Scientific Research Publishing

Journal of Computer and Communications, 2025, 13(12), 134-157
https://www.scirp.org/journal/jcc
ISSN Online: 2327-5227
ISSN Print: 2327-5219

Cyber Diplomacy and Data Security Challenges in Ghana's Foreign Service

Perry Opoku Agyeman, David Laud Amenyo Fiase

Regent University College of Science and Technology, Mallam, Ghana
Email: perrycos7@gmail.com, david.fiase@regent.edu.gh

How to cite this paper: Agyeman, P.O. and Fiase, D.L.A. (2025) Cyber Diplomacy and Data Security Challenges in Ghana's Foreign Service. *Journal of Computer and Communications*, **13**, 134-157.
https://doi.org/10.4236/jcc.2025.1312008

Received: November 27, 2025
Accepted: December 22, 2025
Published: December 25, 2025

Copyright © 2025 by author(s) and Scientific Research Publishing Inc.
This work is licensed under the Creative Commons Attribution-NonCommercial International License (CC BY-NC 4.0).
http://creativecommons.org/licenses/by-nc/4.0/

Open Access

Abstract

This study examines the state of cyber diplomacy and data security within Ghana's foreign service, responding to growing global concerns about securing diplomatic communication in an evolving cyber threat landscape. Guided by four objectives, the research assesses the operationalization of cyber diplomacy, identifies data security vulnerabilities, evaluates institutional and policy gaps, and draws comparative insights to inform strategic recommendations. A mixed-methods approach was applied, combining a survey of 18 Ghanaian diplomatic missions, interviews with seven senior Ministry of Foreign Affairs officials, and document analysis of 15 national and institutional cybersecurity policies. The findings reveal that Ghana's cyber diplomacy is at a nascent stage, with significant operational and institutional limitations. Seventy-two percent of missions rely on unencrypted email systems, 61% operate on outdated ICT infrastructure, and only 33% use multi-factor authentication. Institutional gaps were also prominent: only 11% of missions have trained IT personnel, 72% lack cyber focal points, and 83% of staff report insufficient policy guidance. The study further shows weak coordination between diplomatic missions and domestic cybersecurity agencies, with only 17% reporting active engagement. Comparative analysis with AU, ECOWAS, EU, Estonia, and Rwanda demonstrates that Ghana lags behind global and regional best practices. The study concludes that strengthening institutional capacity, modernizing policy frameworks, and enhancing technical safeguards are essential to safeguard Ghana's diplomatic communications and reinforce its cyber diplomacy posture.

Keywords

Cyber Diplomacy, Data Security, Foreign Service, Ghana, Cybersecurity Governance, Digital Diplomacy

1. Introduction

1.1. Background and Context

Over the past two decades, digital technology has become central to international relations, transforming how states communicate, negotiate, and protect national interests. This shift has given rise to cyber diplomacy, a field where foreign policy increasingly intersects with cybersecurity, digital governance, and information protection. Countries now rely on secure digital channels to conduct bilateral engagements, participate in multilateral negotiations, and coordinate crisis responses. As global cyber threats grow in sophistication, ranging from espionage, ransomware, and data breaches to disinformation, the ability of a state to safeguard its digital interactions has become essential to maintaining diplomatic credibility and national security.

Across Africa, governments are rapidly digitizing public services, and foreign ministries are modernizing communication structures to remain competitive in the global diplomatic environment. However, this transformation brings new risks. Diplomatic missions operate in complex environments where sensitive information routinely passes through electronic systems. Any compromise of these systems has the potential to undermine foreign policy decisions, weaken negotiation leverage, and expose national security vulnerabilities.

Ghana is no exception to these global developments. The country has made significant progress in strengthening cybersecurity, including the establishment of the Cyber Security Authority and the passage of the Cybersecurity Act. Nevertheless, the increasing reliance on digital platforms within the Ministry of Foreign Affairs and Regional Integration (MFA) presents new challenges that require sustained attention. Ghana's diplomatic missions engage with a wide network of international partners, handle classified communication, and manage the personal data of Ghanaians abroad. These functions make them attractive targets for cyberattacks, especially in a geopolitical environment where state and non-state actors seek strategic advantage through cyber means.

As Ghana deepens its engagement in international digital dialogues, including AU, ECOWAS, UN, and bilateral cybersecurity collaborations, understanding the country's cyber diplomacy readiness becomes increasingly important. Mapping these trends provides a foundation for assessing how well Ghana's foreign service can withstand emerging cyber threats and adapt to the digital realities of modern diplomacy.

