low-resource environments, where advanced technologies might not be easily available, these actions are especially important.

Election Day

To ensure the accuracy of the vote tallying and transmission on election day, security measures such as network segmentation, access controls, and real-time monitoring through SIEM systems are put in place (USAID & IFES, 2022d). For example, during Ukraine's 2014 presidential election, cybersecurity experts were able to minimize a malware attack on the Central Election Commission's results transmission system by fast incident detection and response (USAID & IFES, 2022d). As electoral data travels across networks, encryption and safe communication protocols guarantee its integrity and confidentiality.

Post-Election

Accurate and timely public communication in the post-election phase is vital to stop the misuse of false information. Verifying outcomes and guaranteeing openness depend much on tools that enable digital signatures, forensic analyses, and audit trails (USAID & IFES, 2022d). Constant

vulnerability assessments and penetration testing are also vital tools enabling EMBs to find and fix system flaws before they can be used (USAID & IFES, 2022b).

Institutional measures like cybersecurity policies, standard operating procedures, and national cyber plans, creating governance frameworks for electoral security, should complement these technical capabilities. With donor support matching the maturity of current systems, the Electoral Cybersecurity Donor Program Development Guide underlines that cybersecurity capacity-building has to be sustainable and based in the local setting (USAID & IFES, 2022e). Creating resilient voting systems is most effective with a tiered, risk-based strategy that gives infrastructure and human behavior priority.

To ensure that the elections in Ghana are held in a trustworthy manner, the electoral cybersecurity framework includes various essential instruments and tools. To restrict lateral movement inside systems and safeguard critical electoral data, the EC has been recommended to use network segmentation, access control protocols, and firewalls (MyJoyOnline, 2024). Particularly inside the voter management and results collation systems, the Cyber Security Authority (CSA) keeps advocating for encryption for both stored and transmitted data. Though still underused, real-time monitoring via Security Information and Event Management (SIEM) systems is deemed essential by experts for anomaly detection and prompt incident response (MyJoyOnline, 2024). Resource limits also lead to inconsistent application of regular vulnerability assessments and penetration testing.

In Ghana, the EC has adopted several of these tools, including encryption and MFA, though implementation remains inconsistent. These elements underline the need to expand current tools and use a risk-based strategy suited to Ghana's particular electoral and technological setting.

2.4.2 Technical Tools and Policy Instruments of Ghana's EC

To preserve the integrity and openness of its elections, Ghana's EC makes use of several technical tools and policy instruments. To prevent multiple registrations, the Commission's BVR system records voter fingerprints and photos (Electoral Commission of Ghana, 2023; Ministry of Finance, 2024). Voter management software assists in the compilation and authentication of registers and assists in public verification exercises (Ministry of Finance, 2024). The EC uses electronic results transmission technologies connecting polling places to collation centers to improve the speed and security of election operations (National Development Planning Commission, 2016). Geographic Information Systems (GIS) assist with the demarcation of electoral boundaries and the planning of polling logistics (National Development Planning Commission, 2016).

Consistent with best practice, the EC is recommended to take on board Electoral Risk Management (ERM) methodologies, in which electoral risk is tracked and addressed through data analysis and mapping (International IDEA, 2020). Training and civic education are also digitally facilitated to boost staff potential and sensitisation of voters online (Ministry of Finance, 2024).

Policy instruments are the legal and operational tools for pursuing the tasks of the EC. It derives its mandate from the 1992 Constitution, and is supplemented by Acts of Parliament and Constitutional Instruments (National Development Planning Commission, 2016; Judicial Service of Ghana, 2024). Strategic and medium-term plans (2016–2020 and 2018–2021) set out implementations of technological adoption and organizational reformations (National Development Planning Commission, 2016; Ministry of Finance, 2022). Clear guidelines inform registration of voters, parties, and campaign financing, and structures like the Inter-Party Advisory Committee (IPAC) encourage political conversation (National Development Planning Commission, 2016).

Voter education strategies seek to encourage peaceful and informed participation; operational guidelines standardize electoral processes (Judicial Service of Ghana, 2024; Ministry of Finance, 2022). Policies on stakeholder involvement guarantee even more cooperation with civil society, security forces, and foreign partners to enhance electoral processes (National Development Planning Commission, 2016).

(Table 2.2 below summarizes the evolution of cybersecurity instruments in Ghana's EC)

Table 2.2: Evolution of Cybersecurity Instruments in Ghana's EC

Year	Instrument	Purpose	Policy Driver
2012	BVR system launch	Prevent multiple registrations & ghost voters	Election Reform Committee (2021)
2016	EMS upgrade with IDS and 2FA	Protect voter data and results processing	EC internal audit + NCSC input
2018	IT Procurement & Data Guidelines	Secure third-party data handling	EC IT Department EC Charlotte Osei's dismissal in 2018 due to procurement breaches PPA reforms

2020	Cybersecurity Act Compliance (Act 1038)	National incident response + critical infrastructure law	Government of Ghana (Act 1038, 2020) & National Cybersecurity Policy
2021	Election Technology Incident response	Institutionalize EC's digital crisis response	CERT Gh and UNDP collaboration
2023	Electronic Results Transmission (Pilot)	Decrease manual result manipulation risks	EC's 2023-2027 Strategic Plan + EU Election Observer Recommendations(2020)

EMS: Election Management System **2FA:** Two-Factor Authentication

IDS: Intrusion Detection System

Trend analysis

The table suggests a slow but evident acceleration post-2016 across the areas of basic enrollment controls (BVR) to systems hardening (IDS/2FA), procurement governance, and formalized incident response. Act 1038 of 2020 increased duties by deeming EC systems to be critical information infrastructure.

Policy–practice gap

Despite policy wins, operational limitations — staff expertise, maturity of continuous monitoring, vendor governance, and enforcement — result in patchy implementation. Addressing this gap calls

for ongoing skills building, long-term budget lines for maintenance (not only procurement), and independent audits that inform process improvement.

2.4.3 Frameworks and Best Practices for Securing Elections

In response to the increasing threats facing electoral systems, governments, regional bodies, and international organizations have developed frameworks and best-practice models to guide EMBs. These frameworks emphasize several repeating ideas, including risk management, interagency collaboration, defense-in-depth, resilience, transparency, and continual development. For Ghana, they serve as key benchmarks for determining whether present measures are in line with global norms.

Cybersecurity Frameworks and Standards for Election Infrastructure

One influential model is the U.S. National Institute of Standards and Technology (NIST) Cybersecurity Framework Election Infrastructure Profile (NISTIR 8310). This profile, published in 2024, adapts general cybersecurity best practices specifically to election systems (Howell et al., 2024). The NIST states that the Election Infrastructure Profile "provides a voluntary, risk-based approach for managing cybersecurity activities and reducing cyber risk to election infrastructure" (Howell et al., 2024). It is aimed at election administrators and IT professionals, and focuses on identifying critical assets, protecting them through controls, detecting incidents quickly, responding effectively, and recovering (this falls in line with the core functions of the NIST Framework, which consists of Identify, Protect, Detect, Respond, and Recover). For instance, for voter registration, NISTIR 8310 would propose actions such as restricting the database's access,

encrypting personal data, having periodic integrity evaluations, and incident response plans if unauthorized access is found (Howell et al., 2024).

Likewise, for vote tally systems, it also recommends strong audit trails, system hardening, and the physical security of servers. The NIST profile doesn't replace existing standards (e.g., specific national election IT standards) but supplements them with a comprehensive risk management perspective (Howell et al., 2024). In this case, although Ghana may not actively use NIST, aspects of this method are apparent—for instance, the assignment of Critical Information Infrastructure to electoral systems matches the "Identify" function, while the CSA's call for frequent audits falls under the "Protect" and "Detect" functions (The Business & Financial Times, 2024). The review of Ghana's policy documents will consider whether such structured risk-based approaches are being adopted.

Another important set of guidelines comes from international bodies like the International Foundation for Electoral Systems (IFES) and International IDEA. IFES has published a series of papers (2022-2023) on electoral cybersecurity, emphasizing a holistic view of the electoral cycle. In "Understanding Cybersecurity Throughout the Electoral Process," IFES (2023c) details how the various stages (voter registration, candidate nomination, campaigning, voting, results transmission, and post-election) all present unique vulnerabilities and mechanisms of defence. For example, cybersecurity for voter registration involves securing data at rest and in transfer, verifying the integrity of the register, and developing backup plans such as manual lists of voters in case the system goes down (IFES, 2022). At the same time, the security of results management systems involves ensuring encrypted transmission channels, two-factor authentication for result entry, and independent verification (e.g., parallel vote tabulation) to detect anomalies

(USAID/IFES, 2022d). These recommendations align with cases like Kenya 2017, where the failure of the electronic results transmission was a major controversy (Cheeseman et al., 2018).

A common theme in these guides is audits and testing: EMBs must conduct penetration testing on their systems, simulate attacks, and fix flaws long before an election. Also discussed is resilience – understanding that breaches could occur, how quickly the system can recover, and how effectively the election can proceed in an attack situation (NASEM, 2018, emphasizes having paper backups for votes as one of the key resilience measures).

The Commonwealth Cybersecurity for Elections Guide (Brown et al., 2020) also provides best practices and emphasizes the importance of human factors. It suggests detailed training of election officials about cybersecurity hygiene, close collaboration with national security agencies, and educating voters about disinformation. It also recommends that "polling officials must be able to check voters" reliably and keep systems secure until counting, hinting at technology and procedural protection (Brown et al., 2020).

European experiences under the EU's NIS Cooperation Group also illustrate the value of collective defense. Recommendations include designating elections as critical infrastructure, developing rapid alert systems, and even engaging ethical hackers. During the 2019 European Parliament elections, the EU also secured a voluntary Code of Practice with social media companies to limit disinformation (Bendiek & Schulze, 2019). These cooperative, multi-stakeholder measures set a precedent that Ghana appears to be following on a national scale, by bringing together its CSA, EC, telecom providers, and even international partners (as evidenced by Ghana hosting a West African cybersecurity collaboration symposium in 2024 with support from the U.S.) (Adams, 2024).

Interagency Collaboration and Institutional Preparedness

A recurring theme in best practices is that securing elections is not the responsibility of the EMB alone – it requires a whole-of-government and whole-of-society approach. Bendiek and Metzger (2019) note that democracies must integrate election cybersecurity into their national security strategies. Interagency collaboration models vary: in some countries, the intelligence or national security agency takes the lead in protecting elections (e.g., in the U.S., the Department of Homeland Security works closely with state election officials, and US Cyber Command even deploys "cyber protection teams" to safeguard elections). In others, the election commission works with a specialized cybersecurity agency or task force.

A 2019 study by Staak and Wolf on models of interagency collaboration (later updated by IFES in 2023b) outlines a few approaches: (1) EMB-led security, where the election body builds internal capacity (often challenging due to limited expertise); (2) security agency-led, where responsibility is handed to experts (but this can raise concerns of undue security sector influence in elections); and (3) collaborative platforms, where multiple agencies form a joint working group or command center during elections.

Ghana has effectively been moving toward the third model – a multistakeholder approach. According to Adu-Amanfoh and Allen (2023), Ghana's experience is remarkable in Africa in terms of bringing together government institutions, the commercial sector (telecom companies), and even civil society under a single cybersecurity policy. They note that Ghana's establishment of the National Cyber Security Centre (now Authority) provides a focal point for coordination, which has been used to help a variety of sectors, including elections (Ghana Business News, 2022). For example, since 2017, the NCA and CSA have worked together to safeguard critical information infrastructure and improve incident response (Ghana Business News, 2022). By 2022, Ghana's

cybersecurity partnership had greatly improved its Global Cybersecurity Index score, demonstrating the effectiveness of this collaborative effort.

For election preparedness, Ghana's CSA has convened specific engagements: ahead of the 2024 polls, CSA's Director-General noted they were "engaging social media platforms… to ensure that as we get close to elections, we will be able to detect and prevent" the spread of harmful election disinformation (Adams, 2024). Additionally, CSA has been working with the EC and technology providers on secure communication channels. The Ghanaian Times (2024b) reported an "Election Alert" exercise where CSA, together with tech companies, strategized on countering AI-driven fake news and bolstering the EC's systems. Such efforts reflect an understanding that no single entity can handle all facets of election cybersecurity; it requires combining the EMB's domain knowledge, the cybersecurity agency's technical prowess, telecom firms' network control, and even journalists' fact-checking skills (indeed, media and fact-checkers are part of the wider network – e.g., initiatives like Fact-Check Ghana and foreign partners as mentioned by El País (2024) which described "an army of data verifiers" mobilizing to combat misinformation in Ghana).

From an institutional theory perspective (Scott, 2008; Hsu et al., 2012), it can be argued that Ghana's collaborative approach reflects an institutional innovation influenced by normative pressures (international best practice that advocates for multi-agency cooperation) as well as coercive pressures (the Cybersecurity Act mandating certain collaborations). Hsu et al. (2012) discovered that institutional factors such as laws and norms have a substantial impact on the adoption of security measures. Ghana's instance, where Act 1038 legally binds CII owners and empowers CSA, is a living illustration of this dynamic. The study will assess how effectively this interagency collaboration is functioning in practice for election security, as well as whether any

gaps (e.g., coordination hiccups or unclear mandates) remain, as highlighted by previous analyses (Quaynor, 2018 identified policy and institutional gaps in Ghana's cybersecurity at the time, which the research will revisit in light of recent developments).

These best practices, gleaned from literature and global experiences, form the criteria for analysis in later chapters. By comparing Ghana's preparations and past actions to this list, we can gauge areas of alignment or deficiency. The literature consistently shows that a multi-layered defense (sometimes called "defense in depth") and multi-stakeholder engagement are vital – no single silver bullet exists. This supports the stance of the research that improving electoral cybersecurity is as much an organizational and societal challenge as a technical one. It also justifies the methodological choice to include policy analysis and possibly stakeholder interviews, not just technical analysis, since understanding collaboration and awareness is key to evaluating readiness.

(Table 2.3 below summarizes the International Best Practices for securing Election Infrastructure)

Table 2.3: International Best Practices for Securing Election Infrastructure

Best Practice Area	**Key Measures**	**Examples from Global Standards**	**Relevance for Ghana**
Classify Election Systems as Critical Infrastructure	Legal designation of electoral systems as CII; priority protection, audits, and mandatory standards.	NIST Cybersecurity Framework Election Profile (NISTIR 8310); EU NIS	Ghana's Cybersecurity Act 2020 allows CII designation, but EC systems not yet

		Cooperation Group (2018).	formally classified (Owusu-Darko, 2024).
Risk Management & Assessments	Identify critical assets (voter register, tally systems); assess vulnerabilities; continuous updating.	NIST Identify–Protect–Detect–Respond–Recover model (Howell et al., 2024).	CSA requires risk assessments under Act 1038, but evidence of EC-specific risk assessments is limited.
Technical Safeguards	Encryption of data, multi-factor authentication, IDS/IPS, network segmentation, DDoS protection.	IFES (2022–23); USAID/IFES (2022d).	Ghana has introduced MFA, IDS, and firewalls in EMS, but coverage inconsistent (MyJoyOnline, 2024).
Audit & Testing	Pre-election penetration tests, mock elections, post-election audits with paper trails.	NASEM (2018); EU EOM recommendations	EC piloted electronic results transmission (2023) but independent penetration

			testing/audit reports are scarce.
Incident Response & Continuity	Clear response plans, communication protocols, manual backup procedures.	IFES Resilience Guidance (2023c); U.S. DHS Cyber Protection Teams.	Ghana CSA–EC coordination improving; manual backups used in 2012 when biometric verification failed.
Information Sharing & Collaboration	Multi-agency taskforces; real-time intelligence sharing with CERTs, security agencies, and platforms.	EU Rapid Alert System (2019); U.S. DHS/State partnerships.	CSA and NCA collaborate; Ghana hosted 2024 West African cyber symposium (Adams, 2024).
Public Communication & Transparency	Timely press briefings, official results portals, disinformation countermeasures.	EU EOM Ghana 2020; Commonwealth Guide (Brown et al., 2020).	EC improved in 2020 with frequent briefings; CSA engaged platforms on disinformation ahead of 2024.

Capacity Building	Training EMB staff, cyber hygiene drills, public digital literacy.	Commonwealth Guide (Brown et al., 2020).	CSA's Cybersecurity Awareness Month 2024 included voter/media education; EMB training still limited.
Legal & Accountability Frameworks	Criminalize election-specific cyber offenses; clarify EMB responsibilities.	IFES/USAID (2022a–d); EU compendium.	Ghana's Act 1038 criminalizes offenses; enforcement and EMB compliance with audits remain weak.

2.5 Ghana's Legal and Institutional Framework for Cybersecurity

To understand Ghana's capacity to secure its elections, it is crucial to examine the legal and institutional frameworks the country has put in place for cybersecurity and data protection. Over the past decade, Ghana has significantly overhauled its cyber governance structure, moving from a relatively fragmented situation to a more centralized and robust system. This section reviews the key laws, policies, and institutions, and links them to how they specifically support (or could support) electoral security. Grounding the analysis in these frameworks allows this study to directly assess Ghana's preparedness for election cybersecurity, while also identifying where

legislation and institutions enable effective action and where important gaps remain—echoing concerns raised in earlier literature (Quaynor, 2018).

2.5.1 Cybersecurity Act, 2020 (Act 1038) and the Cyber Security Authority (CSA)

The Cybersecurity Act, 2020, is a landmark law in Ghana's cyber regime. Enacted in late 2020, Act 1038 provides a comprehensive framework for regulating cybersecurity activities in the country (The Business & Financial Times, 2024). One of its most significant provisions is the establishment of the Cyber Security Authority (CSA) as the central body to oversee and enforce cybersecurity standards across both public and private sectors (Government of Ghana, 2020). The Act gives the CSA a broad mandate: policy coordination, setting standards, monitoring compliance, responding to incidents, and protecting Critical Information Infrastructure (CII). Under Section 35 of Act 1038, CII is defined as "computer systems or networks essential to national security or the economic and social well-being of citizens" (The Business & Financial Times, 2024). Once an asset is designated as CII, the owners (which could be government agencies or even private operators of critical systems) are subject to specific obligations and CSA oversight.

In principle, Ghana's electoral systems – especially the central voter database, results management system, and related networks – qualify as critical infrastructure, given that "incapacitation or destruction" of these would "severely impact national security [and] public safety" (The Business & Financial Times, 2024). According to the Act, CSA must oversee CII owners to make sure they put in place adequate cybersecurity safeguards. These include conducting frequent risk assessments, following security guidelines, permitting CSA audits on a regular basis, and promptly informing CSA of any cyber events. This implies that in order to safeguard electoral IT systems,

the Electoral Commission (EC), which is the owner and operator of such systems, should preferably collaborate closely with CSA. According to The Business & Financial Times (2024), the Act even gives CSA the authority to "lead in conducting… assessment [of CII security]" if necessary, implying that CSA can initiate audits or interventions on the EC's infrastructure.

However, a nuance noted in an opinion piece (Owusu-Darko, 2024) is that, as of late 2024, the EC's system had not yet been formally classified as CII, and the EC showed reluctance in inviting an independent audit. This indicates a possible gap between the law's provision and its implementation – something our study will explore by checking if, by the time of the 2024 election, the EC's infrastructure was under CII designation or at least under CSA's active oversight. The CSA itself became operational in 2021 (transitioning from the earlier National Cyber Security Centre). It has since issued directives for various sectors, run Cybersecurity Awareness Month campaigns, and recently (Oct 2024) launched an updated National Cybersecurity Policy and Strategy (NCPS) (National Cybersecurity Authority, 2024). According to the Digital Policy Alert (2024), the new NCPS "establishes a National Cybersecurity Risk Management Framework, and sets standards for Critical Information Infrastructure protection". This presumably means that guidelines or regulations now exist in Ghana on how CIIs should be secured – which would apply to election systems once designated. The NCPS also operationalizes the national CERT (Computer Emergency Response Teams) ecosystem, crucial for incident response, and emphasizes capacity-building and certifications. All these align with best practices and, importantly, provide institutional backing for election cybersecurity. The research will gauge how these high-level policies trickle down to actual election preparedness (e.g., was there a specific risk assessment for Election 2024 in light of these frameworks? Did CSA and EC form a joint task force? etc.).

2.5.2 Data Protection Act, 2012 (Act 843) and Personal Data Protection

Ghana's Data Protection Act of 2012 is the primary law guarding personal data privacy. It established principles for data handlers (data controllers) such as lawfulness, purpose limitation, data minimization, security safeguards, and individual rights (like access and correction). The Act also created the Data Protection Commission to oversee compliance. In elections, huge amounts of personal data are collected – names, ages, fingerprints, sometimes photographs, etc., of voters, as well as results data which can be sensitive. Therefore, the EC is a major data controller under this law. A notable requirement of Act 843 (reinforced by later amendments and interpretations) is that certain entities must appoint a DPO and register with the Data Protection Commission (DLA Piper, n.d.). Additionally, any biometric data is considered sensitive personal data, demanding higher protection.

The intersection of data protection and cybersecurity is clear: protecting data means both preventing unauthorized access (cyber breaches) and ensuring proper use. For example, the illegal voter transfer incident in 2024 was not only a cybersecurity lapse but also a breach of data protection rules (data was processed for an unauthorized purpose and without consent). It's likely that, beyond the CSA's involvement, the Data Protection Commission could have an interest in that case, as it violates citizens' privacy and the integrity of personal information. The idea that citizens have a stake in how their data is secured during procedures like elections is highlighted by McDermott's (2017) conceptual discussion, which is wide but emphasizes the need for the EC to be transparent about its data practices. Global guidelines recommend that EMBs disclose privacy policies and be explicit about data retention (e.g., how long biometric data is stored and when it is erased, if at all). However, the literature study did not identify specific studies on Ghana's EC and data protection (this could be a gap).

One challenge is that election data often needs to be shared among agencies: for instance, the EC might share the voter roll with political parties (in Ghana, parties do receive copies of the register), or with the National Identification Authority for verification purposes. Each sharing increases risk if not managed well. The Data Protection Act provides a framework for lawful data sharing (with consent or legal authority and with safeguards). Ensuring that, for example, political parties don't leak the voter data or use it for unintended purposes (like targeted campaigning without consent) is another dimension of election data protection, though one might argue it's beyond cybersecurity and into ethics.

However, given that voter data has monetary and political value, it could also be targeted by hackers for identity theft or intimidation. Thus, Act 843 complements Act 1038 by focusing on the rights and responsibilities around personal data. Our research will consider whether Ghana's election stakeholders (EC, CSA, Data Protection Commission) coordinate on these issues, especially with the introduction of new technologies. A sign of maturity would be if the EC conducted a Data Protection Impact Assessment for new systems like the biometric register – a practice in the EU and some other jurisdictions.

2.5.3 Other Relevant Legislation and Institutions

Aside from the two major Acts above, Ghana has other laws that intersect with election cybersecurity: the Electronic Transactions Act 2008, which criminalizes cyber offenses, the Criminal Offenses Act (amended to cover cybercrimes), and specific electoral laws that increasingly mention electronic systems. For example, the Electoral Commission Act, 1993 (Act 451) establishes the independence and functions of the EC, but back then did not envisage

electronic processes. More recent regulations for voter registration, etc., have had to incorporate the use of biometrics (e.g., CI 91 and CI 126 for voter registration). It would not be surprising if regulations now include provisions on electronic result transmission (if Ghana uses it) or on the handling of devices. The Judicial Service's Election Adjudication Manual (4th ed. 2024) might also mention how to treat electronic evidence or disputes arising from tech issues (Judicial Service of Ghana, 2024).

Institutionally, the National Communications Authority (NCA) plays a role, as it oversees telecom networks on which elections rely (for transmitting data or simply for communication). The NCA's collaboration with CSA (as discussed, reaffirmed in 2022, and ongoing) is crucial in ensuring telecom operators heed election-period needs (like maintaining network uptime, mitigating DDoS). Ghana's CERT (Computer Emergency Response Team), now under CSA and referred to as CERT-GH, is another piece – they would be the ones to respond to any cyber incidents on election day. Monitoring threats and assisting with incident response across industries are the responsibilities assigned to CERT-GH (Ghana Business News, 2022). One hopes that on election day, CERT-GH has a direct line to the EC's IT team to rapidly address incidents.

Ghana's efforts in strategy and policy planning are also noteworthy. High-level guidelines are provided by the National Cybersecurity Policy & Strategy (NCPS) 2021 (and updated 2024). According to Ghana News Agency (2024), the 2024 revision is "a strategic response to both existing and anticipated cyber threats that could undermine Ghana's gains in..." presumably digital growth. It emphasizes capacity-building and specifically calls for the establishment of CII standards (Digital Policy Alert, 2024). Within such strategy documents, elections are likely highlighted as a critical domain (especially given incidents in other countries).

Ghana launched NCSAM 2024 (Cybersecurity Awareness Month) with the theme "Combating Misinformation/Disinformation in a Digitally Resilient Democracy" (National Cybersecurity Authority, 2024), directly tying national cyber efforts to the election. This indicates a high-level recognition and integration: election cybersecurity is now part of national cybersecurity discourse. The study sees this as an evolution from earlier years – Quaynor (2018) had pointed out that Ghana lacked clear policies and institutional clarity on cybersecurity, which could hamper dealing with threats. By 2024, that gap appears to be closing with formal policies and a dedicated Authority.

However, policy existence doesn't automatically mean execution. The implementation constraints are also noted in the literature: Kolog & Tijani (2023) examine implementing the Cybersecurity Act in public financial institutions and found constraints like limited funding, shortage of skilled personnel, and organizational resistance to new procedures. These likely apply to the EC as well – being an autonomous body, the EC might have its own culture and could resist external oversight or struggle with the capacity for new requirements. Lipsky's concept of street-level bureaucracy can analogously apply: if local election IT officers are overburdened or not fully trained, they might not implement every security rule to the letter, focusing on immediate tasks instead (Lipsky, 1980).

To sum it all up, Ghana's legal and institutional framework has, on paper, many elements of a strong defensive posture for election cybersecurity. The Cybersecurity Act and CSA provide authority and structure; the Data Protection Act ensures privacy considerations; collaborations like NCA-CSA and multi-stakeholder engagements show a willingness to operationalize these frameworks. The literature reviewed suggests that Ghana is regarded as a model in Africa for these developments (Ghana Business News, 2024). What remains to be seen, and what our research examines, is how these frameworks are applied specifically to 2024 election preparations. Are the

EC's systems audited and hardened per CSA guidelines? Is there an incident response plan shared between EC, CSA, and security agencies? Is misinformation being actively monitored and countered by a coordinated team (as the symposium and engagements imply)? By investigating these, the study connects the dots between the high-level frameworks and the practical measures on the ground, thereby contributing to understanding the effectiveness of Ghana's approach.

Table 2.4: Ghana's Legal and Institutional Framework for Cybersecurity

Law/Institution	Key Provisions	Relevance to Elections	Observed Gaps/Issues
Cybersecurity Act, 2020 (Act 1038)	Establishes Cyber Security Authority (CSA); regulates Critical Information Infrastructure (CII); mandates audits, reporting, and compliance with cybersecurity standards.	Election IT systems (voter register, results transmission) qualify as CII; CSA empowered to audit and enforce standards.	EC systems not formally classified as CII as of 2024; limited evidence of joint audits with CSA.
Cyber Security Authority (CSA)	National body for cybersecurity oversight; incident response (CERT-	Provides technical expertise, threat intelligence, and collaboration with EC	EC's engagement with CSA sometimes ad hoc; potential gaps

	GH); capacity-building and awareness campaigns.	and telecom operators during elections.	in mandate clarity and enforcement capacity.
Data Protection Act, 2012 (Act 843)	Governs collection, storage, and use of personal data; requires Data Protection Officers and registration of data controllers.	EC is a major data controller (biometric register, voter rolls, results data); biometric data classified as sensitive personal data.	Limited transparency on data retention and protection measures; weak enforcement of party/third-party use of voter data.
Other Relevant Laws (e.g., Electronic Transactions Act 2008; Criminal Offenses Act; Electoral Commission Act 1993)	Criminalize cybercrimes; establish EC's independence and mandate; regulate electronic transactions.	Provide legal basis to prosecute election-related cyber offenses; empower EC to adopt digital systems.	Many laws predate current digital election practices; limited adaptation to biometric and online systems.
Institutional Collaborations (e.g.,	Interagency cooperation mandated	NCA ensures telecom stability; CERT-GH	Coordination mechanisms

CSA–NCA, CSA–EC, CERT-GH)	under Act 1038 and NCPS; telecom operators support secure networks.	provides rapid response; CSA coordinates stakeholders.	evolving; gaps in preparedness exercises and joint incident response planning.

Table 2.4 demonstrates how Ghana's legal and institutional frameworks align with, but also diverge from, international benchmarks. While the Cybersecurity Act and Data Protection Act provide a strong foundation, implementation gaps remain in areas such as critical infrastructure designation and data protection enforcement. This reinforces the importance of our research focus: assessing not only the existence of frameworks but also their operationalization in the electoral domain.

Together, the comparative insights from Tables 2.3 and 2.4 offer a structured benchmark to assess the EC's cybersecurity preparedness. This synthesis not only highlights Ghana's progress and gaps but also sets the stage for the longitudinal analysis in Section 2.6.

2.6 Longitudinal Analysis of Ghana's EC

A longitudinal perspective reveals how Ghana's EC has evolved in response to cybersecurity threats, policy reforms, and technological changes. Examining the 2012-2024 cycles reveals institutional learning rather than tool adoption: early vulnerabilities encouraged incremental adjustments; national mandates (e.g., Act 1038) sped standard-setting and compliance, while recurring election stresses honed operational routines. The approach, which is framed by

Institutional Theory, examines how route dependency and external isomorphic influences (from national legislation and international norms) affected EC choices over time (March & Olsen, 1984). The CIA triad (confidentiality, integrity, and availability) complements this organizational viewpoint by providing technical criteria for determining if reforms significantly decreased risk in voter data management, results integrity, and system uptime. Taken together, the longitudinal analysis moves beyond description to explain why and how the EC's cybersecurity posture changed—and where policy intentions still outpace practice.

2.6.1 Why Longitudinal?

This study adopts a qualitative longitudinal approach to capture the EC's evolving cybersecurity practices over time. Longitudinal analysis is essential because events in one cycle condition decisions in the next—for example, technical glitches or data controversies trigger protocol updates, procurement rules, and capacity-building that persist (or lapse) in later years.

With the complete rollout of Biometric Voter Registration (BVR) and biometric verification tools, the 2012 elections signaled Ghana's significant jump toward digital electoral administration. But this technological change took place without a thorough cybersecurity policy, hence exposing the EC to data integrity and operational issues (Dorpenyo, 2019). By 2016, worries started to surface about efforts to compromise the voter database and flaws in the election result transmission system (Dorpenyo, 2019). These weaknesses spurred internal investigations and resulted in small digital protocol changes like the addition of fundamental firewall systems and backup redundancy.

Coinciding with increasing regional awareness of cyber risks to democracy, including disinformation campaigns and coordinated cyberattacks, the 2020 electoral cycle marked a turning

point. The EC worked with CERT-Gh and the National Communications Authority (NCA) to carry out pre-election cyber risk evaluations, social media monitoring projects, and encrypted result transmission systems in reaction (USAID, 2019). The Cybersecurity Act (2020), which named the EC as a vital information infrastructure (CII) organization, hence driving these projects forward by imposing compliance responsibilities, including incident reporting and infrastructure audits, spurred them even more (Government of Ghana,2020)

The EC's cybersecurity posture by 2024 had developed even more to include a multi-tiered incident response strategy, internal ICT staff training courses, and coordination tools with civil society observers, including the Coalition for Election Cybersecurity (CES). This change shows an institutional learning path that becomes completely apparent only via longitudinal study. It also emphasizes the gradual integration of cybersecurity, from reactive, ad hoc technology solutions to more organized, proactive approaches.

Institutional theory offers a helpful perspective in this regard since it implies that internal constraints and external shocks influence how public organizations change over time (March & Olsen, 1984). A longitudinal viewpoint thereby allows systematic comparison across cycles (2012, 2016, 2020, 2024), tying specific shocks and mandates to observed procedural and technical changes, and captures the interaction between structure, agency, and technological change inside Ghana's EC—evidence directly responsive to the study's aims.

2.6.2 Methodological Insights

Utilizing a longitudinal research of cybersecurity in election governance offers both possibilities and obstacles. Methodologically, the study uses qualitative data gathering techniques including

document analysis, semi-structured interviews with EC officials and cybersecurity specialists, and thematic analysis of media and civil society reporting. These materials offer an analysis of institutional decision-making processes throughout time and help to rebuild the EC's cybersecurity development.

The research covers four important electoral cycles: 2012, 2016, 2020, and 2024. Focusing on the introduction of new technologies, changes in policy orientation, and changes in stakeholder involvement, this periodization allows a phase-by-phase analysis. For example, although 2012–2016 concentrated mostly on technology adoption, like the BVR rollout, the 2016–2020 period saw more concentration on incident response and risk mitigation, then a consolidation of legal frameworks after 2020 (Government of Ghana, 2020).

QL allows for process tracing, which connects triggers (e.g., attempted breaches, disinformation spikes, new statutes) to organizational actions while also identifying continuities (repeated bottlenecks) and inflection points (for example, Act 1038).

Access to critical cybersecurity information presents one methodological difficulty, particularly in light of political and institutional sensitivities over electoral integrity. Many important papers, such as cyber incident logs and internal audit reports, are often classified or limited, hence hindering complete openness. Triangulation of data sources is therefore necessary; it depends on verified interview stories, publicly accessible records, and cross-institutional evidence to confirm important trends. Attribution issues (distinguishing coincidence from causation) are addressed by temporal bracketing and checking for mechanism consistency across sources.

Ethical issues are also quite important, especially when participants are EC staff or cybersecurity authorities revealing possibly sensitive material, interview protocols have to guarantee

confidentiality. Given the sensitivity of election cybersecurity, the study follows institutional review board (IRB)-approved protocols: informed consent, role-based anonymization (removing identifiers), secure storage of notes and transcripts, and careful redaction of operational details that could create security risk. Participants can review excerpts attributed to their roles to ensure accuracy and minimize harm. The sensitive nature of cybersecurity data required careful handling of confidential information and informed consent from participants.

The QL design directly serves the study's core aims by (a) showing how specific tools and policies emerged and interacted, (b) assessing policy–practice alignment over time, and (c) identifying coordination gaps among EC, CSA/CERT-Gh, and stakeholders—thereby grounding conclusions in observed sequences rather than single-year snapshots.

2.7 Gaps in the Literature

Although academic interest in cybersecurity and electoral governance is rising, the literature shows significant gaps in the inclusion of cybersecurity tools and policy frameworks within Ghana's EC. Though seldom both together, existing studies tend to provide either technical evaluations of voting technologies or more general policy studies. Three main thematic gaps—the instrument-policy disconnect, longitudinal blind spots, and stakeholder dynamics in cybersecurity governance—under which this part synthesizes these omissions, are presented.

2.7.1 Instrument-Policy Disconnect

One significant shortcoming is the piecemeal study of cybersecurity techniques with their related policies. Much of the literature treats technical instruments (e.g., BVR, transmission software, IDS) separately from the policies meant to govern them. Although some research has covered biometric voter registration (BVR) systems and other electoral technologies in Ghana, few look at how these tools fit into a comprehensive cybersecurity framework. For example, although Debrah (2019) discusses the technical efficiency of BVR systems, the study does not assess whether their implementation follows domestically mandated cybersecurity rules or international standards like ISO/IEC 27001.

Osei-Tutu, Asare, and Agyei (2020) likewise evaluate Ghana's digital vulnerabilities during election times but do not look into whether certain tools—such as secure data transmission software or intrusion detection systems—are guided by enforceable internal EC policies or national legislative instruments like the Cybersecurity Act (2020) (Government of Ghana, 2020). This gap emphasizes a more general research oversight: the absence of investigation on how technical infrastructure and policy regimes in the Ghanaian electoral setting mutually support or hinder one another.

Document analysis in this study indicates that early BVR rollouts preceded comprehensive cybersecurity standards, creating uneven downstream practices in access control and vendor governance—an archetypal instrument–policy gap.

By pairing tool adoption with the policies and enforcement routines that should govern them, the longitudinal analysis shows where instruments are well-institutionalized and where they remain procedures on paper.

2.7.2 Longitudinal Blindspots

Longitudinal studies following the development of the EC's cybersecurity policies across several electoral cycles constitute another major gap in the literature. Most current studies are snapshot analyses concentrating on certain election years, like 2016 or 2020, without considering continuity, institutional learning, or change over time. These studies, therefore, miss how past events, such as attempted data breaches in 2016 or the increased misinformation threats in 2020, would have guided later legislative changes or technical tool upgrades by 2024.

In settings like Ghana, where institutional capability and regulatory frameworks are still developing, longitudinal studies are particularly important. Determining whether cybersecurity actions are reactionary or part of a sustainable, ongoing plan without a temporal perspective is quite challenging. Countries with a long-term policy path are better placed to discourage, detect, and react to cyber attacks, as Bendiek and Metzger (2019) point out in their comparative study on digital election interference. Ghana's situation thus calls for a comparable analytical approach to evaluate institutional change across time.

This study contributes to the literature by providing the first qualitative longitudinal analysis of the EC's cybersecurity evolution from 2012 to 2024. It provides a qualitative longitudinal analysis (2012–2024) that connects shocks, mandates, and adoption sequences to observed organizational routines—showing where learning has consolidated and where vulnerabilities persist.

2.7.3 Stakeholder Dynamics and Institutional Roles

The third main gap is in electoral cybersecurity governance with regard to stakeholder relationships. Although certain studies recognize the contributions of the Cybersecurity Authority (CSA), CERT-Gh, and other government agencies to national cyber defense (Baker & Osei-Tutu, 2019), very few emphasize their cooperation or absence thereof with the Electoral Commission. Still mostly uninvestigated are issues with collaborative incident response, role clarification, and coordination procedures.

For example, the Cybersecurity Act (2020) names the EC as a vital information infrastructure (CII) owner, thereby legally requiring its cooperation with national cybersecurity agencies (Government of Ghana, 2020). Especially during high election times, there is little study on how this legal duty converts into operational cooperation, such as data exchange, risk assessments, and threat intelligence integration.

Furthermore, the function of civil society organizations (CSOs) and international development partners in fostering electoral cybersecurity is under-theorized. Although USAID (2019) records some outside technical support to the EC for the 2020 elections, there is too little scholarly involvement with how these entities affect institutional norms, frame cybersecurity debate, or support capacity creation. Given that election trust is not merely a question of technology or law but also of multi-stakeholder legitimacy and openness, this disparity is very significant.

Bridging these gaps is crucial not just for academic advancement but also for enhancing Ghana's democratic fortitude vis-à-vis emerging digital threats. The thesis, therefore, seeks to make a timely intervention to address the gaps through a qualitative longitudinal study specifically on Ghana's Electoral Commission. Using interviews and document triangulation, it maps who does

what, when, and with what constraints, highlighting coordination frictions (e.g., incident reporting cadence, baseline security for parties/candidates) and proposing practice-oriented improvements.

Future research can extend this work by (a) comparative analysis with peer EMBs in the region, (b) structured audits of cross-agency exercises, and (c) platform-level studies of election-period content governance and data access for verified researchers.

2.8 Summary

This chapter has examined the growing intersection of elections, technology, and cybersecurity, with a focus on Ghana's Electoral Commission (EC). It reviewed global and Ghanaian experiences of election technology, highlighting both benefits and risks, and analyzed vulnerabilities across the electoral cycle. The discussion also considered the EC's tools and policy instruments, situating them against international frameworks and best practices.

The review identified three major gaps: the lack of integration between instruments and policies, the absence of longitudinal studies, and insufficient analysis of stakeholder dynamics. Addressing these gaps justifies the present study, which applies a qualitative longitudinal approach to trace how Ghana's EC has adopted and adapted cybersecurity measures across four electoral cycles. These insights provide the conceptual foundation for the methodology presented in Chapter Three.

CHAPTER THREE

METHODOLOGY

3.1 Introduction

This chapter describes the technique used to investigate the development of cybersecurity technologies and legislative regulations at the EC. The study takes a qualitative longitudinal methodology, which allows for a thorough examination of how the EC has responded to evolving cyber risks and changed its institutional processes throughout four important election cycles: 2012, 2016, 2020, and 2024.

The approach used is directly related to the study questions and objectives. Research Objective 1, which involves evaluating the evolution of the EC's cybersecurity framework, necessarily requires a design that can track change across time. Research Objective 2, which assesses the effectiveness of policies and instruments, calls for qualitative methods in favor of contextual interpretation over numerical reduction. Finally, Research Objective 3, which identifies gaps and formulates recommendations, depends on the triangulation of insights from multiple data sources.

Accordingly, this chapter explains the philosophical stance guiding the research, the research design and approach, the data collection methods, the data analysis techniques, and the measures taken to ensure trustworthiness and ethical compliance. Each section illustrates how the methodological choices lead to answering the study's research questions and accomplishing the study's objectives.

3.2 Research Philosophy and Approach

This study is anchored in an interpretivist research paradigm, which holds that reality is socially constructed and that knowledge is generated through the subjective experiences and meanings individuals and institutions attach to their actions (Bryman, 2016). Interpretivism is thus ideal for investigating how a public organization such as the EC perceives, understands, and responds to the dynamic threat of cybersecurity.

Using this paradigm, the study can disentangle the complex institutional dynamics of decision-making, discretion, and policy adaptation. Interpretivism also serves as an analytical lens through which meanings are derived from semi-structured interviews with EC officials and stakeholders, as well as the interpretation of documents such as policy papers, legislative instruments, and audit reports.

This interpretivist stance directly informed the adoption of a qualitative research design. Qualitative inquiry is best suited to exploring complex issues such as inter-agency cooperation, policy formulation, and cybersecurity implementation—topics that do not lend themselves to quantitative measurement. The emphasis is therefore on meaning-making, contextual understanding, and historical trajectories rather than statistical generalization.

Pragmatically, interpretivism informed both data collection—prioritizing open-ended interviews and rich documentary evidence—as well as analysis, through thematic and longitudinal techniques that foreground participants' interpretations and institutional learning over time.

3.3 Research Design: Qualitative Longitudinal Study

This study uses a qualitative longitudinal research design, which tracks development, discontinuities, and patterns of change by collecting and analyzing data over a long period of time. The longitudinal methodology makes it possible to track institutional learning and policy evolution over several election cycles, in contrast to a cross-sectional qualitative study that only offers a picture of a phenomenon at one particular moment in time.

The study's goal of analyzing how the Electoral Commission (EC) has responded to evolving cybersecurity threats, legislative reforms, technological developments, and external pressures is best achieved by this methodology. The approach makes it possible to determine whether institutional responses have been proactive in predicting dangers or reactive to crises by tracking the EC's cybersecurity posture over time.