1.2. Problem Statement

Despite Ghana's efforts to improve national cybersecurity, its foreign service still faces significant risks associated with digital communication and data handling. Diplomatic missions routinely exchange sensitive information through electronic channels, yet many of these channels are not adequately protected against intrusion, interception, or manipulation. Threat actors, including cybercriminals, hacktivists, and state-sponsored groups, are increasingly targeting diplomatic networks to gain intelligence or undermine foreign policy initiatives. These risks are amplified by limited cybersecurity awareness among diplomatic staff, outdated communication systems, inconsistent compliance with data protection protocols, and weak coordination between the MFA and national cybersecurity institutions.

The core problem, therefore, is that Ghana's foreign service operates in a rapidly evolving cyber threat environment without a fully developed cyber diplomacy framework or comprehensive data security posture. This gap exposes the country to diplomatic vulnerabilities that could compromise national interests, erode trust among international partners, and weaken Ghana's capacity to participate effectively in global cyber governance. Addressing these concerns requires a clear understanding of current practices, institutional gaps, and emerging security challenges.

1.3. Research Gap

Existing literature on cybersecurity in Ghana has largely focused on national critical information infrastructure, financial systems, and the broader digital economy. While these studies provide valuable insights, they rarely examine the foreign service as a unique operational environment with distinct data security demands. Research on cyber diplomacy in Africa often highlights continental frameworks or regional cooperation but offers limited analysis of country-specific institutional readiness. Moreover, most available studies do not explore how cyber threats intersect with diplomatic practices such as negotiation, consular services, multilateral engagement, or the protection of sensitive foreign policy data.

This gap is particularly significant given the increasing globalization of cyber norms and the growing expectation for states to establish clear digital foreign policy positions. By concentrating on Ghana's foreign service, this study addresses a critical but under-examined intersection between diplomacy and cybersecurity, offering insights that can inform policy and institutional reforms.

1.4. Research Objectives

This study is guided by four interconnected objectives designed to align with the mixed-methods design and the analytical structure of the findings. The objectives are as follows:

1) To assess the current state of cyber diplomacy within Ghana's foreign service, focusing on the preparedness of diplomatic missions, existing communication systems, institutional awareness, and the extent to which cyber norms are integrated into day-to-day diplomatic practice.

2) To identify and analyze the data security challenges facing Ghana's diplomatic missions, including technical vulnerabilities, human-factor risks, and organizational weaknesses that expose diplomatic communications to cyber threats.

3) To evaluate institutional and policy gaps within the Ministry of Foreign Affairs (MFA) and its missions that hinder the operationalization of cyber diplo-

macy, with emphasis on staffing capacity, coordination mechanisms, and the adequacy of existing policy and regulatory frameworks.

4) To compare Ghana's cyber diplomacy practices and data security posture with regional and international benchmarks (AU, ECOWAS, EU, Estonia, Rwanda) and develop evidence-based recommendations for strengthening cyber diplomacy and securing diplomatic communication systems.

1.5. Significance of the Study

This research is significant for both academic and policy communities. Academically, it contributes to the emerging body of knowledge on cyber diplomacy by presenting an in-depth, country-specific case that highlights how digital transformation is reshaping diplomatic practice in Africa. It offers a nuanced understanding of how cybersecurity concerns influence foreign policy operations, providing a foundation for future comparative or regional studies.

From a policy perspective, the study provides evidence-based insights that can guide the Ministry of Foreign Affairs and its partners in developing stronger cybersecurity frameworks. By identifying vulnerabilities and institutional gaps, the findings can support the design of targeted training programs, capacity-building initiatives, and inter-agency collaboration mechanisms. Ultimately, the study helps position Ghana to engage more effectively in global cyber governance debates while protecting its diplomatic communications and national interests.

2. Literature Review

2.1. Conceptualizing Cyber Diplomacy

Cyber diplomacy has emerged as a central pillar of modern foreign policy as states increasingly rely on digital infrastructures to project influence, negotiate international norms, and secure national interests in cyberspace. The concept broadly refers to the use of diplomatic tools and processes to manage cyberspace-related issues, including cybersecurity cooperation, internet governance, cyber norms, and digital rights [1]. Initially, cyber diplomacy evolved from broader discussions on information security and critical infrastructure protection in the early 2000s, driven largely by the rise of transnational cybercrime and state-sponsored intrusions. Over time, it has expanded to encompass digital trade, technological standards, and the geopolitical implications of emerging technologies such as artificial intelligence and 5G [2].

The European Union, the United States, China, and Russia have been particularly active in shaping global cyber diplomacy strategies. The EU's External Cyber Capacity Building Agenda and the U.S. State Department's Bureau of Cyberspace and Digital Policy exemplify how major actors integrate cyber issues into diplomacy and national security [3]. Similarly, the United Nations Group of Governmental Experts (UN-GGE) has played a critical role in negotiating voluntary norms of responsible behavior in cyberspace, highlighting how diplomacy is used to reduce risks of cyber conflict [4].