The focus on four electoral cycles — 2012, 2016, 2020, and 2024 — is deliberate. The 2012 elections marked the rollout of biometric voter registration, signaling Ghana's entry into digital electoral governance. The 2016 cycle saw rising concerns about voter database vulnerabilities and electronic results transmission. The 2020 elections coincided with the passage of the Cybersecurity Act, which reclassified the EC as Critical Information Infrastructure. Finally, the 2024 elections offer the opportunity to capture the latest adaptations, including electronic transmission pilots and responses to AI-driven disinformation.

Thus, the qualitative longitudinal design not only fills a gap in the literature—where most studies remain single-election snapshots—but also provides a temporal and institutional perspective on Ghana's evolving electoral cybersecurity landscape.

3.4 Data Collection Methods

This study employs a multi-source qualitative data collection strategy to investigate the development of cybersecurity tools and policy regulations within Ghana's Electoral Commission. Institutional adaptation is inherently complex, involving interactions across law, technology, and governance; hence, two complementary methods were selected: document analysis and semi-structured interviews.

These methods were chosen to enable triangulation, which involves cross-checking information from multiple data sources to enhance the validity and reliability of the results. In this study, triangulation guarantees that institutional narratives from interviews are backed (or disputed) by documented evidence, resulting in a more balanced and rigorous assessment.

Document Analysis: Primary sources included EC policy manuals, strategic plans, and reports from 2012 to 2024, supported by national legislation such as the Cybersecurity Act (2020) and the Data Protection Act (2012). Operational guidelines from the Cyber Security Authority (CSA), CERT-Ghana, and advisories from development partners (e.g., UNDP, EU observer reports) were also examined. Secondary materials, such as academic journal articles, media reports, and international best practice frameworks (e.g., IFES, NIST), enriched the analysis.

Semi-Structured Interviews: These were conducted with purposively selected informants, including EC staff (IT, legal, and operations units), officials from CERT-Ghana and the CSA, private cybersecurity consultants, civil society watchdogs, and civil society representatives engaged in digital election monitoring. A chain referral (snowball) sampling strategy was adopted, where initial participants identified further key informants with relevant expertise. This method proved very useful for reaching actors who held insider insights into electoral cybersecurity.

On average, the interviews were 45 minutes each. Open-ended questions enabled respondents to elaborate on their own experiences, challenges, and interpretations of cybersecurity threats and responses, which were then extended by the researcher with probing questions to get more in-depth and clarification on key issues.

Document analysis and interviews combined provided a triangulated evidence base to illustrate the evolution of EC's cybersecurity tools and frameworks over time.

3.5 Data Analysis

The study uses thematic analysis and qualitative content analysis to systematically interpret the data. Thematic analysis was chosen for its capability to find, analyze, and report patterns in rich textual material, while content analysis offered the systematic coding of documents and transcripts. The analysis process is broken down as follows.

The analytic process followed several stages:

1. Familiarization – Interview transcripts and documents were read multiple times to gain an in-depth understanding.

2. Initial Coding – Both inductive codes (emerging directly from the data) and deductive codes (based on research questions and theoretical frameworks) were applied.

3. Theme Development – Codes were organized into broader categories, which reflected key areas such as the evolution of cybersecurity tools, policy-practice congruence, and stakeholder engagement.

4. Longitudinal Comparison – A coding matrix was constructed to compare data across the four electoral cycles (2012, 2016, 2020, 2024), enabling the identification of continuities, disruptions, and reform trajectories.

5. Member Checking – Preliminary interpretations were shared with selected interviewees to validate accuracy and enhance credibility.

6. Analytic Memos – Notes were written throughout the process to capture emerging insights, clarify coding decisions, and link empirical observations to theoretical frameworks.

The data was organized and coded using NVivo software to facilitate efficient search of coded sections and to compare the analysis with other cases. NVivo, for instance, allowed for the mapping of themes in the "policy-practice gaps" field with electoral cycles, making longitudinal patterns visible.

Co-evolution guided the interpretive aspect of the analysis. Co-evolution describes the process whereby institutions and technologies adapt with respect to each other, in which changes in EC policies (e.g., compliance with the Cybersecurity Act) influence technical practices (e.g., encryption, results transmission), and vice versa. By following these interlocking dynamics, the analysis discloses how the EC's cybersecurity posture has evolved—or stagnated—over time.

The thematic and longitudinal strategy ensured the study was not merely descriptive of cybersecurity developments but also was meaningful in articulating how institutional actors understood and navigated these challenges in Ghana's political and resource environment.

3.6 Trustworthiness and Rigor

To ensure credible and reliable findings, this study followed the four criteria of trustworthiness in qualitative research: credibility, transferability, dependability, and confirmability (Lincoln & Guba, 1985).

Credibility

Triangulation and member checking were used for credibility. Triangulation describes the use of multiple data sources—document analysis, stakeholder interviews, and media reports, in this case—to validate the findings and mitigate bias. This evidence convergence enhanced interpretive accuracy. A member checking process was performed where major thematic interpretations were shared with selected participants to check if the analysis accurately captured their viewpoints. This process strengthened confidence in the authenticity of the narratives.

Transferability

Transferability was enabled through the use of thick description—the detailed presentation of contextual data that incorporates participant accounts and documentary evidence within the historical and institutional context of Ghana's Electoral Commission. Thick description helps to enable readers to judge whether and how the findings may generalize elsewhere, while still making them grounded in the Ghanaian case.

Dependability

In an effort to enhance the reliability, an audit trail was kept in the course of the research work. To ensure dependability, an audit trail was maintained throughout the research process. An audit trail consists of detailed records of coding decisions, analytic memos, interview protocols, and

methodological reflections. This documentation provides transparency and allows future research to be guided by an understanding of the logic of the study, for replication or critical evaluation.

Confirmability

Finally, confirmability was addressed by systematically documenting analytic decisions and reflecting on potential researcher biases. This was achieved by utilizing multiple sources of data, as well as participant validation, to validate the findings based on the evidence as opposed to personal biases.

Together, these strategies enhanced the trustworthiness of the study by ensuring that the findings are credible, contextually grounded, and supported by systematic documentation.

3.7 Ethical Considerations

Given the sensitivity of cybersecurity and electoral governance, ethical safeguards were integral at every stage of the research process. The study received ethical approval from the University of Ghana Institutional Review Board (IRB) before data collection.

Informed Consent and Voluntary Participation

All participants were provided with clear information about the study's purpose, their rights, and the measures taken to protect confidentiality. Written or verbal consent was obtained, depending on the interview mode. Participation was voluntary, and participants were informed of their right to withdraw at any time without penalty.

Confidentiality and Anonymity

Context-appropriate confidentiality was rigorously maintained. Interview data were anonymized using pseudonyms, and institutional identifiers were masked where disclosure could compromise security or reputation. Digital files—including recordings and transcripts—were encrypted and stored on password-protected, restricted-access systems.

Handling Sensitive Information

Particular care was taken in managing cybersecurity-related data, such as internal EC procedures or potential system vulnerabilities. A harm-reduction approach was adopted: information was presented in ways that protected national security, institutional credibility, and the professional integrity of individual participants. The study adhered to high ethical standards throughout, ensuring that findings were reported responsibly and without exposing participants or institutions to risk.

By following these ethical protocols, the research ensured integrity, respect for participants, and compliance with both institutional regulations and national data protection laws.

3.8 Limitations of the Methodology

While the chosen methodology is well-suited to the research objectives, several limitations must be acknowledged. One significant constraint is access to data. Given the sensitive nature of electoral cybersecurity, obtaining official documents or information on cyber incidents was sometimes hindered by bureaucratic processes or confidentiality restrictions. This affected the completeness of some datasets, particularly internal audit reports and classified threat assessments.

Secondly, the rapidly evolving nature of cyber threats presents a methodological challenge. As digital risks and attack strategies evolve faster than institutional responses or research timelines, some findings may become outdated or lose relevance in subsequent electoral cycles. This temporal limitation is inherent in cybersecurity research and requires that findings be interpreted within their specific timeframes.

Third, scheduling and access to elite participants posed logistical challenges. High-ranking EC officials and cybersecurity experts often operate within constrained timeframes and politically sensitive contexts, especially during election years. Although purposive sampling allowed for the selection of knowledgeable participants, the number and depth of interviews may have been limited by these availability constraints.

Finally, an important limitation to acknowledge is the heavy reliance on internal sources. Perspectives from some external stakeholders, like political party IT representatives, are largely absent from the data. This means the study leans more on the EC's and the government's own accounts of cybersecurity improvements. While this insider view is valuable for understanding institutional intent and self-assessment, it may introduce bias or blind spots, as external critiques or independent validations of the EC's cybersecurity posture are not deeply captured.

Despite these challenges, the longitudinal qualitative design of the study remains robust and appropriate. The triangulation of multiple data sources, combined with the thematic and longitudinal analysis, ensures that the study generates meaningful insights into the institutional evolution of Ghana's electoral cybersecurity landscape.

3.9 Summary

This chapter has presented the philosophical foundation, research approach, design, data collection, and analysis procedures adopted for investigating the cybersecurity instruments and policy frameworks of Ghana's Electoral Commission. By grounding the study in an interpretivist paradigm and employing a qualitative longitudinal design, the research is able to capture the evolving nature of the EC's responses to cybersecurity threats across four election cycles (2012, 2016, 2020, and 2024).

The chosen methodology is particularly well-suited to the research objectives. It allows the study to:

Address Objective 1 by tracing institutional learning and the evolution of cybersecurity frameworks over time.

Address Objective 2 by evaluating the effectiveness of policies and instruments through the perspectives of practitioners and documentary evidence.

Address Objective 3 by identifying gaps and challenges, supported by triangulated data sources.

The strengths of this methodology lie in its ability to integrate diverse forms of evidence, ensure trustworthiness through triangulation, and provide context-sensitive insights that situate cybersecurity within Ghana's electoral governance framework.

The insights generated through this methodological approach will be presented and discussed in detail in the following chapter, which sets out the empirical findings of the study.

CHAPTER 4

FINDINGS, DISCUSSION, AND ANALYSIS

4.1 Introduction to Findings and Thematic Overview

This chapter presents the empirical findings of the study, examining how Ghana's EC has addressed cybersecurity across the 2012, 2016, 2020, and 2024 elections. The results are organized both chronologically and thematically, focusing on tools implemented, challenges, incident responses, and best practices. The analysis applies Nye's theory of power diffusion and Schneier's surveillance/trust frameworks to interpret the findings, particularly the influence of non-state actors, vendors, and external partners, and the need to maintain trust in electoral systems. Evidence from field interviews with EC officials, CSA, CERT-Ghana, civil society, observers, and development partners provides a triangulated perspective. Special attention is given to insider threats, the balance between reactive and proactive measures, and preparations for the 2024 elections. The chapter concludes with preliminary policy insights, including the potential establishment of a permanent EC cybersecurity unit or multi-agency task force to institutionalize cybersecurity efforts beyond election years.

4.2 Evolution of EC Cybersecurity Practices Across Electoral Cycles (2012–2024)

4.2.1 2012: Nascent Use of Technology and Minimal Cybersecurity Focus

The 2012 elections were Ghana's first major foray into biometric voter registration and verification, integrating substantial technology into the electoral process. At the time, the EC's approach to security was primarily reactive and IT-focused, rather than comprehensively cyber-

focused. According to interviewees, during the biometric launch in 2012, the Commission experienced *"serious weaknesses in equipment, network connectivity, and even officer training*." These early issues highlighted the EC's lack of preparedness for cybersecurity; the emphasis remained on manual processes and basic IT troubleshooting rather than anticipating and mitigating cyberattacks.

Indeed, multiple respondents suggested that *"there wasn't much focus on cybersecurity"* around 2012, as the EC was only beginning to grapple with digital systems and did not yet distinguish cybersecurity from general IT concerns. Before 2012, there were no formal cyber risk frameworks in place, and knowledge of the threat posed by risks such as those from cyberspace was low.

In essence, the 2012 cycle exposed an early phase in the EC's cyberspace evolution: technology adoption was underway (biometric voter registration, electronic results transmission pilots, etc.), but cybersecurity policy was embryonic or nonexistent, with the Commission relying on manual backup processes and the inherent security of physical, paper-based voting as its main safeguards.

4.2.2 2016: Wake-Up Call – Cyber Incident and Reactive Measures

The 2016 general elections represented a turning point for cybersecurity awareness at the EC, precipitated by a highly publicized cyber incident. In the midst of the 2016 results transmission, the EC's official website was *hacked and defaced*, causing it to display incorrect results. This breach – later understood to have involved an insider threat within the EC's ranks – forced the Commission to temporarily halt the release of results and revert to manual processes. The incident *"delayed [results] announcements"* and immediately raised suspicions and political tensions about potential manipulation. Notably, the EC leadership at the time (under Chair Charlotte Osei)

publicly cited a cyberattack as the reason for the delay, though Ghana's nascent cybersecurity authorities later assessed that *"nothing like that happened"* – suggesting either a false alarm or miscommunication.

Regardless, the 2016 website defacement was a wake-up call that revealed the EC's vulnerabilities. An expert from civil society observed that *"2016 changed everything"*, spurring the EC to recognize that its assumptions about being secure (for example, believing that reliance on fax machines or offline processes alone guaranteed safety) were *"not very valid"*. In the immediate aftermath, the EC responded in a largely reactive manner: patching the specific vulnerability (the website) and bolstering basic IT controls. CERT-GH, which was founded in 2014, worked with the EC throughout the crisis to provide guidance on how to respond, despite the fact that it had no direct hands-on control over EC systems. This division highlighted a crucial dynamic: the EC maintained control of its infrastructure even during a crisis, with CERT-GH serving as an advisory body and without *"touching their systems."*

Beyond the immediate disaster response, 2016 triggered deeper changes. Interviewees repeatedly cited the 2016 breach as the catalyst for subsequent reforms. According to a respondent from a tech-focused civil society organization, noted that *"2016… was when the EC's approach changed a bit"*, prompting new investments in security between 2016 and 2020. In particular, the EC began upgrading its systems – for example, overhauling the biometric voter equipment and strengthening network safeguards – in direct response to the weaknesses revealed in 2016. This period also saw the EC start to engage (albeit informally) with emerging cybersecurity stakeholders.

For instance, by the late 2010s, external assessments were conducted: a *"Commonwealth…foundation"*-linked expert team evaluated the EC's cyber readiness ahead of 2020 and "was not very impressed", concluding that Ghana's EC remained at a *"very low level"*

of cybersecurity preparedness. The EC's organizational learning from 2016 was thus significant but initially ad hoc – the Commission was learning the hard way that cyber threats were real and could directly disrupt election operations, and it took steps (new tools, seeking advice from CSA/CERT, etc.) largely after the damage was done.

In terms of Nye's power diffusion concept, 2016 illustrated how a single individual or small group (possibly an insider or hacker) could wield outsized influence over a national institution, thereby diffusing power away from the EC's central control. The experience forced the EC to start reallocating power in the cybersecurity domain – for example, by relying more on outside expertise and tools – to prevent future incidents.

4.2.3 2020: Institutionalization – Legal Reforms and System Upgrades

By the 2020 election cycle, Ghana's electoral cybersecurity landscape had evolved further, shaped by both the lessons of 2016 and significant legal/institutional changes. A landmark development was the passage of the Cybersecurity Act, 2020 (Act 1038), which created the CSA and formally designated the EC as one of Ghana's CII owners. According to a CSA official, *"from 2021, when the cybersecurity authority designated the Electoral Commission as a critical infrastructure owner,"* the EC came under new regulatory requirements and oversight.

By requiring compliance audits and reporting and imposing baseline cybersecurity requirements on CIIs, the Act (more specifically, Sections 35–40) essentially institutionalized cybersecurity procedures that were previously optional or nonexistent. Experts referred to this legal change as a *"turning point"* that *"formalized [the] national CERT structures"* and compelled agencies such as the EC to cooperate with the CSA and adopt security standards. To put it briefly, by 2020, the

policy environment had shifted from a vacuum to a defined framework, giving the EC both a "stick" (legal obligations and oversight) and a "carrot" (access to support from CSA/CERT-GH) for cybersecurity.

The EC introduced new procedures and technological advancements during the 2020 elections. The Commission *"did an upgrade of the biometric systems"* before 2020, replacing and updating voter registration kits and verification equipment, according to interviewees. Database management improved, with stricter identity checks (such as integration with the national Ghana Card), enhancing data integrity. These adjustments show a progressively more proactive approach: the EC attempted to strengthen identified vulnerabilities (such as unreliable devices and data quality issues) before the elections rather than waiting for a disaster.

However, the period was also transitional – the new CSA was *"in preparatory stages before the [2020] election"* and not yet fully operational. Thus, coordination between the EC and cybersecurity authorities was nascent in 2020. The Commission's cybersecurity efforts were still developing in a somewhat piecemeal fashion – for example, some simulation exercises or risk assessments were reportedly conducted *"closer to elections"*, but not consistently. On the positive side, by 2020, there was greater awareness within the EC that cybersecurity is distinct from general IT. The Commission sent personnel to CSA-led training and awareness sessions, reflecting a recognition of the need for specialized knowledge (the CSA noted that *"the fact that they [EC staff] would attend [training] means they recognize there's a difference between cybersecurity and IT"*).

External influence, while downplayed by the EC publicly, was nonetheless present: donor and diplomatic actors began highlighting cyber risks in election observer reports, and international knowledge-sharing forums for election commissions included cybersecurity on the agenda. A

European Union (EU) expert mission in 2020, for instance, *"made note of this topic"* in its recommendations. Still, the EU assessment was that the EC's focus on cybersecurity by 2020 was driven *"independently"* and followed a global trend more than direct donor pressure.

In essence, 2020 solidified the structural foundations: the legal framework (Act 1038) and emerging institutional partnerships (EC–CSA linkages) set the stage for a more systematic approach, even if on-the-ground capabilities were still maturing and largely untested by any major new cyber incident in 2020.

4.2.4 2024: Consolidation of Practices and New Threat Landscapes

The 2024 election cycle built upon the changes of 2020, with Ghana entering a campaign period where cybersecurity was recognized as *"one of the prime security challenges"* facing elections. The CSA was completely functional and highly engaged with the EC by 2024. Regular compliance checks and collaboration were being conducted on the EC's systems and processes under the direction of the Critical Information Infrastructure Protection unit of the CSA. According to a senior CSA official, the EC *"responds to us"* on regulatory instructions and *"took measures to make sure their posture is in the right place"* in accordance with national standards and the Cybersecurity Act.

Notably, the EC and CSA collaborated on pre-election cybersecurity preparations, conducting *"cyber activities that the authority engages the EC on before elections"* (such as audits or drills) to improve readiness. The Ghana Police Service has also developed a cybersecurity unit that *"works with the EC,"* indicating a broader multi-agency strategy by 2024. Interviewees reported *"some level of seriousness and collaboration"* in 2024, which was lacking in previous years. For

example, the National Election Security Task Force, which was previously focused on physical security, began to incorporate cyber threat monitoring inputs from agencies and civil society (Penplusbytes provided social media threat alerts to this Task Force and the EC during the election). This indicates a more holistic security posture in 2024, where cyber incidents (like misinformation surges or hacking attempts) were addressed within the broader election security architecture.

At the same time, new threats and challenges emerged or intensified in 2024. The rise of AI-generated misinformation and more sophisticated hacking techniques became a concern: the CSA believed the EC was preparing for such "hybrid" threats through inter-agency collaboration, whereas independent experts cautioned that Ghana was *"just beginning to grapple"* with threats like deepfakes and supply-chain attacks, with preparation *"more awareness than capability"* at this stage.

The geopolitical context also loomed – fears of foreign cyber interference, such as Russian influence operations, were voiced by some observers, though no large-scale external attack materialized in 2024. Rather, the cybersecurity environment was dominated by domestic factors: politically driven social media misinformation campaigns aimed to damage the EC's reputation, continuing a trend in which opposition actors accuse the EC of bias and propagate fraud rumors. Such campaigns in late 2023, according to an EU official, *"aimed to undermine… the validity of the electoral process,"* contributing to a decline in public trust in the EC.

The EC's response in 2024 included more agile public communication – the Commission *"use[d] Twitter… quite a lot to respond to incidents and misinformation"*, countering false narratives in near real-time. Nonetheless, trust issues persisted; surveys showed public confidence in the EC

had eroded compared to earlier decades, a trend the EC struggled to reverse even with better cybersecurity, highlighting a central theme that technical security and public trust are interlinked.

Internally, 2024 also put the EC's compliance with procedures and handling of insider threats to the test. Despite advancements, there was a reported instance during the 2024 process where a staff member was accused of violating protocol: *"some staff was somewhere transferring people's votes."* Even though interviewers did not go into great detail about this incident, it shows that insider threats—whether from carelessness or malevolent intent—were still a problem in 2024. In order to discourage such behavior, it also emphasizes the necessity of more stringent enforcement of staff guidelines and the punishment of infractions.

On a positive note, the absence of any major external cyber-attack in 2024 (no repeat of a website hack, for example) suggests that the EC's preventive measures were at least moderately effective. Several respondents judged the EC's cybersecurity posture by 2024 to be *"effective to a moderate extent"* or *"fairly effective"*, given that no significant disruptions were observed in the conduct of the election. However, experts hastened to add that Ghana's defenses had *"not been fully put to the test"* by a determined adversary.

According to Nye's theory of power diffusion, by 2024, cybersecurity responsibilities had become more decentralized. The EC, CSA, police cyber units, and even civil society watchdogs shared power, demonstrating an acknowledgment that no single entity could secure the election process on its own. Meanwhile, the events surrounding 2024 demonstrate, using Schneier's trust framework, that preserving the credibility of elections requires not only technical precautions but also open communication and reliable oversight to reassure the public that the system has integrity. For example, the EC's prompt responses to false information on Twitter, now X, serve as both a security measure and a trust-building exercise.

In summary, the trajectory from 2012 to 2024 reveals a clear evolution in Ghana's cybersecurity maturity: from negligible attention in 2012, to a rude awakening in 2016, to structural reforms and capacity-building by 2020, and towards a more integrated and collaborative approach in 2024. The next sections delve into the key thematic findings across this timeline – examining the specific tools and practices employed, the major gaps and challenges that persist, the nature of inter-agency and external engagement, and critical areas such as insider threats and public trust – all through the lens of the theoretical frameworks guiding this study.

4.3 Thematic Analysis of Ghana's Electoral Cybersecurity Posture

4.3.1 Cybersecurity Tools, Measures, and Practices Implemented

Across the past four election cycles, the EC has incrementally built up a set of cybersecurity measures and tools. By 2024, the Commission had in place many of the standard technical controls expected in an election management context. Interviewees familiar with the EC's ICT setup indicated that the EC employs controls such as firewalls, IDS, MFA, encryption for data, and endpoint protection on devices. A CSA official similarly believed the EC had deployed these technical safeguards, noting *"they have those in place"* as part of compliance with the national baseline standards for CIIs.

Beyond tools, the EC developed certain policy frameworks and procedures. For instance, an incident handling framework exists (though it is not public), outlining how to manage cyber incidents around elections. The EC has also instituted some form of incident response plan and drills in collaboration with the CSA, especially as elections approach. A CSA representative confirmed that *"there are some cyber activities [exercises]… before elections"* which have *"done*

a great deal to help [the EC] prepare". These likely include simulation exercises or tabletop drills coordinated by CSA to test EC's readiness, although details remain confidential.

Additionally, audits and compliance checks became part of the routine after Act 1038: the EC is subject to audits by the CSA's CII unit, which assesses whether the EC meets the *"Directive for the Protection of Critical Information Infrastructure"* – a baseline cybersecurity framework issued to all critical sectors. The EC has been *"responsive"* to such audits, sending required documentation and addressing advisories from the regulator.

In terms of securing specific electoral systems, the EC's approach has been to blend technology with manual redundancies. The heavy reliance on physical, paper-based processes (e.g., paper ballots, fax or hand delivery of results sheets) is itself considered a deliberate security measure that limits electronic attack surfaces. An international expert pointed out that Ghana's *"very paper-based"* voting and tabulation is *"its own protection"*, since purely digital manipulation is less feasible when final verification occurs with *"paper pink sheets, etc."* at multiple levels. Thus, one could say the EC's "toolkit" includes low-tech defenses (paper trails, air-gapped workflows) alongside more advanced tools.

That said, the EC also maintains critical digital assets, notably the biometric voter register (with ~17 million records) and internal networks at its headquarters and regional offices. To protect the voter database, access controls and data governance measures have been tightened over time – for example, integrating the voter roll with the national ID (Ghana Card) system to verify identities added a layer of data validation and reduced duplicates. The Data Protection Act, 2012, compelled the EC to implement data security measures and limit unnecessary data sharing, effectively treating the voter information as sensitive personal data that must be safeguarded.

By 2024, the EC also reportedly benefitted from continuous monitoring support: the national Security Operations Centre (SOC) run by CERT-Ghana/CSA provided threat intelligence and monitoring during the election period. For instance, during the 2020 and 2024 elections, CSA and CERT-GH helped with *"public awareness campaigns during election seasons"* and monitoring of government networks. The EC's collaboration meant its systems could be plugged into broader government monitoring infrastructure, improving detection capabilities (e.g., alerts for any abnormal traffic to the EC website or databases).

Despite these measures, it is important to note that many tools were introduced incrementally and often in reaction to identified threats. For example, secure backup systems and disaster recovery plans became a focus after the threat of potential data loss or manipulation; yet experts stated that *"resilience planning and disaster recovery drills aren't yet routine"*, suggesting continuity capabilities remain a work in progress.

Penetration testing and external audits have been conducted, but not in a consistent, institutionalized manner. A cybersecurity expert noted that penetration tests are usually done *"closer to elections, but not always consistently or independently,"* and their value depends on whether the EC actually fixes the vulnerabilities found. The lack of continuous, year-round testing means potential security holes might persist across cycles if they emerge in off-election years.

This observation ties into Schneier's emphasis on *"security processes"* over just tools – Ghana's EC had acquired many technical tools by 2024, but the processes to regularly use, test, and update these tools lagged. An insider from civil society encapsulated this by recommending the EC adopt a comprehensive *"framework or strategy… that deals with [cybersecurity] whether elections are happening or not – before, during, and after elections"*, essentially a living security policy that is continuously enforced. Such a framework would ensure that tools (firewalls, IDS, etc.) are not just

installed, but effectively managed through regular training, audits, and updates, even in non-election years.

In essence, Ghana's EC has significantly broadened its cybersecurity instruments over the last decade: it now uses standard technology protections, adheres to national policy guidelines, and benefits from collaborative oversight and support. These precautions most likely contributed to the absence of significant disruptions in recent elections. However, the effective implementation of tools remains uneven; some controls exist on paper or in partial form, and consistent enforcement is a challenge. The findings show that tools alone are insufficient; human factors and institutional practices are equally important, as discussed in the subsequent sections on gaps and challenges.

4.3.2 Gaps and Ongoing Challenges in the EC's Cybersecurity Posture

Despite evident improvement, the study identified numerous gaps, vulnerabilities, and challenges that limit the EC's ability to fully protect the electoral process. These obstacles are institutional, technical, and human in nature, and they frequently overlap with issues in other developing democracies. The key gaps and problems are as follows:

1. **Limited Internal Capacity and Expertise:**

A consistent finding is that the EC lacks a sufficient in-house corps of cybersecurity specialists. Both election experts and technical experts pointed out that *"there aren't enough specialized cybersecurity experts inside the Commission."* The Commission's ICT staff handle general IT operations, but dedicated cybersecurity roles (such as a CISO or cyber analysts) are either absent or too few. This leads to heavy reliance on external vendors and the CSA/CERT for expertise,

which in turn creates dependency risks (discussed further below). One interviewee bluntly stated that the EC would benefit from *"building its own in-house cybersecurity team… [to] respond to incidents and oversee vendors properly,"* because at present *"the balance is tilted more toward external support."*. The CSA also acknowledged this gap indirectly: a representative noted that common challenges for government agencies include *"hiring permanent technical staff"*, implying that the EC may struggle to attract or retain cybersecurity talent on its payroll. Without strong internal expertise, the EC's ability to be proactive is limited – for instance, detection of sophisticated threats remains "patchy," and the EC often *"has to lean on vendors or CSA"* when responding to incidents.

2. **Funding Constraints and Resource Prioritization:**

Funding emerged as a critical challenge that underpins many other issues. The EC's budget is mostly election-centric – it peaks during election years and ebbs in between. Respondents highlighted that *"cybersecurity requires continuous investment,"* yet in Ghana, budget allocations for the EC (especially for IT/cyber needs) are inconsistent. One expert noted the EC *"receives big budgets around elections, but… tends to fade after,"* making it hard to sustain initiatives like regular system upgrades, staff training, or maintenance of security tools. Furthermore, the EC is dependent on government funding approved by Parliament, which can become politicized. A civil society interviewee recalled incidents where Parliament delayed or threatened EC budget approvals due to political tussles, saying *"if [MPs] are not happy, they tend to use [budget approval] against the Commission"*. Such uncertainty in funding complicates long-term planning for cybersecurity improvements. In practical terms, limited funding means some known issues remain unaddressed – e.g., replacing outdated infrastructure. By 2024, there were still complaints that *"all our systems are obsolete, let's go and buy a new one,"* only at the last minute, indicating

a cycle of neglect and last-minute capital expenditures rather than steady upgrades. This reactive procurement pattern not only strains budgets but also opens windows of vulnerability when systems age without proper patching.

3. **Dependency on External Vendors and Supply Chain Risks:**

The EC's reliance on external vendors for key technologies (biometric devices, software systems, data center management, etc.) presents a twofold challenge. First is the risk of dependency and vendor lock-in. If a vendor fails to deliver, or if a technical problem arises, the EC may lack the in-house capacity to fix issues promptly. A cybersecurity expert warned that *"if a vendor introduces vulnerabilities, the EC may not have the in-house knowledge to detect or mitigate it quickly,"* highlighting how outsourcing critical systems can leave the EC blind to embedded risks. Second is the supply-chain security risk: equipment or code sourced from external companies (sometimes overseas) could be compromised or influenced by malicious actors. One interviewee specifically flagged that vendors *"work for other entities and can be influenced… if you are buying from vendors… you are exposed to external people"*, whereas building systems in-house could be safer. The 2020 introduction of new biometric devices, for example, brought concerns about whether those devices had been independently tested for vulnerabilities and whether the contracts allowed the EC full access to audit the software (often, proprietary vendor systems are a "black box"). Several experts recommended improving vendor governance – e.g., by stipulating in contracts for election technology that the EC gets *"source-code access and independent testing"* rights. The current gap is that such stringent requirements have not always been enforced, partly due to the EC's weaker negotiating position and urgency to procure systems before elections.

4. **Fragmented Governance and Inter-Agency Coordination Issues:**

Institutional fragmentation is another challenge; multiple agencies and units have roles in election cybersecurity, but coordination is not yet seamless. The EC must interface with the National Identification Authority (NIA) (for voter registration with the Ghana Card), the National Communications Authority or telecom providers (for results transmission networks), the Data Protection Commission (for personal data oversight), the CSA/CERT (for cyber defense), and security agencies (Police, intelligence) for threat intelligence. One respondent described this as the EC having *"to deal with a lot of institutions… which is fragmented"* – making their work *"quite complicated"* and sometimes leaving gaps where *"they cannot be on top of all issues."* For example, if a cyber threat emerges that involves social media (under NCA jurisdiction) and also impacts voter data (under the Data Protection Commission), it may be unclear who leads the response, unless pre-arranged protocols exist. The Inter-Agency collaboration sub-question is addressed in more detail in section 4.3.3, but in brief, while structures like the Election Security Task Force and CSA-EC collaboration protocols exist, they often rely on goodwill and are not fully mandated or institutionalized. As a civil society expert put it, agencies *"have those structures… but they are not required to [engage]; they can choose to either engage or not,"* resulting in ad hoc cooperation. The lack of a formal joint cybersecurity task force or clear assignment of roles means some threats could fall through bureaucratic cracks.

5. **Reactive Culture and Transparency Deficit:**

Another set of challenges lies in the culture of security management at the EC – historically, the Commission has been reactive rather than proactive, and somewhat secretive about cyber matters. Multiple interviewees observed that the EC typically addresses cybersecurity only when a problem has already occurred or when external pressure (e.g., from political parties or media) is applied.

For instance, the EC did not voluntarily disclose attempted breaches or system weaknesses; as one expert noted, *"they don't do proactive disclosure… they tend to keep that to themselves,"* unless *"political parties start making accusations,"* which force the EC to respond. This reactive communication strategy can undermine trust – it creates a perception that the EC is hiding problems, and it delays public or stakeholder awareness of issues. The transparency gap was also highlighted by observers: domestic civil society has *"been pushing for more openness, like publishing audit results or risk assessments,"* but so far the EC only provides high-level reassurances without technical detail. The EU's election observation noted the EC did improve real-time communications (via social media) during 2024, yet at the same time, some officials felt the EC leadership *"is denying the facts that trust levels are crumbling,"* indicating a reluctance to fully confront and openly discuss the shortcomings. Culturally, there is also a rationale for discretion: cybersecurity is "sensitive", and openly admitting vulnerabilities can invite attacks. The challenge is finding a balance between necessary confidentiality and constructive transparency that can bolster stakeholder confidence. At present, the balance skews towards secrecy, which may impede external support (donors and experts can only help with problems that the EC acknowledges and brings to light) and also slows organizational learning (if issues are swept under the rug, they may recur).

6. **Persistent Technical Vulnerabilities:**

In terms of specific technical weak points, a few stand out from the findings. Endpoint security in the field is one: Ghana's polling process involves thousands of biometric devices and laptops in the field, which an expert described as having *"weak endpoint security at polling stations."* This could include devices not being encrypted, using default passwords, or being susceptible to tampering on election day. Another vulnerability is inconsistent connectivity – Ghana has areas

with limited internet access, leading the EC to use offline methods for transmitting results in those locales. Ironically, this is double-edged: while offline transmission (physical delivery of results) reduces hackable points, the lack of a secure dedicated network forces reliance on ad hoc means (USB drives, etc.), which can be lost or altered if not properly secured. Additionally, monitoring of insider activity was cited as insufficient; the EC might not have robust systems to detect if, for example, an authorized user is accessing data they shouldn't or copying files. Lastly, Ghana's heavy use of social media by the public means disinformation has become a serious vulnerability – while not a technical breach, false information can "undermine trust even if systems remain uncompromised". The EC and security agencies have struggled to stem the tide of viral misinformation, which can spread faster than official facts.

The above gaps illustrate that Ghana's EC is still on a maturity curve in cybersecurity. Many of the issues – limited staff capacity, funding cycles, vendor dependence, coordination, culture – are typical for governmental institutions in developing contexts. They suggest that building a truly resilient electoral cybersecurity posture requires not just adding new tools but addressing these systemic and structural challenges. From Nye's perspective of power diffusion, one can see these challenges partly as a result of distributed responsibilities and influences: e.g., reliance on vendors diffuses power to private companies, while lack of funding can reflect political power struggles affecting the EC. Schneier's framework would emphasize that these gaps, especially around transparency and insider monitoring, erode the trust mechanisms vital for security; if people and processes cannot be trusted (due to lack of training or oversight), technical security will falter. The next section examines how the EC and its partners have been collaborating to overcome some of these challenges, and where those cooperative efforts themselves need strengthening.

4.3.3 Incident Response, Inter-Agency Collaboration, and Proactive vs. Reactive Approaches

Effective cybersecurity for elections is inherently a multi-stakeholder effort. The study found that Ghana's approach to protecting electoral systems has increasingly involved inter-agency and cross-sector collaboration – yet this collaboration is not without its limits. This section discusses how the EC has responded to incidents and the role of collaboration, while also contrasting reactive versus proactive strategies observed.

Incident Response Practices: When cyber incidents or threats have occurred, the EC's immediate responses have typically been collaborative but reactive. The prototypical case is the 2016 website defacement: the EC's ICT team worked in tandem with CERT-Ghana, wherein CERT *"gave directions on what to do… [but did] not directly touch [EC] systems."*. This coordination indicates that by 2016, a channel existed for the EC to call on national cybersecurity resources in a crisis. However, the response was largely ad hoc – essentially a damage control approach (taking the site offline, re-securing it, and reverting to manual count announcements) rather than a pre-planned incident response playbook. Following that experience, there is evidence that the EC, with CSA's guidance, has developed better incident response plans. By 2024, the EC had some form of incident response plan and simulation exercises, as noted earlier. Also, the creation of standard operating procedures for cyber incidents was implied by interviewees referencing *"incident handling frameworks"*. Despite these improvements, one expert assessed the EC's response capacity as limited: often the EC *"has to lean on vendors or CSA for expertise"* during an incident, meaning it may not independently handle complex attacks. Recovery from incidents is another weak area – absent routine drills, *"a major disruption could take longer to resolve than desirable."*. In practice, Ghana has avoided truly catastrophic cyber incidents so far, so the EC's full incident response capability remains unproven. The interviews suggest a cautious optimism that the EC could

manage an incident (given support from CSA/CERT), but also a recognition that a major attack would severely test the system.

Inter-Agency Collaboration: Collaboration between the EC and other agencies – notably the Cyber Security Authority (CSA), CERT-Ghana, security services, and even non-state actors – has improved significantly post-2020, but certain gaps remain. On one hand, officials report generally *"good"* working relations. The CSA's CII Protection lead stated that when the regulator *"asks for collaboration or… compliance efforts, [the EC] respond[s]."*. He rated inter-agency collaboration *"pretty good… maybe not an A-plus but… they try to be efficient."*. A tangible example of collaboration is the joint activities before elections: the CSA and EC have pre-election cybersecurity checklists, and the National Election Security Task Force includes a cyber sub-committee that connects EC officials with law enforcement and intelligence on threat monitoring. Civil society groups like Penplusbytes also became de facto collaborators by feeding real-time information on misinformation or alleged cyber incidents to the EC and police. This multi-sector sharing of information helped the EC respond faster to rumors or emerging threats in 2024, illustrating the benefit of *"joint incident response exercises or clear communication channels"* that experts have called for. On the other hand, collaboration is not yet institutionalized or continuous. A recurring critique is that cooperation peaks in election years and then lapses. As one interviewee put it, *"whether there are elections or not, the EC should be working with [CSA]… but you see, they will wait… when it's election year… it shouldn't be that way."*. This indicates that regular inter-agency meetings or joint operations outside the immediate election period are lacking. The voluntary nature of current collaboration means it depends on personalities and goodwill. For instance, the EC and CSA have an MoU (implicit through the Act), but if EC leadership is resistant, there is no strong enforcement mechanism compelling deep collaboration.

The IDEG expert bluntly noted that the EC's coordination with others *"has so many shortcomings"*, and that *"inter-agency cooperation… does not work that well"* without formal structures. He advocated for *"institutionaliz[ing] the collaboration between the EC and the cybersecurity authority"* via a legal mechanism, so that it isn't left to the whim of a given chairperson.

From an international cooperation viewpoint, the EC has also been part of knowledge networks (e.g., exchanging notes with other election commissions globally), but direct operational collaboration with foreign entities is limited due to sovereignty concerns. The EC has shown some reluctance to accept direct donor assistance on cybersecurity in recent years, preferring to project self-reliance. As noted earlier, donors like the EU have offered help, yet *"the EC wasn't really open to receiving support from donors"* around 2020, in part because the election was fully state-funded and the EC wished to avoid external influence. This stance may reduce the EC's access to cutting-edge expertise that international partners could provide. However, it aligns with the EC's emphasis on independence. The compromise, as evidenced in 2024, is that international actors operate at arm's length: for example, the EU's expert mission observed and reported on cybersecurity issues but *"did not have active collaboration with the EC"* on tech platforms, and instead supported broader initiatives (like funding observer groups or convening dialogues). Thus, the collaboration domain for Ghana's electoral cybersecurity is principally domestic and government-led, supplemented by civil society inputs.

Reactive vs. Proactive Approaches: Over the studied period, a shift from a reactive to a proactive approach is discernible, but not uniformly nor sufficiently, according to participants. Initially, as seen in 2012–2016, the EC was almost entirely reactive – security improvements came after crises or complaints. By 2020–2024, some proactive elements emerged: the introduction of regular

audits, pre-emptive drills, and risk assessments shows foresight. The CSA's insistence on continuous audit cycles… *"before, during and after elections"* aims to bake proactivity into the system. Penplusbytes similarly urged that the EC "ensure continuous assessment of their systems" rather than scrambling every four years. In practice, however, the EC's ingrained culture and resource limitations mean many actions are still event-driven. For instance, the EC often updates security policies when new laws come out or when new threats get media attention, rather than through an internal continuous improvement loop. There is also a tendency to focus on visible, immediate issues (like preventing a recurrence of the exact 2016 website hack scenario) but not on less obvious, long-term risks (like insider espionage, or deeply embedding cybersecurity into procurement processes). The interviews reflect this gap: EC interlocutors would assert that *"we're up to scratch because we collaborate with CSA"*, yet others pointed out that many measures are not institutionalized beyond personalities. For true proactivity, the EC would need to treat cybersecurity as a constant priority. Encouragingly, some of the 2024 developments – such as faster misinformation rebuttals and planning for AI-related threats – show a forward-looking mindset. An EU official acknowledged *"there is quite a bit of emphasis and focus on this topic already"* in Ghana and even recommended the EC further *"test the system… in the off-season"* with rigorous exercises to find latent fragilities. This recommendation for tabletop exercises in non-election years epitomizes the proactive philosophy the EC is being encouraged to adopt.

In summary, Ghana's EC has made progress in developing a collaborative, multi-agency strategy to electoral cybersecurity, and it has begun to shift from a reactive to a more proactive and planned approach. However, to properly achieve a proactive attitude, these collaborations must be formalized (ensuring constant engagement, not only during election times), and the EC must embrace a culture of continuous improvement and early response to cyber risks. According to

Nye's power diffusion theory, because power (knowledge, resources) is diffused across multiple actors, the EC must proactively network with these actors (CSA, CERT, civil society, etc.) to pool their capacities before crises. Schneier's trust framework reminds us that being proactive – transparently preparing and practicing for incidents – will enhance public trust, whereas a purely reactive approach risks public confidence if a surprise incident occurs without an evident plan.

4.3.4 Insider Threats and Internal Security Culture

A prominent theme that emerged is the risk of insider threats and the overall security culture within the EC. "Insider threat" refers to the potential for employees or contractors with authorized access to systems to intentionally or inadvertently compromise security. The Ghanaian experience underscores that while foreign hackers and external attackers capture headlines, insiders can pose equally serious risks if not properly managed.

The 2016 website incident is a case in point: as discussed, evidence pointed to an insider's involvement in that defacement attack. The interview with the CERT-Ghana representative explicitly confirmed that the 2016 breach *"was an insider threat… It came from an insider."*. This revelation is critical – it means that a staff member or someone with privileged credentials facilitated the hack, betraying internal trust. In 2024, again, an example surfaced where *"some staff… transferring people's votes"* outside of proper procedure caused alarm. Although details were scant, it implies a willful act by an insider to manipulate or mishandle electoral data, which constitutes a serious security breach. These incidents highlight a vulnerability that technology alone cannot fix: the human element. If insiders choose to abuse their access or are co-opted by malicious actors, they can bypass or undermine many security measures. As one cybersecurity

expert noted, *"many breaches worldwide start with a single compromised staff account,"* emphasizing that phishing or coercion of insiders is a leading vector for attacks.

How has the EC addressed insider threats? The findings suggest that measures are still inadequate and mostly reactive. There is some recognition of the issue: experts cited *"insufficient monitoring of insider activity"* as a remaining gap. This indicates the EC may not be comprehensively logging or reviewing staff actions on IT systems, or if it does, the analysis of those logs is limited. The CSA did not comment on specific insider controls, which perhaps falls more under the EC's internal purview. Penplusbytes recommended that the EC *"take staff training very seriously"* and enforce strict adherence to protocols, suggesting that a strong security culture can deter insider misbehavior. They further argued that if staff do break cybersecurity protocols, the EC should *"sanction them appropriately to deter others"*. This implies that one way to combat insider threats is through organizational discipline and clear consequences for security violations. Presently, it's unclear if the EC has a formal insider threat program (such as background checks, principle of least privilege in account access, rotation of duties, etc.). The baseline directive for CIIs likely requires role-based access control and periodic user access reviews; however, enforcement details were not shared by the interviewees.

The internal security culture at the EC intersects with the issue of insider threats. A robust security culture means every staff member understands the importance of cybersecurity and their personal responsibility in protecting the system. Historically, the EC's culture was not oriented towards cybersecurity – technology was seen as a tool to use, not a domain where every action has security implications. After 2016, there were efforts to raise internal awareness; for example, CSA's training sessions and the general increase in discourse around cybersecurity would have permeated the EC to some extent. Yet, culture change is slow. One sign of cultural shortcomings is that the

EC tends to treat cybersecurity as an external domain handled by IT specialists or external partners, rather than a daily concern for all staff. For example, phishing awareness among EC staff was not explicitly mentioned, but given global trends, such training would be essential. A single click on a malicious email by a staffer could open the door for attackers. The absence of mention likely means this area needs strengthening.

Applying Schneier's trust lens, insider threats are fundamentally about trust – the EC must decide how much trust to place in its employees and what verification or surveillance of their actions is prudent. Schneier notes that security often involves creating systems such that participants are forced to act in a trustworthy manner, either through oversight or incentives. Currently, the EC appears to operate on a high-trust model internally (perhaps due to institutional independence ethos), with insufficient surveillance of insiders. The downside is obvious: too much unchecked trust can be exploited. However, swinging to the opposite extreme – heavy surveillance of staff – can erode morale and trust in the employer. The EC thus faces a delicate balance. One potential solution raised in interviews is institutional reforms like establishing a permanent cybersecurity unit (discussed in section 4.4), which could include an internal audit or security oversight function. Such a unit, staffed with skilled personnel, could continuously monitor systems for suspicious insider activity and ensure compliance with security protocols.

In conclusion, insider threats remain a potent risk for Ghana's electoral cybersecurity. The 2016 and 2024 incidents serve as warnings that must be heeded. Building a stronger internal security culture – through training, strict protocols, and possibly technological monitoring (like identity management systems, audit trails, and anomaly detection for insider behavior) – is essential. Moreover, addressing insider threats is not only about preventing malice but also honest mistakes: many insiders might inadvertently cause breaches by ignorance. Thus, continuous education is

key. As one interviewee wisely noted, *"human error — whether through poor training or deliberate misconduct — remains a major vulnerability."*. Combating that vulnerability is as important as any firewall or encryption the EC might deploy.

4.3.5 Misinformation, Public Trust, and the Human Factor in Cybersecurity

Beyond technical vulnerabilities, a crucial finding of this research is the role of misinformation and public perception in electoral cybersecurity. In today's interconnected environment, attacks on elections need not target hardware or software; they can target minds and trust. Ghana's recent election cycles illustrate how cyber and information domains merge: false information about election processes or results can undermine legitimacy just as severely as a technical hack.

Interviewees from both domestic and international perspectives highlighted misinformation/disinformation as a significant challenge. The EU elections lead remarked that politically motivated attempts to discredit the EC – often through spreading fake news on social media – were *"quite serious"* and follow a pattern: *"whoever is in the opposition will give the EC a hard time and accuse them of bias."*. This has led to a documented decline in trust: Afrobarometer surveys show that public trust in the EC has fallen compared to 10–20 years ago. From a security standpoint, this is alarming because public trust is the ultimate target of election cybersecurity. As one expert put it, *"if false narratives spread unchecked, they can undermine trust just as much as a hacked system."*.

Ghana's strategy to counter misinformation around elections has involved both the EC's own efforts and multi-stakeholder initiatives. The EC, learning from past lapses, took a more active communication stance in 2020 and 2024. It launched the *"Let the Citizen Know"* initiative in 2020

(alluded to by an interviewee as "let the citizens do" – likely a reference to that program), which gave frequent updates to the public. In 2024, as mentioned, the EC adeptly used social media (Twitter/X) to dispel rumors and provide clarifications in real-time. The EU observers praised the EC's responsiveness on Twitter and suggested they replicate that agility on their official website to reach an even wider audience. Additionally, the National Election Security Task Force's scope was expanded to monitor "information integrity" threats: civil society organizations like Penplusbytes built tools like the *"Disinformation Detecting Platform"* to crawl social media for election-related fake news, feeding alerts to the EC and police. This kind of civil society initiative, in collaboration with the authorities, proved valuable in 2024 to catch and rebut harmful stories quickly. It reflects Schneier's idea of community-driven trust-building: non-governmental actors can hold institutions accountable and supplement their efforts, enhancing overall trust in outcomes.

However, fighting misinformation is inherently reactive, as false content often spreads faster than the truth. Proactively, Ghana has considered legal and educational approaches – for example, CSA's public cyber hygiene campaigns during elections and NCCE's civic education on discerning fake news. But deep-rooted distrust, often fueled by political polarization, is not easily fixed by fact-checking alone. The EU expert's insight that Ghana's concern is mostly *"domestically originated"* misinformation (rather than foreign interference) means it is tied to internal politics. This suggests solutions must also be political and social – building cross-party consensus to refrain from undermining the EC's credibility, and promoting media literacy among the electorate.

From the interviews, it's clear that public trust in the EC's cybersecurity measures is mixed. On one hand, the absence of major hacks and the EC's assurances give some confidence. On the other hand, opposition narratives and past glitches fuel skepticism. The EC has attempted to demonstrate

transparency at times – for instance, when accusations flew about the voter register quality in 2020, the EC *"came out with a fairly structured and public response, which was data-driven"* to defend itself. Such actions likely prevented misinformation from festering. Yet, the Commission could institutionalize transparency further. A strong recommendation from experts was to introduce credible oversight and public reporting: for example, *"mandate independent audits and make the results public"* so that observers and the public can be assured of the systems' integrity. This has *"not been institutionalized yet,"* but if it were, it could significantly improve trust. Oversight bodies exist on paper (Parliament, Data Protection Commission, CSA as regulator), but they seldom publicly scrutinize the EC's cyber readiness in between elections. Strengthening those mechanisms (perhaps a requirement for the EC to report cybersecurity status annually to Parliament or a multi-agency board) could enforce both better practice and public accountability.

It is also pertinent to connect this discussion to Schneier's trust and security framework more explicitly. Schneier posits that security is ultimately about maintaining trust in systems – people follow rules and use systems because they trust them to work properly and fairly. If that trust erodes, the system (democracy, in this case) suffers even if no technical failure occurs. Ghana's scenario exemplifies this: even with secure tech, if a large portion of the populace believes the EC's systems are rigged or compromised (perhaps due to viral disinformation), the election's legitimacy is in jeopardy. Therefore, the EC's cybersecurity strategy must encompass public communications and transparency as core components, not as afterthoughts. The cybersecurity expert interviewee echoed this, concluding that *"technical defenses can fail, but if institutions are transparent, resilient, and responsive, public confidence can be preserved"* – and that *"the ultimate goal… is not perfection, but trustworthiness."*. This insight neatly ties the human factor back into the concept of security: the end-goal is to ensure stakeholders (voters, parties, observers)

trust that the election outcome is valid. That trust is built through both preventing incidents and convincingly demonstrating readiness and honesty about challenges.

In conclusion, misinformation and public trust issues form a critical frontier of electoral cybersecurity for Ghana. The EC and its partners have taken steps to counter misinformation through rapid response and collaborative monitoring, yielding some success in recent elections. Yet, to fortify public trust long-term, more systematic transparency and education are needed. In a way, Ghana must secure not just its ICT infrastructure but also the "information space" around elections. Doing so will involve ongoing adaptation, as new forms of disinformation (deepfakes, AI-generated lies) emerge in future cycles. The findings here underscore that cybersecurity is as much social and institutional as it is technical, aligning strongly with the theoretical perspective that security measures must foster trust at the societal level to truly safeguard democratic processes.

4.4 Theoretical Reflections: Power Diffusion and Trust in Ghana's Electoral Cybersecurity

Having presented the key findings, it is useful to explicitly interpret how the Electoral Commission's evolving behavior reflects both concrete institutional changes and also through the lens of the study's theoretical frameworks – Joseph Nye's theory of power diffusion in the digital age and Bruce Schneier's surveillance and trust frameworks.

Over the 2012–2024 period, the EC underwent an institutional transformation in its approach to cybersecurity. Early on, the EC's posture was ad hoc and reactive; for instance, in 2012, there was minimal formal cybersecurity policy, and the introduction of biometric voting devices was fraught with improvisation. When devices failed in 2012, "street-level" adaptations by polling staff filled

the gap (for example, reverting to manual voter checks), but those well-intended discretionary actions later opened the door for losing parties to allege manipulation. This highlights how implementation at the front lines can shape outcomes: individual EC officers exercising discretion under pressure sometimes deviated from ideal protocols, affecting the perceived integrity of the process.

By contrast, in subsequent cycles the EC gradually institutionalized more standardized responses, a shift indicative of organizational learning. A civil society expert noted that *"2016 changed everything"*, spurring the EC to recognize its prior complacency and invest in stronger security measures. Indeed, the 2016 website defacement and related incidents became a catalyst for reform: after that wake-up call, the EC upgraded its biometric systems, strengthened network defenses, and started engaging (informally at first) with cybersecurity stakeholders. By 2020, this evolution was codified in institutional policy. The passage of the Cybersecurity Act 2020 (Act 1038) formally designated the EC as a Critical Information Infrastructure operator and subjected it to mandatory audits and standards for the first time. In other words, what had been optional security measures became obligatory – a clear sign of institutional transformation. The EC moved from a siloed approach to being embedded in a national cybersecurity framework, marking a shift from insular decision-making to regulated, coordinated governance of electoral IT systems. Concrete examples from the data illustrate this transformation: the EC's reluctance before 2016 to seek outside help gave way to active cooperation with agencies like the Cyber Security Authority (CSA) and CERT-GH after 2020, and one interviewee observed that the Commission even began consulting peers in other countries to learn best practices. These changes in behavior, from reactive patching of problems to proactive planning and collaboration, underscore an organization adapting

its structures and culture in response to environmental pressures. They reflect a growing institutional maturity in the EC's cybersecurity governance over the four election cycles studied.

Despite these high-level changes, the street-level implementation of cybersecurity within the EC has varied across electoral cycles, affecting policy outcomes. Frontline EC staff (registration officials, polling officers, district IT personnel, etc.) are the "street-level bureaucrats" of election cybersecurity, and their discretion can either bolster or undermine the formal measures in place. The 2012 biometric rollout exemplified this: many poll workers were insufficiently prepared for device failures and had to devise on-the-spot solutions, introducing inconsistencies. By 2016 and 2020, training had improved somewhat – the EC, for example, sent staff to CSA-led cybersecurity awareness sessions ahead of 2020 – yet interviews suggest that implementation gaps persisted. One recurring theme was uneven compliance with security protocols at the operational level. Stakeholders noted uneven enforcement of rules and a continued reliance on individual initiative. A civil society respondent recommended that the EC *"take staff training very seriously"* and enforce strict adherence to protocols, underscoring that a strong security culture is crucial to counter insider risks. Indeed, building a cybersecurity mindset among all staff has been slow. Even by 2024, the EC tended to treat cybersecurity as the domain of IT specialists or external partners, rather than a daily concern of every employee. This cultural lag means that at the street level, some security measures are applied inconsistently or left to personal discretion, which can create vulnerabilities. For instance, if a regional officer bypasses a password policy for convenience, or if polling staff neglect a new verification step under pressure, the overall defense is only as strong as its weakest link. Thus, the human factor at the implementation level emerged as a double-edged sword: staff initiative and improvisation kept elections running during technical glitches (as in 2012), but a lack of uniform practice also created opportunities for security lapses and reduced

trust. The data across cycles indicate gradual improvement (for example, more training and awareness by 2020) but also highlight that policy intentions often outpace practice on the ground. Recognizing this, recent efforts by the EC and its partners have focused on standardizing procedures and incentivizing compliance (such as calls to sanction staff who flout cyber protocols), aiming to limit the variability introduced by street-level discretion. In sum, the EC's cybersecurity readiness has not only been a matter of acquiring technology and drafting rules, but also of influencing the everyday behaviors of its personnel. Sustained progress will require institutionalizing a security-conscious culture so that the de facto implementation of measures aligns with their de jure design across all levels of the Commission.

It is also instructive to place Ghana's experience in a regional context, comparing the EC's trajectory with other West African electoral bodies. Ghana is not alone in facing rapidly evolving digital threats to elections, and lessons can be drawn in both directions. Notably, Nigeria's Independent National Electoral Commission (INEC) has grappled with similar challenges on an even larger scale. During Nigeria's 2023 general elections, for example, officials reported an onslaught of nearly 13 million cyberattacks against election-related systems, including aggressive attempts to breach INEC servers on polling day. Nigerian authorities responded by activating a coordinated, multi-agency cybersecurity task force that successfully blocked or neutralized these attacks in real time (Izuaka, 2023). This outcome underscores the importance of robust inter-agency collaboration and advanced monitoring capabilities – an area where Ghana's EC has been making strides but still has ground to cover. Compared to INEC, Ghana's EC operates on a smaller scale and has not publicly faced a single concentrated cyber onslaught of that magnitude. However, the potential for such threats looms, and the proactive measures taken by INEC provide a benchmark. For instance, Nigeria established dedicated cybersecurity operation centers and

response teams between 2020 and 2023 to guard election infrastructure. Ghana's EC, by 2024, was moving in a similar direction by liaising more closely with the CSA and national CERT, but these efforts remain nascent.

A direct comparison reveals both the commonalities and differences: both Ghana and Nigeria have recognized election cybersecurity as critical to legitimate outcomes and have passed national cyber laws (Act 1038 in Ghana; Nigeria's cybersecurity initiatives under its Digital Economy Policy) to empower defenses. Both have also introduced biometric and electronic result technologies that demand new security protocols. Yet, while INEC in 2023 leveraged a surge capacity of multi-agency experts to protect the vote (essentially a short-term "cyber war room"), Ghana's EC has thus far leaned on periodic support and has called for a more permanent solution (like an Election Cybersecurity Task Force) to institutionalize such collaboration. Regionally, other electoral commissions, from Liberia to Sierra Leone, are also watching these developments. Ghana's experience contributes to a growing West African body of knowledge on election tech: for instance, the difficulties Ghana faced with biometric verification in 2012 and the subsequent improvements by 2020 can inform neighbors embarking on similar upgrades. Conversely, Nigeria's handling of large-scale digital threats highlights best practices (and perhaps the political will and resources required) that Ghana can emulate. In summary, contextualizing Ghana's EC against peers like INEC demonstrates that security challenges are shared, but responses vary in execution. Ghana appears to be charting a middle path, learning from incidents and gradually bolstering its framework, whereas Nigeria's recent experience shows a more forceful, centralized defense against cyber threats. This comparative lens reinforces the idea that Ghana's ongoing reforms (for example, closer inter-agency ties, better funding for cybersecurity) are not just internally driven but part of a broader regional trend toward fortifying electoral integrity in the

digital age. It also adds weight to calls for Ghana's EC to accelerate certain measures (like 24/7 network monitoring during elections) to keep pace with emerging threats witnessed in neighboring states.

Beyond the region, Ghana's progress can be measured against international standards and best practices in election cybersecurity. Organizations such as the U.S. National Institute of Standards and Technology (NIST), the International Foundation for Electoral Systems (IFES), and USAID have developed frameworks to guide electoral bodies in protecting their digital assets. Ghana's evolving framework aligns partially with these global benchmarks, though gaps remain. For example, NIST has outlined an Election Infrastructure Security Framework (NISTIR 8310) that provides a risk-based approach tailored for election administrators, emphasizing core functions like identifying critical assets, protecting them with appropriate controls, detecting incidents promptly, and having plans to respond and recover in case of attacks. By 2024, the EC had made headway in the "identify" and "protect" stages: it now formally falls under the "Critical Infrastructure" category per Act 1038, meaning critical electoral systems are inventoried and subject to baseline protections. Measures such as strengthened access controls on voter databases and the use of data encryption for results transmission were noted improvements, which echo NIST's recommended safeguards. However, in the "detect", "respond", and "recover" dimensions, Ghana is still developing capacity. The study found that continuous network monitoring and incident response drills were not yet routine, and that post-incident recovery protocols (such as comprehensive backup and restore testing) were only beginning to be fleshed out. This is an area where NIST's framework – and experiences from countries with more mature systems – suggest the EC should focus next.

Similarly, best-practice guidelines from IFES and USAID advocate a layered, proactive defense and a strong security governance process for election management bodies. IFES, often in partnership with USAID, has stressed that as elections become more digitized, EMBs must complement technical safeguards with rigorous policies and human-focused measures. Recommendations include affordable but effective steps: regular software patching of election IT systems, continuous cybersecurity training for staff, multi-factor authentication for sensitive systems, and well-drilled incident response plans. Ghana's EC has started to implement some of these. For instance, by 2020, it introduced two-factor authentication for its new biometric verification devices and database systems, and it established basic incident reporting lines with the national CERT. These steps are in line with IFES/USAID guidance that emphasizes controlling access and preparing for contingencies.

Additionally, interviewees noted that the EC has begun to schedule more frequent security audits and "table-top" simulation exercises (albeit mostly close to election time), reflecting an uptake of international best practices in testing systems before they fail. Crucially, though, the EC still lacks a dedicated cybersecurity unit and does not yet conduct year-round training and penetration testing – practices recommended by bodies like IFES as essential for maintaining readiness. The absence of fully independent external audits (and the fact that internal assessments are often kept confidential) is another gap when compared to the transparency encouraged by global standards. Publishing audit summaries or inviting third-party evaluators could both improve security and build public trust, as seen in international cases. In summary, Ghana's electoral cybersecurity posture by 2024 shows incremental convergence with international best practices: the fundamentals are being put in place, and there is awareness of what an ideal, standards-aligned framework looks like, but several advanced measures (continuous monitoring, comprehensive

training programs, public accountability mechanisms) are still maturing. A positive sign is that the EC has expressed openness to "do what works for your country" while learning from others – indicating a willingness to adapt global recommendations to local context, which will be key in closing the remaining gaps.

Turning to the study's theoretical frameworks, these lenses help interpret the above developments by illuminating the broader dynamics at play. Joseph Nye's concept of power diffusion in cyberspace and Bruce Schneier's trust-versus-surveillance model both offer insight into Ghana's electoral cybersecurity evolution, without resorting to abstraction beyond what the evidence supports.

Power Diffusion (Nye): Nye's concept of cyber power diffusion suggests that power in the realm of cybersecurity is not concentrated solely in state authorities; instead, it is distributed among a wide array of actors – from individuals (hackers, insiders) to non-state groups (companies, civil society) to international players. The findings from Ghana strongly reflect this diffusion of power. The EC, as the statutory body managing elections, found that it cannot unilaterally control all aspects of electoral cybersecurity. For instance, a lone insider or small hacking group in 2016 managed to disrupt the EC's operations and narrative (albeit briefly), demonstrating how a traditionally less powerful actor can exert outsized influence – a hallmark of power diffusion in cyberspace. Similarly, political disinformation campaigns orchestrated by opposition activists or social media influencers chipped away at the EC's authority and public trust. On the positive side, power diffusion is seen where the EC has had to share responsibility and cooperate with other entities to achieve security: it relies on tech vendors for equipment (shifting some power to the private sector), on the CSA and CERT-GH for expertise and incident response (empowering these agencies in the election context), and on civil society for monitoring information space. A donor

representative observed that the EC *"consults quite a bit with election commissions in other countries"* to learn best practices – again acknowledging that knowledge and ideas flow across borders, rather than emanating top-down from the EC. Even Ghana's strategy of keeping some processes manual (paper-based) can be interpreted as avoiding over-centralization of digital power; by not fully digitizing, the EC prevents a scenario where a single cyber incident could seize nationwide control (in effect, power remains diffused across thousands of polling stations via paper ballots).

The interplay of these actors exemplifies Nye's assertion that state actors must act as nodes in a network rather than sole controllers. The EC's relative reluctance to accept donor support in recent elections adds nuance: it shows the EC attempting to reclaim or retain power (to protect its independence) in a diffused environment, perhaps to a fault. The research suggests that a more effective approach is embracing managed interdependence – e.g., establishing a *"multi-agency task force"* or permanent coordinating body would formally acknowledge that securing elections is a shared power endeavor, aligning incentives and information among key actors. The IDEG interviewee's call to *"institutionalize the collaboration"* via legal mechanisms is essentially a call to create a stable power-sharing arrangement among EC, CSA, security agencies, etc., instead of ad hoc diffusion. In summary, Ghana's case validates that power in electoral cybersecurity is indeed diffuse. The EC's evolution – from initially trying to handle issues internally (pre-2016) to now engaging multiple stakeholders – illustrates a shift towards recognizing and leveraging diffused power (though there remains room to formalize these networks).

Schneier's Surveillance/Trust Frameworks: Schneier's work often contrasts security approaches based on surveillance and enforcement with those based on trust and transparency. In Ghana's electoral cybersecurity, this dichotomy can be seen in how the EC manages its relationships with

stakeholders and the public. On one hand, certain security measures align with a "surveillance" approach: for example, the CSA's role as a regulator conducting audits and requiring compliance reports is a form of oversight (or institutional surveillance) ensuring the EC behaves securely. The idea of installing monitoring tools to catch insider misuse is also a surveillance-oriented defense. These are necessary controls – they compel actors to act in a trustworthy manner by the threat of detection and sanction. However, an over-reliance on secrecy and surveillance can backfire if it undermines trust. The EC's tendency to be opaque about its cybersecurity issues is perhaps rooted in a surveillance mindset – i.e., *"we will manage security internally and not divulge anything, to maintain control"*. Yet this has led to criticisms of a lack of transparency and possibly fueled conspiracy theories, which harm trust. Schneier would argue that transparency, when carefully balanced, can strengthen security by enlisting the broader community's trust and cooperation.

We see attempts at a "trust-based" framework emerging: by publishing data-driven responses to allegations or quickly correcting misinformation on official channels, the EC builds trust with the public. The recommendation that independent audits be published is quintessentially trust-building – it would show the EC has nothing to hide and is accountable. The ultimate form of trust framework is when the public and all stakeholders have confidence in the system's integrity and therefore comply willingly with the rules (e.g., accepting election results even if their side loses, because they trust the process). Ghana is striving for this: peaceful transfers of power in 2016 and 2020 indicate a baseline of trust in the electoral system, but the downward trend in trust metrics is a warning sign. If not addressed, no amount of technical security could save the day – an election could be perfectly secure yet politically rejected by a mistrustful populace. The human factor programs (like civic education on misinformation, engaging with political parties through IPAC on cybersecurity topics) are efforts to mend and bolster this trust. Schneier's perspective also

reminds us that over-surveilling insiders or treating everyone as a potential threat can degrade trust internally, which can be counterproductive. Thus, the EC must cultivate an internal culture of trust but verify – staff should feel trusted to do their jobs, yet know that systems are in place to catch breaches and that ethical behavior is expected and rewarded.

In conclusion, applying these theoretical lenses to Ghana's case underscores the following insights: (1) Power in securing elections is distributed, so the EC must function collaboratively and cannot succeed in isolation – a reality that has driven many of the changes observed by 2024. (2) Trust is both an objective and a tool in cybersecurity – the EC needs the trust of the public and partners to effectively secure elections, and it must also design its security governance in ways that promote trust (through transparency, accountability) instead of solely relying on secrecy or top-down control. These insights reinforce why some of the upcoming recommendations (Chapter 5) emphasize multi-agency structures (reflecting power diffusion) and transparency/continuous engagement (fostering trust).

4.5 Preliminary Policy Insights and Conclusion of Findings

Drawing together the above findings and analysis, several policy-relevant insights emerge as preliminaries to the formal recommendations in the next chapter:

Need for Institutionalized Cybersecurity Structures: The EC would benefit from creating a permanent cybersecurity unit or committee dedicated to election security. This could be an internal unit within the EC – a team of specialists maintaining year-round vigilance – and/or a multi-agency task force that operates continuously (not just in election years), bringing together EC, CSA, CERT, police, and perhaps private sector experts. The research consistently pointed to

fragmentation and episodic collaboration as weak links. A formal structure, backed by policy or legislation, could close this gap. Such a body could enforce the institutional memory of 2016's lessons and 2020's new standards, ensuring that knowledge isn't lost with staff rotations or leadership changes. It aligns with interviewees' suggestions to *"institutionalize the collaboration"* and ensure the EC does not only rely on personal initiative for security cooperation.

Balancing Independence and Cooperation: Ghana's EC highly values its independence, an essential principle for credible elections. However, cybersecurity is one area where strategic cooperation does not necessarily impinge on independence but rather can safeguard it. The insights suggest the EC should not view accepting help (technical or financial) as a loss of autonomy. Instead, wisely leveraging donor offers (for training or systems, under EC control) and peer learning can strengthen its capacity. The EC's move to fund elections fully from government sources in 2020 was politically understandable, but cyber expertise can be welcomed in other forms. The policy insight here is to develop clear guidelines for external engagement: e.g., creating a framework where international best practices are reviewed and possibly adopted by the EC in a way that fits local context (as one expert said, *"do what works for your country"* while still learning from others).

Continuous Capacity Building and Testing: A major insight is that cybersecurity must be a continuous effort, not a periodic campaign. The EC should institute regular training, audits, and drills as part of its standard operating procedures. The idea of conducting off-season tabletop exercises or red-team simulations came up repeatedly. This is a proactive measure to test the system under controlled conditions and learn from any discovered weaknesses without the high stakes of an actual election at risk. Additionally, capacity building isn't just technical – it's also about process. For example, ensuring knowledge transfer from outgoing IT staff to new ones,

maintaining updated documentation of systems, and scenario planning for new threats (like a sudden ransomware attack on voter data). The findings show that Ghana's preparedness is "moderate" and somewhat untested, which implies a need to drill and improve before a real adversary tests it in a potentially more damaging way.

Enhanced Transparency and Public Engagement: Another insight is that trust-building measures should be integrated into the EC's cybersecurity policy. This could mean regularly communicating with stakeholders about steps taken to secure systems (without revealing sensitive details that would aid attackers). It also means involving political parties and civil society in cybersecurity dialogues – for instance, briefing them on election tech changes or inviting them to observe parts of the cybersecurity preparedness process. The IPAC (Inter-Party Advisory Committee) could have a sub-committee on technology security. As noted, the EC did defend itself with data publicly when under criticism; making that more routine (e.g., publishing a post-election cybersecurity report) can strengthen public confidence. The interviews underscore that when people see the EC being forthright and responsive, it helps counteract misinformation. Therefore, a policy insight is to institutionalize accountability mechanisms – such as mandatory reporting of cyber incidents to a parliamentary committee and disclosure of how they were handled, which is currently limited.

Focus on Insider Threat Management: Internally, the EC should develop clear policies and controls for insider threats. This includes vetting processes, least-privilege access principles (no one person should have unchecked access to critical systems), and monitoring and audit logs to detect unusual access patterns. Furthermore, fostering a culture where staff understand why these measures exist – not as an affront to their integrity, but as protection of the national interest – is key. Insight from incidents indicates that human failures or malfeasance can be as dangerous as

external attacks, so any forthcoming policy reform (for example, if the EC were to update its internal IT usage policies or code of conduct) should emphasize cybersecurity responsibilities of staff and penalties for violations.

In conclusion, Chapter 4 has detailed the trajectory and current state of Ghana's Electoral Commission cybersecurity efforts, revealing significant improvements over the past decade as well as persistent challenges. The EC has moved from an arguably naive position in 2012 to a more aware and structured stance by 2024, aided by national policies and collaboration. Yet, the environment of threats is evolving, and the Commission's approaches must continue to adapt. The critical analysis using Nye's and Schneier's frameworks has shown that broad trends like the diffusion of power and the centrality of trust are highly relevant in this context – Ghana's experience is a microcosm of global shifts in how technology and society interact around elections. The findings here set the stage for the final chapter, which will propose concrete recommendations to reinforce Ghana's electoral cybersecurity, ensuring that future elections are not only technically secure but also command the confidence of all stakeholders.

CHAPTER 5

SUMMARY OF FINDINGS, CONCLUSIONS, AND RECOMMENDATIONS

5.1 Reiterating the Research Problem and Key Insights

This study set out to examine how Ghana's Electoral Commission has developed and implemented cybersecurity policies over time to protect the integrity of elections. The research problem centered on identifying the progress made, the gaps that remain, and how theoretical concepts of power diffusion and trust manifest in this domain. Through Chapters 2 and 4, we saw that election management bodies worldwide face growing cyber threats, and Ghana's EC is no exception. Chapter 4 in particular presented detailed findings across the 2012–2024 electoral cycles, highlighting both achievements (e.g., legal reforms, improved collaboration, and adoption of security tools) and ongoing vulnerabilities (e.g., insider threats, resource constraints, and public trust deficits).

Summarizing the key insights from Chapter 4: Ghana's EC has evolved from a largely reactive stance on cybersecurity (especially before and immediately after the 2016 incident) to a more structured approach by 2024, underpinned by the Cybersecurity Act 2020 and partnerships with the Cyber Security Authority. The Commission has embraced various technical safeguards and has shown increased awareness of threats such as misinformation. However, the EC's cybersecurity framework is still maturing – it suffers from limited in-house expertise, inconsistent funding, heavy reliance on external vendors, and a need for stronger continuous collaboration and transparency. Critically, the analysis revealed that technical measures alone are insufficient; institutional and human factors (like insider vigilance, staff capacity, and public communication) are equally pivotal. Nye's theory of power diffusion illuminated how securing elections is a multi-

actor endeavor, not solely under the EC's command, while Schneier's trust framework emphasized that preserving public trust is as important as patching software vulnerabilities.

In essence, the research problem – how to strengthen electoral cybersecurity holistically – was addressed by uncovering where Ghana's EC stands now. The findings serve as a basis to inform both scholarly understanding and practical interventions. Scholarly-wise, this study contributes by offering a longitudinal perspective on cybersecurity in an electoral context within a developing democracy, applying international relations and security theories to a real-world case. Practically, it surfaces concrete areas for improvement that Ghana's policymakers, the EC itself, and supporting organizations can act upon. The remainder of this chapter will outline specific recommendations in three domains: technical measures, policy initiatives, and capacity-building efforts. These proposals are aimed at consolidating the gains made so far and addressing the identified gaps, with the ultimate goal of ensuring that future Ghanaian elections are resilient against cyber threats and maintain public trust.

5.2 Contributions of the Study

Before delving into recommendations, it is important to highlight the contributions this study makes to both scholarship and practice:

Scholarly Contribution: This research adds to the academic literature on cybersecurity governance in election management. It provides an in-depth case study of Ghana, informed by empirical data (interviews and documents), thus enriching theoretical discussions of how global cyber norms and frameworks (like those by Nye and Schneier) apply in a Sub-Saharan African context. The longitudinal approach (2012–2024) offers insights into how changes in technology,

law, and threat landscape influence institutional behavior over time. Few studies have documented election cybersecurity evolution in a developing country with the granularity presented here; thus, this thesis helps fill a gap by combining theoretical analysis with field data. It also underscores the interdisciplinarity of the subject, bridging political science (e.g., power dynamics, institutional independence) with information security (technical controls, standards like ISO 27001). Future researchers can build on this work to compare Ghana with other countries or to delve deeper into specific aspects like misinformation or insider threat modeling in electoral contexts.

Practical Contribution: For practitioners – including the EC, the Cyber Security Authority, government policymakers, and civil society organizations – this study provides a diagnostic assessment of Ghana's electoral cybersecurity posture. The thematic findings highlight what is working (such as the legal framework compliance) and what needs urgent attention (such as establishing continuous cybersecurity roles and routines). By capturing the voices of various stakeholders (EC officials, cybersecurity experts, observers, etc.), the research synthesizes a 360-degree view that can inform more inclusive policy development. The analysis offers justification for recommendations that align with both local insights and international best practices. For example, the call for regular penetration testing and independent audits is backed by interview evidence that current testing is ad hoc and by international standards (ISO 27001) that emphasize continuous improvement. As such, the study's recommendations are not abstract ideals but grounded proposals responding to documented needs. Additionally, the discussion on trust and communication could help electoral management bodies in Ghana and beyond recognize the often underappreciated "soft" aspects of cybersecurity – managing information and public perception.

In summary, this study's contributions lie in advancing academic knowledge on a timely issue and offering actionable insights to those directly involved in safeguarding elections. With these

contributions in mind, we now transition to detailed recommendations organized under technical, policy, and capacity-building categories. Each set of recommendations is designed to be concrete, achievable, and aligned with international standards (including ISO 27001 and other relevant benchmarks) to ensure that Ghana's electoral cybersecurity measures are on par with global best practices.

5.3 Technical Recommendations

1. **Implement Regular Penetration Testing and Red-Team Exercises:** The EC should institutionalize a schedule of penetration tests on its critical systems (voter registration database, results transmission system, public website, etc.) at least annually, and before every major election event. These tests should be conducted by independent, certified experts (potentially through CSA's accreditation or external consultants) to provide an unbiased assessment. Equally important is to perform red-team simulations, where a group mimics attackers trying to breach the EC's systems or processes. Such simulations should test not only technical defenses but also the EC staff's detection and response. Crucially, the findings from each test must be promptly addressed – vulnerabilities patched, misconfigurations fixed, and lessons learned documented. This proactive approach aligns with the recommendation from both local experts and international observers to *"really test the system in the off-season"*. By making penetration testing a routine (rather than a one-off reactive measure), the EC will consistently improve its security posture and reduce the risk of surprise attacks during actual elections.

2. **Strengthen Network and Endpoint Security (Zero-Trust Architecture):** The EC should move towards a zero-trust security framework for its IT infrastructure. In practice, this means verifying every user and device each time they access resources, segmenting networks, and enforcing strict access controls. Concrete steps include deploying updated intrusion detection and prevention systems (IDPS) that cover both the central EC network and extend, where feasible, to regional offices and even field devices. All endpoints (e.g., biometric verification devices, laptops used in collation centers) should be secured with modern endpoint protection platforms and, if possible, unified under a central monitoring system (such as a Security Information and Event Management – SIEM – tool for real-time alerting). Multi-factor authentication (MFA) should be mandatory for all sensitive systems – for example, when EC officials access the voter database or upload results, they should use MFA to mitigate credential theft risks. Adopting a zero-trust model is recommended by cybersecurity experts and is in line with international best practices, ensuring that even if one node is compromised, an attacker cannot easily move laterally through EC systems.

3. **Encrypt and Backup Critical Data with Resilience in Mind:** The EC must ensure that all sensitive data (voter register, tally databases, communications) is encrypted at rest and in transit. Modern encryption standards should be employed, with proper key management (keys stored securely, rotated periodically). Additionally, a robust backup and disaster recovery system is needed. Backups of critical systems should be done regularly (with offline copies stored securely to protect against ransomware). The EC should explore maintaining a real-time redundant system (or at least a hot standby) for the results management system during elections, so that if one system fails or is attacked, a backup can take over with minimal downtime. Regular drills on data restoration should be

conducted to ensure backups are viable. Given an expert's observation that *"resilience planning and disaster recovery drills aren't yet routine"*, making them routine is imperative. An international standard like ISO 27001 emphasizes backup, redundancy, and availability as key controls, so these steps would also move the EC toward compliance with such standards.

4. **Deploy Advanced Monitoring and Incident Response Tools:** To improve real-time detection of threats, the EC (in collaboration with CSA) should deploy advanced monitoring tools. This includes expanding the use of a Security Operations Center (SOC) approach during election periods, where logs from EC systems are fed into a central analytic platform under heightened scrutiny. Machine learning-based anomaly detection could help flag unusual patterns, such as an insider querying the database at odd hours or an unexpected surge of traffic on the website (possibly indicating a DDoS attempt). In addition, the EC should invest in digital forensics capabilities – either internal or accessible via CERT-Ghana – to investigate incidents swiftly and determine root causes. Having forensic tools and trained personnel means that if a breach or suspicious activity occurs, the EC can contain and analyze it effectively, preserving evidence and learning from it. A cybersecurity expert recommended *"invest in digital forensics and incident response capacity within the EC"*, underlining that tools are useless without people ready to use them under pressure. Therefore, tool deployment goes hand-in-hand with staff training (addressed in capacity-building).

5. **Audit and Secure the Supply Chain of Election Technology:** Technically securing elections also means ensuring that the hardware and software procured from vendors are free from known vulnerabilities and malicious implants. The EC should establish a practice

of supply chain security audits. This involves vetting vendors for their cybersecurity practices, requiring vulnerability assessments on devices/software before acceptance, and possibly engaging third-party code reviewers for critical software (especially if source code can be obtained in escrow). Contracts should include clauses that mandate vendors adhere to cybersecurity standards and support the EC in patching any issues. As suggested in the findings, *"audit their supply chains… make sure there are no leaks"*. For example, if the EC buys biometric devices, it should verify firmware checksums, disable any unnecessary functionalities, and ensure secure configuration from the start. Partnering with CSA's technical teams could be helpful here, as they might assist in evaluating the security of products. Ensuring the integrity of the supply chain is consistent with ISO 27001's control set, which addresses supplier relationships and security in development/acquisition. By tightening technical control over what enters the EC's ecosystem, the risk of backdoors or exploitable flaws introduced via vendors is reduced.

Collectively, these technical recommendations will bolster the EC's defenses against cyber attacks. They emphasize not only acquiring technology but using it systematically – aligning with a defense-in-depth strategy. Importantly, these measures should be documented in the EC's technical guidelines and reviewed regularly for effectiveness, possibly with the involvement of external experts or an advisory group on election tech security.

5.4 Policy Recommendations

1. **Integrate and Enforce Act 1038 Provisions within EC Operations:** Ghana's Cybersecurity Act (Act 1038) provides a strong legal foundation, but the EC should take

further steps to internalize those requirements into its own policies. This can start with the EC developing a Cybersecurity Policy Handbook that explicitly references Act 1038 obligations – for example, obligations to report certain incidents to the CSA, to implement the Directive for Critical Information Infrastructure Protection, and to appoint a liaison for cybersecurity. The EC should designate a high-ranking official (or unit) responsible for compliance with Act 1038, essentially serving as the EC's Chief Information Security Officer (CISO) function if one doesn't formally exist. By embedding these legal provisions into everyday workflow (e.g., requiring cybersecurity risk assessments as part of any new electoral technology deployment, as implied by the law), the EC ensures legal compliance is not just on paper. Moreover, incident reporting protocols should be clearly defined: what constitutes a notifiable incident, how quickly it must be reported to CSA/CERT, and who has the authority to do so. During the research, it was noted that communication about cyber incidents was often delayed or kept internal. Reforming incident reporting to be more timely (even internally and to oversight bodies) will enable better support and transparency. Essentially, the EC's internal policies should mirror national law, making Act 1038 a living document within the Commission.

2. **Establish a Permanent Multi-Agency Electoral Cybersecurity Task Force:** As a policy measure, Ghana should formalize the coordination between the EC and other key actors through either legislation or an executive instrument. This could be the creation of a National Election Cybersecurity Coordination Center or task force, mandated to operate continuously (not just in election year). Its composition should include representatives from the EC, CSA, CERT-Ghana, Ministry of Communications and Digitalisation, National Security, and perhaps liaisons from civil society (in advisory roles). The task force

would develop joint plans, conduct regular inter-agency drills, and ensure that roles and responsibilities are clear in the event of an election-related cyber incident. This addresses the collaboration gaps identified (where cooperation was ad hoc). Such a body could be modeled after the existing National Election Security Task Force but focusing on cyber and information security. If needed, an amendment to the electoral law or a new regulation can codify this group's authority and scope. The benefit is twofold: it institutionalizes information-sharing (preventing scenarios where agencies are siloed) and it signals high-level commitment to electoral cybersecurity. In times of heightened threat, this task force can rapidly convene to coordinate defensive measures or responses, something that interviewees hinted was lacking in past cycles. This policy essentially aims to hardwire collaboration into the system, aligning with Nye's observation that diffused power requires networked governance.

3. **Mandate Cybersecurity Audits and Certifications for EC Systems (Aligning with ISO 27001):** The government or the EC's governing board should mandate that the EC undergo annual independent cybersecurity audits of its critical systems and processes. These audits, perhaps conducted by the Auditor-General's IT audit unit in conjunction with the CSA, should evaluate the EC against international standards like ISO 27001 or the NIST Cybersecurity Framework. The results of these audits should feed into actionable plans, and a summary (non-sensitive) version of the audit findings should be made available to oversight bodies or even the public to build confidence. Additionally, the EC could pursue ISO 27001 certification for its information security management. While resource-intensive, obtaining such certification for at least the IT Department of the EC would formalize security processes (asset management, access control, incident management,

etc.) and subject the EC to regular external review. This aligns with the CSA official's recommendation that institutions adopt *"internationally best recognized frameworks like ISO 27001."*. Over a reasonable timeline (e.g., 2-3 years), the EC can work towards meeting all ISO requirements, which would dramatically professionalize its cybersecurity posture. Policy support might be needed, such as budgetary allocations for this certification process and perhaps technical assistance from development partners who often support capacity-building in such areas.

4. **Reform Cyber Incident Disclosure and Communication Policies:** Building on transparency needs, a formal policy should be introduced regarding how the EC communicates about cyber incidents or significant cybersecurity measures. This could be an internal policy with external effect: for example, if a cyber incident occurs (even an attempt that was thwarted), the EC policy could be to issue a brief statement to the public or at least to stakeholders like political parties within a defined timeframe. This is not to alarm the public, but to pre-empt rumors and demonstrate control. The content can be carefully managed (e.g., "Attempted intrusion detected and mitigated, no impact on systems, under investigation"). Such candor, practiced judiciously, would counteract misinformation that thrives on secrecy. Additionally, the EC can institute a regular "Cybersecurity Preparedness Briefing" ahead of each general election, where it outlines to the media and stakeholders what measures have been taken to secure the election. This idea is supported by civil society calls for more openness. Policy-wise, the EC may collaborate with the Ministry of Information to ensure these communications are done responsibly. Over time, if the public becomes used to the EC talking about cybersecurity in a factual, non-alarming manner, it will increase general literacy on the issue and trust that the EC is

on top of things. Reforms in this area guard against the vacuum that conspiracy theories often fill – a trend noted where lack of info led to accusations and distrust.

5. **Review and Enhance Legal Penalties and Deterrence for Electoral Cyber Offenses:** While Ghana's laws (Act 1038 and others) criminalize cyber offenses, it may be worth reviewing whether they adequately cover election-specific cybercrimes and whether enforcement is effective. The EC, in partnership with the Attorney General's Department, should advocate for any needed legal refinements – for instance, explicitly outlawing unauthorized access to election systems by insiders (breach of trust) or imposing stiffer penalties during election periods to deter attacks aimed at disrupting polls. Moreover, the prosecution of the 2016 website hacker (if identified) or any 2024 insider malfeasance should be publicized to serve as a deterrent. Deterrence is partly a policy stance: making it clear that anyone (be it a staff member, external hacker, or political actor) who attempts to subvert the electoral process through digital means will face serious consequences. This complements the technical defenses by reducing the motivation to attack in the first place. Additionally, legal reform could consider establishing clear authority for the EC to take pre-emptive action against misinformation – e.g., working with courts to swiftly issue takedown orders for demonstrably false content that threatens public order during elections. Of course, this must be balanced with freedom of expression rights, but a narrowly tailored legal tool could be explored.

In summary, the policy recommendations aim to create a supportive governance framework around the EC's cybersecurity efforts. They ensure that rules, mandates, and organizational structures are in place to reinforce what technical measures accomplish, and to embed best practices (like ISO standards and multi-agency cooperation) into the official modus operandi of election management.

5.5 Capacity-Building and Organizational Recommendations

1. **Develop and Train a Dedicated Cybersecurity Team within the EC:** One of the clearest needs is for the EC to boost its internal human capacity on cybersecurity. The EC should create positions for a dedicated cybersecurity team – even a small unit of 3-5 specialists to start with – whose full-time job is managing and improving cybersecurity. This team would be responsible for tasks like continuous risk assessment, maintaining security configurations, coordinating with CSA/CERT, and training other staff. To make this effective, the EC must invest in capacity-building for these individuals: sending them to advanced training (such as Certified Information Systems Security Professional – CISSP courses, or specialized trainings offered by organizations like ECOWAS or international election bodies), and facilitating peer-learning exchanges with cybersecurity units in other countries' election commissions. Several interviewees stressed the current staffing gap – this recommendation addresses that directly. Over time, this team could grow and possibly evolve into the recommended permanent cybersecurity unit for the EC. It's also worth considering secondments or fellowships: for example, inviting a CSA officer to be embedded in the EC during election years, and vice versa, to cross-pollinate skills. Building in-house capacity will reduce over-reliance on vendors and external actors, giving the EC more control and agility in responding to issues.

2. **Continuous Professional Development and Certification for EC IT Staff:** Beyond the core cyber team, all EC IT staff (national and regional) should undergo regular training to keep skills updated. This includes training on secure system administration, database security, network defense, and also emerging areas like handling AI-driven threats. The EC could partner with the Cyber Security Authority's training programs or leverage

initiatives by bodies like ISACA Ghana. A structured professional development path could be established: for instance, require that each IT staff member completes at least one cybersecurity certification (even entry-level ones like CompTIA Security+ or ISO 27001 Foundation) within a certain timeframe. Encourage higher-level certifications for senior personnel. By professionalizing the workforce, the EC not only improves security but also contributes to job satisfaction and retention (staff feel their skills are being invested in). Capacity-building also has a policy angle: the EC should advocate for budget allocations earmarked for training, highlighting that continuous training was a recommendation to address dynamic threat landscapes (a limitation noted in this study). We saw from interviews that *"continuous training"* was advised as a way to ensure cybersecurity improvement doesn't stagnate after elections. Therefore, making training continuous and mandatory is key.

3. **Conduct Regular Tabletop Simulations and Joint Exercises:** In collaboration with CSA, CERT-GH, and security agencies, the EC should hold tabletop simulation exercises, perhaps every year or every six months. These simulations would be scenario-based discussions/plays of potential incidents – for example, "24 hours before polls, a ransomware attack encrypts the voter register – what do we do?" or "On results day, deepfake audio of the EC Chair announcing false results goes viral – how do we respond?". By involving all relevant parties (technical teams, communications officers, leadership), these exercises help identify gaps in incident response plans, clarify roles, and improve coordination. As noted by an EU expert, such an exercise *"to create a big threat and see how… in the off-season… [the EC and others] respond"* would help *"identify the fragilities"*. These should be followed by debriefs and action items to fix any shortcomings

discovered. Additionally, more hands-on drills can be conducted: for instance, an unannounced drill where CERT-Ghana might simulate a DDoS on the EC's test website to gauge response. These activities build muscle memory and prevent complacency. They are capacity-building in that they elevate the skill and preparedness of everyone involved. Importantly, including regional EC offices in some drills can ensure preparedness is nationwide, not just at HQ.

4. **Enhance Collaboration with Academic and Civil Society Experts:** Ghana has a growing pool of cybersecurity academics and civic tech organizations (e.g., university researchers in computer security, think tanks like Imani, NGOs like Penplusbytes). The EC should tap into this local expertise through periodic consultations, workshops, or even advisory committees. For example, convene a semi-annual "Electoral Technology Roundtable" where EC officials meet with external experts to discuss new threats and brainstorm solutions. Civil society can often provide innovative ideas and act as a bridge to the public. The study showed that civil society was already helping monitor misinformation and advocating for certain improvements. Embracing their input more formally could aid capacity-building – EC staff can learn from tech community insights on the latest vulnerabilities or tools. Additionally, collaboration with academic institutions (e.g., internships for computer science students at the EC's IT department, or research partnerships to develop custom security solutions for the EC) can be a cost-effective way to build capacity. International development partners could support such initiatives by funding fellowships or technical assistance. Ultimately, fostering a community of practice around electoral cybersecurity in Ghana will ensure that the EC is not alone in capacity-building – it can draw on a broader reservoir of knowledge.

5. **Build Public Capacity through Voter Education on Cyber Awareness:** While this recommendation goes slightly beyond the EC's internal capacity, it is relevant to the capacity of the overall system to resist certain threats like disinformation. The EC, in partnership with the National Commission for Civic Education (NCCE) and civil society, should integrate cybersecurity awareness into voter education programs. For example, educating the public on how election results will be transmitted and announced through official channels can reduce the impact of fake results circulating online. Teaching citizens basic skills to verify information (like checking the EC's official website or social media for confirmations) is also crucial. When the public is more cyber-aware, it becomes harder for malicious actors to exploit ignorance. This study pointed out the issue of misinformation and the decline of trust; improving the public's understanding of EC's processes and what is or isn't possible (e.g., clarifying that the voting machines are not connected to the internet, if that's the case, so they can't be hacked remotely) can pre-empt false narratives. Therefore, expanding the scope of capacity-building to include resilience of the electorate's mindset forms a comprehensive approach.

These capacity-building recommendations focus on strengthening the human and organizational elements of cybersecurity. They recognize that technology and policy alone will not succeed without skilled people and a culture of security. By implementing these, the EC can cultivate a sustainable internal capability and a supportive external environment, ensuring that improvements are maintained and updated as threats evolve.

5.6 Alignment with International Standards and Best Practices

It is worth explicitly noting how the above recommendations align with international standards such as ISO/IEC 27001 (Information Security Management) and other best practices frameworks:

ISO 27001 Alignment: This standard requires organizations to systematically manage sensitive data by implementing an Information Security Management System (ISMS). Recommendations like regular risk assessments (penetration testing), access control (MFA, least privilege), physical and environmental security (not directly covered here, but relevant for data centers where servers are kept), incident management (drills, reporting), and compliance (legal requirements) are all mapped in ISO 27001 controls. For instance, Section A.12 of ISO 27001 covers operations security – our technical recommendations on monitoring, backup, malware protection fit here. Section A.16 covers incident management – our suggestions on incident response planning, tabletop exercises, and reporting match these controls. By pursuing these recommendations, the EC is inherently moving towards ISO compliance, which in turn could be formalized by seeking certification as mentioned.

NIST Cybersecurity Framework: This widely used framework organizes activities into Identify, Protect, Detect, Respond, and Recover. Our recommendations span all these: Identify (audits, risk assessments, supply chain security checks), Protect (access controls, encryption, patches, vendor governance), Detect (SOC monitoring, anomaly detection), Respond (incident response team, drills, communications policy), Recover (backups, recovery plans). The emphasis on continuous improvement and feedback loops is integral to NIST and is reflected in our iterative drills and audit cycles. So, the EC's plan moving forward could be explicitly structured around NIST functions, which many governments find accessible.

Election-Specific Guidelines: Bodies like the International Foundation for Electoral Systems (IFES) and the European Union have issued guidelines on election cybersecurity. Common recommendations include creating crisis committees, having backup paper processes (which Ghana already does as a strength), and engaging stakeholders transparently. Our recommendation for a multi-agency task force and communication strategy aligns well with such guidelines. Moreover, global best practice encourages parallel testing of results (Ghana's civil society does PVT as noted, which is good) and ensuring an independent audit trail – something the paper ballots provide, but the digital systems also need integrity verification (hence calls for independent audits, source code access, etc.). Aligning with these practices ensures Ghana remains ahead among peers – as one interviewee noted, *"Ghana is ahead of many of its peers but has a long way to go to meet international best practice."* The recommendations precisely aim to cover that "long way."

By aligning with international standards, the EC not only improves security but also can demonstrate assurance to both domestic stakeholders and international observers. Achieving something like ISO 27001 certification, for example, would be a strong signal that the EC manages information systematically and is externally audited, thereby boosting confidence in its operations. Additionally, alignment means the EC can benefit from global resources – templates, training materials, and even funding (donors often support projects that implement recognized standards).

In conclusion, the recommendations are not operating in a vacuum; they are interwoven with tried-and-tested frameworks that have been adopted by organizations worldwide. Ghana's EC can adapt these to local realities, but the core principles of these standards – risk-based approach, continuous improvement, broad stakeholder involvement, and documented processes – should underpin the EC's roadmap for cybersecurity enhancement.

5.7 Limitations of the Study

While this study has provided comprehensive insights, it is important to acknowledge its limitations:

Access Constraints and Potential Bias: One limitation was access to information. Cybersecurity, especially in the electoral context, is a sensitive topic. Some information may have been withheld by interviewees due to confidentiality (as noted in the CERT-GH interview where the expert said providing certain details would be "misleading… because it is [the EC's] constituency"). This means there might be gaps in the data regarding the EC's most up-to-date internal measures or undisclosed incidents. Additionally, since the research relied on voluntary interviews, there is a possibility of response bias: officials might portray their agency in a favorable light or downplay issues. Conversely, civil society or opposition-leaning informants might emphasize problems. The researcher mitigated this by triangulating multiple sources, but some bias could still influence the findings.

Dynamic Threat Landscape: The cybersecurity field evolves rapidly. What was true during data collection (up to late 2024) might have changed by the time of writing or reading this thesis. New threats such as novel malware or attack techniques can emerge, and the EC's security posture might improve or degrade with new developments (e.g., if a major project to upgrade systems is undertaken, or conversely if budget cuts occur). Therefore, some findings, especially regarding preparedness for emerging threats like AI-generated fake news, are time-sensitive. This study is a snapshot; the dynamic nature of cyber threats means that recommendations will require updating and continuous monitoring for relevance.

Generalisability: This research is focused on one country's context, which has specific institutional arrangements and political culture. While the findings have relevance for similar electoral commissions, caution should be taken in generalizing to all contexts. Ghana's relatively peaceful political environment and established institutions might differ from countries with more volatile settings, which could affect how cybersecurity measures play out. Thus, while theoretical insights (like power diffusion) are broadly applicable, practical recommendations might need adaptation elsewhere.

Scope of Technical Analysis: Due to the qualitative methodology and available access, the study did not include hands-on technical auditing of the EC's systems (no penetration testing was performed by the researcher, for instance). The analysis of technical measures is therefore based on reported information rather than direct verification. There is a chance that some technical details were misunderstood or not fully revealed in interviews. A more technical audit could complement this study, but was outside its scope.

Election-Specific Factors: Elections are periodic and influenced by context (e.g., the stakes of a particular election, the candidates involved). The study covered four election cycles, which gives a good longitudinal view, but each election had unique circumstances. For instance, 2016 was a hotly contested election with a new technology introduction (transmission system) and saw a cyber incident; 2020 was conducted during the COVID-19 pandemic, which this study didn't deeply cover in terms of its impact on operations; 2024 had a former president vs incumbent scenario, which might heighten certain types of threats. Not every nuance of each election's political context could be included, yet these contexts can influence cybersecurity (like targeted attacks from certain interest groups in one year but not another). This complexity is a limitation in drawing universal conclusions even from the Ghana case itself.

By recognizing these limitations, the study remains transparent about what confidence readers can have in the findings. Despite limitations, the triangulated and theory-informed approach gives a strong degree of credibility to the core conclusions. Future research, as will be discussed next, can address some of these gaps by using different methods or an extended scope.

5.8 Suggestions for Future Research

Building on this study, several avenues for future inquiry emerge:

Comparative Electoral Cybersecurity Studies: A comparative study between Ghana and other countries (for example, Nigeria or Kenya in Africa, or India, or even Western democracies) would be valuable. This could validate which challenges are universal and which are context-specific. A comparative lens could also explore how differing institutional designs (independent commission vs. government-run elections) influence cybersecurity approaches. Such research can leverage the framework developed here and apply it elsewhere, contributing to a more global theory of electoral cybersecurity management.

Quantitative Risk Modeling: Future research could introduce quantitative methods, such as developing a risk model for electoral cybersecurity. This might involve creating metrics for various factors (number of attempted attacks per election, time to detect/respond to incidents, budget allocated to cybersecurity, trust index from surveys, etc.) and using mathematical modeling or simulations to predict outcomes (for instance, what is the probability of a significant disruption given current measures?). Mathematical modeling could also be applied to assess the impact of specific interventions (e.g., how much does adding an extra IT auditor reduce risk in a probabilistic

sense?). This would complement the qualitative findings with numerical analysis, aiding resource prioritization.

Public Trust and Cybersecurity Perception Studies: Given the importance of trust highlighted, future researchers might conduct surveys or focus groups with the Ghanaian public to gauge perceptions of electoral cybersecurity. What does the average voter believe about the security of the voting process? Do reports of hacking (even if false) affect their confidence? Such studies could tie into communication strategies: testing which messages or information increase public understanding and which might inadvertently cause alarm. It intersects psychology, communications, and security. Afrobarometer data was cited qualitatively; more granular research here could track how cybersecurity improvements (or incidents) correlate with public trust over time, providing empirical backing to the trust discussions.

Insider Threat Mitigation Strategies in Electoral Bodies: A focused study on insider threats in election commissions, possibly comparing different organizational cultures or technologies used (like role-based access systems, surveillance cameras in data centers, etc.), would be useful. Since our research identified insider issues, a deep dive could involve case studies of insider incidents (in Ghana or elsewhere) and what measures effectively prevented or caught them. This might entail interviews with former insiders, ethical hackers, or managers in charge of internal audits. It could result in a tailored framework for election bodies on how to balance trust and monitoring internally – something not extensively covered in literature yet.

Impact of New Technologies (AI, Blockchain) on Electoral Security: Looking ahead, emerging technologies will influence elections. Future studies could examine how AI might both threaten and aid electoral security (e.g., AI-generated disinformation vs. AI for detecting anomalies). Also, proposals like blockchain-based voting or result transmission have been floated internationally,

researching their viability and security implications in the Ghanaian context would be timely, as the country explores digital innovations. Understanding whether these technologies diffuse power further or concentrate it, and how they affect trust, would link back to the theories used here.

In essence, there is a rich scope to extend the work begun in this thesis. The intersection of cybersecurity and elections will only grow in importance, and Ghana provides a fertile ground for innovative research, given its status as a stable democracy adopting new technologies. Future inquiries, especially those that incorporate both technical assessments and social science perspectives, will be crucial for developing holistic solutions.

5.9 Conclusion

In concluding this thesis, we return to the fundamental issue at hand: safeguarding the integrity of elections in the digital age. Ghana's journey over the past decade, as dissected in this study, reflects a broader narrative of adaptation – a traditional electoral institution coming to grips with modern threats. The Electoral Commission of Ghana has made commendable strides: from virtually no cyber focus to establishing collaborative mechanisms with cybersecurity authorities and upgrading its systems. Yet, this journey is far from over. The 2024 elections, relatively successful in cyber terms, should not breed complacency but rather motivate the EC and stakeholders to institutionalize and deepen those successes.

The recommendations put forth provide a roadmap for strengthening technical defenses, policy frameworks, and human capacity. Implementing them will require commitment and resources, but the cost of inaction could be far higher – measured not just in monetary terms or system downtime, but in the erosion of public trust and the stability of the nation's democracy. A key message of this

research is that cybersecurity in elections is not merely an IT issue; it is a governance issue, a people issue, and ultimately a trust issue.

By establishing a permanent cybersecurity unit or multi-agency task force, Ghana can ensure that knowledge and vigilance persist between elections, not just during crises. By conducting regular audits, drills, and transparency initiatives, the EC can create a culture of continuous improvement and openness, countering both technical threats and malicious narratives. And by investing in its people – training staff, collaborating with experts – the EC can reduce its dependence on external actors and respond to challenges with agility and confidence.

In theoretical terms, Ghana's case has illustrated Nye's power diffusion: power over election security is shared among state, non-state, local, and international actors, and success lies in harnessing that network. It has also illustrated Schneier's wisdom that security is about trust: the ultimate victory in electoral cybersecurity is when the public, regardless of political affiliation, trusts the process and outcome because they are secure and transparently so. The hope and expectation are that Ghana will continue to lead by example among its peers, showing that a developing democracy can proactively adapt to the cyber era while maintaining the fundamental principles of fairness, transparency, and sovereignty in its elections.

As Ghana moves toward future elections – 2028, 2032, and beyond – the recommendations and insights here should be revisited and updated. Cyber threats will evolve, but with a solid foundation and a forward-looking strategy, Ghana's Electoral Commission can remain a resilient pillar of the country's democracy. The conclusion of this study is therefore not an endpoint but a call to action: to translate analysis into implementation, and knowledge into practice, ensuring that the power of technology is harnessed to strengthen, not undermine, the voice of the people.

REFERENCES

Access Now. (2020). *Biometric technologies in elections: Risks and policy recommendations*. https://www.accessnow.org

Adams, C.N. (2024, April 19). Ghana: Cyber Security Authority engages tech providers to counter misinformation powered by AI. *Ghanaian Times*. Retrieved from https://allafrica.com/stories/202404190236.html

Adu-Amanfoh, K., & Allen, N. D. F. (2023). Learning from Ghana's multistakeholder approach to cyber security. Africa Center for Strategic Studies. Retrieved from https://africacenter.org/spotlight/ghana-multistakeholder-cyber-security/

Africa Center for Strategic Studies. (2022, March 8). Ghana's multistakeholder approach to cybersecurity. Africa Center for Strategic Studies Spotlight.

Akata Pore, D. A. (2024, May 29). Protecting our elections in cybersphere: EC alone cannot ensure the security and integrity of our elections. *MyJoyOnline*. https://www.myjoyonline.com/protecting-our-elections-in-cybersphere-ec-alone-cannot-ensure-the-security-and-integrity-of-our-elections/

Amoah, M. (2020). Sleight is right: Cyber control as a new battleground for African elections. *African Affairs, 119*(474), 68–89.

Baker, A., & Osei-Tutu, J. (2019). Cyber Threats and Institutional Preparedness in Ghana. *KAIPTC Policy Brief, 11*(3), 1–8.

BBC News. (2016, December 8). Ghana elections: Fake results claim as votes counted. https://www.bbc.com/news/world-africa-38247987

Bendiek, A., & Metzger, T. (2019). *Digital election interference: Threats and responses* (SWP Research Paper 2019/RP 10). Stiftung Wissenschaft und Politik.

Bendiek, A., & Schulze, M. (2019). *Disinformation and elections to the European Parliament.* (SWP Comment No. 16/2019). Stiftung Wissenschaft und Politik. https://doi.org/10.18449/2019C16

Botchwey, G. (2018). E-governance and cybersecurity: User perceptions of data integrity and protection in Ghana. In 5th Biennial Social Science Conference of the University of Education, Winneba, Ghana.

Brady, M., Howell, G., Franklin, J. M., Sames, C., Schneider, M., Snyder, J., & Weitzel, D. (2024). *Cybersecurity framework election infrastructure profile* (NIST VTS 200-1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.VTS.200-1

Brown, I., Marsden, C. T., Lee, J., & Veale, M. (2020). Cybersecurity for elections. In *Cybersecurity for elections: A Commonwealth guide on best practice*. Commonwealth Secretariat. https://doi.org/10.14217/e56e4289-en

Bund, J. (2016). *Cybersecurity and democracy: Hacking, leaking and voting*. European Union Institute for Security Studies, 1–5. https://www.jstor.org/stable/resrep06791

Cheeseman, N., Lynch, G., & Willis, J. (2018). Digital dilemmas: The unintended consequences of election technology. *Democratization, 25*(8), 1397–1418.

Cheng, Q., Cunningham, C., Gacayan, F., Gu, A., Hall, A., Lee, O., … & Yi, J. (2018). *Hacking democracy: Cybersecurity and global election interference*.

Cybersecurity Act, 2020 (Act 1038). (2020). Retrieved from https://csdsafrica.org/wp-content/uploads/2021/08/Cybersecurity-Act-2020-Act-1038.pdf

Data Protection Act, 2012 (Act 843). (2012). Retrieved from https://nita.gov.gh/wp-content/uploads/2017/12/Data-Protection-Act-2012-Act-843.pdf

Debrah, E., Effah, J., & Owusu-Mensah, I. (2019). Does the use of a biometric system guarantee an acceptable election's outcome? Evidence from Ghana's 2012 election. *African Studies, 78*(3), 347–369. https://doi.org/10.1080/00020184.2018.1519335

DLA Piper. (n.d.). Data protection officers in Ghana. DLA Piper Data Protection Laws of the World. https://www.dlapiperdataprotection.com/?c=GH&t=data-protection-officers

Dorpenyo, I. K. (2019). Risky election, vulnerable technology: Localizing biometric use in elections for the sake of justice. *Technical Communication Quarterly, 28*(4), 361–375.

Dorpenyo, I. K. (2020). *User localization strategies in the face of technological breakdown*. Switzerland: Palgrave Macmillan–Springer Nature.

Dorpenyo, I. K. (2019). Biometric technology: The savior of a risky electoral system. In *User localization strategies in the face of technological breakdown: Biometric in Ghana's elections* (pp. 37–52). Cham: Springer International Publishing.

Effah, J., & Debrah, E. (2018). Biometric technology for voter identification: The experience in Ghana. *The Information Society, 34*(2), 104–113. https://doi.org/10.1080/01972243.2017.1414720

E-Governance Knowledge Hub. (2023). African countries e-gov challenges & solutions. E-Governance Knowledge Hub.

Ehin, P., Solvak, M, Willemson, J., & Vinkel, P. (2022). Internet voting in Estonia 2005–2019: Evidence from eleven elections. *Government Information Quarterly, 39*(4), 101718.

El País. (2024, December 7). Un ejército de verificadores de datos para luchar contra la desinformación electoral en Ghana. https://elpais.com/planeta-futuro/2024-12-07/un-ejercito-de-verificadores-de-datos-para-luchar-contra-la-desinformacion-electoral-en-ghana.html

Election Commission of India. (2020). *Annual report on election technology*. Government of India.

Electoral Commission Act, 1993 (Act 451). (1993). Retrieved from https://judicial.gov.gh/jsweb/index.php/jsg-services/libraryservices/statute-on-elections/388-electoral-commission-act-1993-act-451

Electoral Commission of Ghana. (2023). *Presentation by Mrs. Jean Mensa* (4th ed.). https://ec.gov.gh/wp-content/uploads/2023/03/PRESENTATION-BY-MRS-JEAN-MENSA.pdf

EU EOM Ghana. (2020). *Final report: Ghana presidential and parliamentary elections 2020*. European Union Election Observation Mission. https://www.eods.eu/library/eu-eom-ghana-2020-final-report_en.pdf

Fidler, D. P. (2022). Transforming election cybersecurity. Council on Foreign Relations.

Gadasu, E. K. (2023). Election 2024: Using technology to curb political disinformation and misinformation on social media. Institute of ICT Professionals Ghana. Retrieved from

https://iipgh.org/election-2024-using-technology-to-curb-political-disinformation-and-misinformation-on-social-media/

Garnett, H. A., & James, T. S. (2020). Cyber Elections in the Digital Age: Threats and Opportunities of Technology for Electoral Integrity. *Election Law Journal: Rules, Politics, and Policy, 19*(2), 111–126. https://doi.org/10.1089/elj.2020.0633

Ghana News Agency. (2024, October 3). Ghana launches National Cybersecurity Policy and Strategy. https://gna.org.gh/2024/10/ghana-launches-national-cybersecurity-policy-and-strategy/

Ghanaian Times. (2024a, December 5). Election alert: Cyber Security Authority engages tech providers to counter misinformation powered by AI. Retrieved from https://ghanaiantimes.com.gh

Ghanaian Times. (2024b, April 21). NCA, CSA vow to work together to develop safe cyber security. https://ghanaiantimes.com.gh/nca-csa-vow-to-work-together-to-develop-safe-cyber-security/

GhanaToday. (2024, September 16). CSA urges Electoral Commission to address misinformation ahead of 2024 elections. https://ghanatoday.gov.gh/sector-news/communications-and-digitalisation/csa-urges-electoral-commission-to-address-misinformation-ahead-of-2024-elections/

Government of Ghana. (2020). Cybersecurity Act, 2020 (Act 1038). Accra: Ministry of Communications.

Howell, G., Brady, M., Snyder, J., Weitzel, D., Schneider, M., Sames, C., & Franklin, J. (2024). *Cybersecurity Framework Election Infrastructure Profile* (NIST VTS 200-1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.VTS.200-1

Hsu, C.-L., Lee, J.-N., & Straub, D. W. (2012). Institutional influences on information systems security innovations. *Information Systems Research, 23*(3), 918–939.

IMANI Africa. (2021). *Evaluation of Ghana's 2020 Elections*. https://imaniafrica.org/wp-content/uploads/2021/01/Evaluation-of-2020-Elections.pdf

International Foundation for Electoral Systems (IFES). (2022). *Biometric voter registration and cybersecurity: Emerging threats in developing democracies*. https://www.ifes.org

International Foundation for Electoral Systems (IFES). (2023a). *Cybersecurity and voter registration [Briefing paper]*. IFES. https://www.ifes.org/sites/default/files/2023-06/Briefing_Paper_Cybersecurity_and_Voter_Registration.pdf

International Foundation for Electoral Systems (IFES). (2023b). *Cybersecurity in elections: Models of interagency collaboration.* IFES. https://www.idea.int/sites/default/files/publications/cybersecurity-in-elections-models-of-interagency-collaboration.pdf

International Foundation for Electoral Systems (IFES). (2023c). *Understanding cybersecurity throughout the electoral process.* IFES. https://www.ifes.org/sites/default/files/2023-06/Understanding-Cybersecurity-Throughout-the-Electoral-Process_1.pdf

International Institute for Democracy and Electoral Assistance (IDEA). (2020). *Electoral risk management tools in West Africa*.

https://www.idea.int/sites/default/files/publications/electoral-risk-management-tools-in-west-africa.pdf

Izuaka, M. (2023, March 15). Nigeria recorded 12.9 million cyber attacks during presidential, NASS elections – minister. *Premium Times*. https://www.premiumtimesng.com/business/business-news/587712-nigeria-recorded-12-9-million-cyber-attacks-during-presidential-nass-elections-minister.html

Jacobsen, K. L. (2020). Biometric voter registration: A new modality of democracy assistance?. *Cooperation and Conflict, 55*(1), 127–148.

Jonathan, S., Sanusi, S. A., Akinbola, T. E., & Nwankwo, E. G. (2024). *Information ecosystem ahead of Ghana's 2024 elections*. CJID.

Judicial Service of Ghana. (2024). *Election Manual* (4th ed.). https://judicial.gov.gh/jsfiles/election_manuel_4th_edition.pdf

Kersting, N. (2019). Cyber interference in elections: Lessons from Kenya and beyond. *Electoral Studies, 60*, 102050.

Kolog, E. A., & Tijani, M. (2023). Implementing the Cyber Security Act in public financial institutions in Ghana: What are the constraints and enabling factors? In *Proceedings of the Seventeenth International Conference on Digital Society (ICDS 2023)*.

Lipsky, M. (1980). *Street-level bureaucracy: Dilemmas of the individual in public services*. Russell Sage Foundation.

Madise, Ü., & Martens, T. (2006). E-voting in Estonia 2005: The first practice of country-wide binding Internet voting in the world. *Electronic Voting, 86*, 15–26.

Mahoney, J., & Rueschemeyer, D. (2003). Comparative historical analysis. *Comparative historical analysis in the social sciences*, 3–38.

McDermott, Y. (2017). Conceptualizing the right to data protection in an era of Big Data. *Big Data & Society, 4*(1), 1–7. https://doi.org/10.1177/2053951716686994

Media Foundation for West Africa. (2022, March 28). Ghana's cybersecurity law implementation: CSOs demand more awareness creation. MFWA Issues in Focus.

Ministry of Finance. (2022). *Programme based budget estimates for 2022: Electoral Commission*. https://www.mofep.gov.gh/sites/default/files/pbb-estimates/2022/2022-PBB-EC.pdf

Ministry of Finance. (2024). *Programme based budget estimates for 2024: Electoral Commission*. https://mofep.gov.gh/sites/default/files/pbb-estimates/2024/2024-PBB-EC_.pdf

Mohan, V., Vaughan, J. W., & Reiter, M. K. (2023). A systematization of voter registration security. *Journal of Cybersecurity, 9*(1), tyad008. https://doi.org/10.1093/cybsec/tyad008

MyJoyOnline. (2024, November 14). EC urged to implement robust cybersecurity measures in upcoming elections. https://www.myjoyonline.com/ec-urged-to-implement-robust-cybersecurity-measures-in-upcoming-elections/

NASEM (National Academies of Sciences, Engineering, and Medicine). (2018). *Securing the vote: Protecting American democracy*. The National Academies Press.

National Cyber Security Centre. (n.d.). CERT-GH. https://cybersecurity.gov.gh/cert.html

National Cybersecurity Centre. (2021). *Ghana's national cybersecurity policy and strategy*.

National Development Planning Commission. (2016). *Strategic Plan 2016–2020: Electoral Commission of Ghana*. https://new-ndpc-static1.s3.amazonaws.com/CACHES/PUBLICATIONS/2016/05/03/electoral-commission-ghana-strategic-plan-2016.pdf

National Information Technology Agency. (2012). Data Protection Act, 2012 (Act 843). https://nita.gov.gh/theevooc/2017/12/Data-Protection-Act-2012-Act-843.pdf

National Institute of Standards and Technology. (2021). *Cybersecurity framework election infrastructure profile* (NISTIR 8310). U.S. Department of Commerce. https://www.nist.gov/publications/cybersecurity-framework-election-infrastructure-profile

NCA. (2023, November 15). NCA collaborates with CSA to hold cybercrime and cybersecurity sensitisation for staff. https://nca.org.gh/2023/11/15/nca-collaborates-with-csa-to-hold-cybercrime-and-cybersecurity-sensitisation-for-staff/

Neale, B. (2019). *What is qualitative longitudinal research?* Bloomsbury Academic. https://doi.org/10.5040/9781472532992

NIS Cooperation Group. (2018). *Compendium on cyber security of election technology*. European Commission.

Nobles, C. (2024). Cybersecurity and threat prevention in elections: A multi-layered approach. *Journal of Cybersecurity, 10*(1), Article PMC11073482. https://pmc.ncbi.nlm.nih.gov/articles/PMC11073482/

Norris, P. (2019). Do threats to electoral integrity undermine trust in elections? *Political Studies, 67*(1), 3–25.

Nye, J. S., Jr. (2011). *The future of power*. PublicAffairs.

Office of the Director of National Intelligence. (2017). *Assessing Russian activities and intentions in recent US elections*. https://www.dni.gov

Owusu-Darko, K. A. (2024, October 1). Election integrity at risk: The cybersecurity consequences of the Electoral Commission's illegal transfer of voters. LinkedIn Pulse.

Owusu-Oware, E., & Effah, J. (2022). Biometric system for protecting information and improving service delivery: The case of a developing country's social security and pension organisation. *Information Development.* https://doi.org/10.1177/02666669221085709

P3 Risk Management. (2023). *Cybersecurity tools, techniques and reporting*. Chapter 10. Retrieved from uploaded document.

Paun, M. (2018, May). Review: *Data and Goliath by Bruce Schneier*. *Law, Innovation and Technology.*

Pettigrew, A. M. (1990). Longitudinal field research on change: Theory and practice. *Organization Science, 1*(3), 267–292. http://www.jstor.org/stable/2635006

Public Services Commission. (2024). Ghana faces cyberattack threat ahead of December elections – ACDT. https://psc.gov.gh/ghana-faces-cyberattack-threat-ahead-of-december-elections-acdt/

Quaynor, N. (2018). Cybersecurity strategy in Ghana: Policy and institutional gaps. *Ghana Policy Journal, 4*(1), 21–36.

Quinn, C. (2015, June 5). Surveillance, bulk data collection and intelligence: An interview with Bruce Schneier. *Schneier on Security*.

Schneier, B. (2015). *Data and Goliath: The hidden battles to collect your data and control your world*. W.W. Norton & Company.

Scott, W. R. (2008). *Institutions and organizations: Ideas and interests* (3rd ed.). Sage.

Staak, S. van der, & Wolf, P. (2019). *Cybersecurity in elections: Models of interagency collaboration*. International Institute for Democracy and Electoral Assistance.

Tech Africa News. (2024, November 6). Ghana faces highest volume of cyberattacks in West Africa – NETSCOUT reports. https://techafricanews.com/2024/11/06/ghana-faces-highest-volume-of-cyberattacks-in-west-africa-netscout-reports

The Business & Financial Times. (2024, October 1). Election integrity at risk: The cybersecurity consequences of EC's illegal transfer of voters. https://thebftonline.com/2024/10/01/election-integrity-at-risk-the-cybersecurity-consequences-of-ecs-illegal-transfer-of-voters/

Thiel, A. (2020). Biometric identification technologies and the Ghanaian 'data revolution'. *The Journal of Modern African Studies, 58*(1), 115–136.

Tidal Cyber. (2024). Election cyber interference threats and defenses. https://www.tidalcyber.com/election-cyber-interference-threats-and-defenses

USAID & IFES. (2022a). *Primer: Cybersecurity and elections*. USAID Digital Frontiers Project. Retrieved from https://www.ifes.org

USAID & IFES. (2022b). *Understanding cybersecurity throughout the electoral process: A reference document*. USAID Digital Frontiers Project. Retrieved from https://www.ifes.org

USAID & IFES. (2022c). *Briefing paper on cybersecurity of voter registration*. USAID Digital Frontiers Project. Retrieved from https://www.ifes.org

USAID & IFES. (2022d). *Briefing paper on cybersecurity of election results management systems*. USAID Digital Frontiers Project. Retrieved from https://www.ifes.org

USAID & IFES. (2022e). *Electoral cybersecurity: A donor program development guide*. USAID Digital Frontiers Project. Retrieved from https://www.ifes.org

Whitman, M. E., & Mattord, H. J. (2017). *Principles of information security* (6th ed.). Cengage Learning.

Wolf, P., Alim, A., Kasaro, B., Namugera, P., Saneem, M., & Zorigt, T. (2017). *Introducing biometric technology in elections*. International Institute for Democracy and Electoral Assistance (International IDEA).

World Bank. (2022). *Biometric digital ID systems: A global overview*. https://www.worldbank.org

Yin, R. K. (2018). *Case study research and applications: Design and methods (6th ed.)*. Sage.

APPENDICES

APPENDIX A: INTERVIEW GUIDE FOR EC, CSA, AND CERT-GHANA

THE CYBERSECURITY INSTRUMENTS AND POLICY FRAMEWORK OF GHANA'S ELECTORAL COMMISSION: A QUALITATIVE LONGITUDINAL STUDY

Introduction

Thank you for agreeing to speak with me today. This interview is part of my MPhil research, which aims to examine how Ghana's Electoral Commission has developed and implemented cybersecurity policies over time to protect the integrity of the electoral process.

With your permission, I would like to record our conversation; please note that your identity will remain confidential. Participation is voluntary, and you are free to decline to answer any question or withdraw at any point during the interview.

If you have any doubts or wish to clarify anything related to this research, you may contact my academic supervisor, Dr. Nene-Lomotey Kuditchar, on 0547790352 or via email at nkuditchar@ug.edu.gh.

Do you have any questions before we begin?

a. To the best of your knowledge, when did the Electoral Commission first begin considering cybersecurity as part of its electoral process?

(Follow-up: What prompted this consideration? Was it a specific event, trend, or internal concern?)

b. Were there any formal or informal measures in place to address cyber-related risks before 2012?

(Follow-up: Can you describe what those measures looked like? Who was involved in their design or implementation?)

c. Can you describe the EC's general approach to digital threats at the time you first got involved?

(Follow-up: Was there any specific awareness of cybersecurity as distinct from general IT concerns?)

d. What kinds of information systems or digital platforms were being used by the EC before cybersecurity became a concern?

(Follow-up: Were there any discussions at the time about the risks these systems might pose?)

e. Was there any external pressure or internal awareness that highlighted the need for more structured cybersecurity policies in the early stages? (e.g., donor partners, government, internal audits, regional incidents, etc.)

A. EVOLUTION AND DRIVERS OF CYBERSECURITY POLICY (RESEARCH OBJECTIVE 1)

1. How has the EC's approach to cybersecurity changed across the different electoral cycles (2012, 2016, 2020, 2024)?

2. Can you identify key events or threats that triggered major changes in cybersecurity policy or practices?

3. How were lessons learned from previous elections (e.g., cyber incidents, technical failures) incorporated into policy reforms?

4. What role did legal instruments such as the Cybersecurity Act (2020) and Data Protection Act (2012) play in shaping the EC's cybersecurity posture?

5. Have international best practices or donor pressure influenced EC's cybersecurity policy decisions?

B. IMPLEMENTATION AND EFFECTIVENESS OF CYBERSECURITY MEASURES (RESEARCH OBJECTIVE 2)

6. What are the key cybersecurity tools or frameworks currently implemented by the EC (e.g., intrusion detection systems, multi-factor authentication, firewalls, encryption)?

7. In your opinion, how effective have these tools been in protecting electoral integrity and public trust?

8. How would you assess the EC's capacity to detect, respond to, and recover from cyber incidents?

9. Are there formal audits, incident response plans, or simulation exercises conducted before elections? How effective are they?

C. GAPS, INSTITUTIONAL CHALLENGES, AND RECOMMENDATIONS (RESEARCH OBJECTIVE 3)

10. What are the major institutional, legal, or technical challenges the EC faces in implementing robust cybersecurity?

11. Are there particular vulnerabilities or threats (e.g., insider threats, outdated infrastructure, disinformation) that remain inadequately addressed?

12. How would you describe inter-agency collaboration (e.g., between EC, CSA, CERT-GH, Ministry of Communications) in protecting electoral systems?

13. In what ways can cybersecurity capacity at the EC be strengthened, whether in staffing, training, funding, or governance?

14. What best practices (from Ghana or elsewhere) would you recommend for improving the EC's cybersecurity framework?

D. FORWARD-LOOKING PERSPECTIVES

15. From your perspective, how prepared is the EC for emerging cybersecurity threats, including AI-generated misinformation and hybrid attacks?

16. What mechanisms can ensure the continuous improvement of cybersecurity policy between electoral cycles (not just in election years)?

17. Are there structural reforms or new institutional arrangements you would recommend for enhancing electoral cybersecurity in Ghana?

E. BACKGROUND, ROLE AND EXPERIENTIAL CONTEXT

18. Can you briefly describe your current role and how it relates to electoral cybersecurity in Ghana?

19. How long have you been involved with the Electoral Commission (or CSA/CERT-GH/other relevant body), and in what capacity?

20. What was your involvement in Ghana's past electoral cycles, especially 2012, 2016, 2020, or 2024?

E. PARTICULARS OF INTERLOCUTOR

21. Name:

22. Place of Work:

23. Position:

24. Duration:

APPENDIX B: INTERVIEW GUIDE FOR CIVIL SOCIETY AND DEVELOPMENT PARTNERS

Introduction

Thank you for agreeing to speak with me today. This interview is part of my MPhil research, which aims to examine how Ghana's Electoral Commission has developed and implemented cybersecurity policies over time to protect the integrity of the electoral process.

With your permission, I would like to record our conversation; please note that your identity will remain confidential. Participation is voluntary, and you are free to decline to answer any question or withdraw at any point during the interview.

If you have any doubts or wish to clarify anything related to this research, you may contact my academic supervisor, Dr. Nene-Lomotey Kuditchar, on 0547790352 or via email at nkuditchar@ug.edu.gh.

Do you have any questions before we begin?

SECTION A: OBSERVATIONS ON EVOLUTION OF EC'S CYBERSECURITY (OBJECTIVE 1)

1. Based on your organization's experience, how has the EC's approach to cybersecurity changed across the 2012, 2016, 2020, and 2024 election cycles?

2. Have there been any key moments, incidents, or external events that you believe led to major changes in EC cybersecurity practices?

3. What is your assessment of the influence of donor support, policy advocacy, or civil society engagement on EC's adoption of cybersecurity reforms?

SECTION B: EFFECTIVENESS OF CYBERSECURITY MEASURES (OBJECTIVE 2)

4. To what extent do you think current EC cybersecurity policies and tools are effective in protecting electoral integrity?

5. Has the EC been transparent and responsive in communicating cybersecurity measures to stakeholders and the public?

6. Have you observed any improvements in the EC's capacity to respond to cyber incidents or misinformation campaigns in recent elections?

7. Does the EC collaborate with your organization (or others like yours) on digital election monitoring or civic technology platforms?

SECTION C: GAPS, COLLABORATION, AND RECOMMENDATIONS (OBJECTIVE 3)

8. From your viewpoint, what are the most pressing cybersecurity risks or weaknesses facing Ghana's electoral systems today?

9. What institutional, legal, or capacity-related challenges do you believe are limiting EC's ability to fully safeguard elections?

10. How effective is inter-agency collaboration between the EC, CSA, CERT-GH, and relevant ministries?

11. What reforms, capacity-building strategies, or best practices (local or international) would you recommend for strengthening Ghana's electoral cybersecurity?

SECTION D: ROLE OF YOUR INSTITUTION

12. Can you describe your institution's role in supporting or monitoring electoral cybersecurity in Ghana?

13. What contributions (technical support, policy dialogue, public advocacy, election observation) has your institution made in this area?

14. How have the EC or government stakeholders received your work — has there been active engagement or resistance?

Closing

15. Is there anything else you would like to share regarding Ghana's preparedness for cyber threats to elections?

PARTICULARS OF INTERLOCUTOR

16. Name:

17. Place of Work:

18. Position:

19. Duration:

20. Elections Involved (if any):