For developing states, including those in Africa, cyber diplomacy provides a platform to articulate digital sovereignty concerns, build cooperative defense mechanisms, and address cyber asymmetries [5]. In this sense, cyber diplomacy is not only a security endeavor but also an instrument for shaping global power relations within the digital domain. This conceptual foundation frames the relevance of cyber diplomacy for Ghana, whose foreign service increasingly depends on digital infrastructure to conduct diplomatic engagements.

2.2. Digital Transformation in Foreign Services

The digital transformation of foreign services has fundamentally altered how diplomacy is conducted. Modern diplomatic operations rely heavily on electronic communication systems, cloud platforms, and digital archives for transmitting classified and unclassified information. These technologies have enhanced the speed and volume of diplomatic interactions but have simultaneously increased exposure to cyber threats. According to Cornish, Hughes, and Livingstone (2009), digitalization has expanded the attack surface of foreign ministries, making them prime targets for espionage, data theft, and disruptive cyber operations [6].

Several high-profile incidents highlight the vulnerability of diplomatic networks. The 2014 breach of the U.S. State Department's unclassified email system, attributed to Russian state-linked groups, resulted in prolonged operational disruptions and exposed sensitive communications [7]. The 2018 cyber-espionage campaign targeting the EU's diplomatic cables, where thousands of classified documents were compromised, further illustrates the persistent exposure of diplomatic communication systems [8]. These incidents underscore how foreign ministries must adapt their security protocols to mitigate advanced persistent threats (APTs).

Digital transformation has also reshaped internal foreign service practices. Cloud-based systems facilitate real-time communication between missions, while videoconferencing tools have become essential for remote diplomacy, especially after the COVID-19 pandemic [9]. However, the adoption of these technologies introduces challenges related to encryption, authentication, and compliance with national data protection regulations. Many countries lack standardized cybersecurity guidelines for diplomatic missions, leading to uneven security implementations across embassies.

For Ghana's foreign service, which is expanding its digital footprint through e-diplomacy initiatives and online consular services, understanding these global trends is crucial. Without adequate cybersecurity mechanisms, digital transformation may amplify vulnerabilities and expose diplomatic operations to significant strategic risks.

2.3. Data Security Challenges in Embassies

Embassies and diplomatic missions operate in high-threat environments where geopolitical interests often motivate sophisticated cyber operations. The security of embassy communication systems is vital because these missions routinely transmit classified political, economic, and security information. According to Rid and Buchanan (2015), embassies are among the most frequently targeted institutions due to their symbolic and strategic value [10].

A significant example is the 2010 breach of the Australian diplomatic network, where attackers infiltrated systems used by the Department of Foreign Affairs and Trade, accessing sensitive cables and communications [11]. Similarly, the 2015 compromise of the U.S. Office of Personnel Management (OPM), although not an embassy, exposed millions of personnel records, including data on diplomats and intelligence officers, demonstrating the global scale of vulnerabilities in government systems [12].

Embassies also face risks related to insecure third-party technologies. The African Union Headquarters incident, in which data was reportedly transferred nightly to servers in China between 2012 and 2017, raised concerns about the security of ICT equipment in diplomatic environments [13]. Moreover, the shift toward cloud-based diplomacy tools means that vulnerabilities in commercial platforms may directly impact foreign service operations.

Insider threats present additional challenges. Diplomatic staff, contractors, or locally employed personnel may unintentionally or deliberately compromise systems through weak passwords, phishing susceptibility, or malicious behavior [14]. Limited cybersecurity training among diplomats further compounds the problem.

These case studies demonstrate that embassies face a complex mix of external, internal, and systemic data security threats. Understanding these dynamics is essential for assessing Ghana's exposure to similar risks and evaluating the safeguards required to protect diplomatic information.

2.4. African & Ghanaian Context

Africa's cybersecurity landscape has expanded significantly over the last decade as states increasingly engage with digital technologies for governance, commerce, and diplomacy. The African Union's Convention on Cyber Security and Personal Data Protection (known as the Malabo Convention) provides the most comprehensive regional framework, although ratification and implementation remain slow across the continent [15]. Regional bodies such as ECOWAS have also adopted supplementary acts on cybersecurity and data protection to strengthen harmonization among West African states [16].

Ghana is often regarded as one of the more proactive countries in Africa regarding cybersecurity governance. The Cybersecurity Act, 2020 (Act 1038) established the Cyber Security Authority (CSA) to regulate cybersecurity activities, protect critical information infrastructure, and ensure national cyber resilience. In addition, Ghana's Data Protection Act, 2012 (Act 843) mandates the protection of personal data and establishes compliance obligations for public and private institutions [17]. These frameworks collectively shape the legal environment within which Ghana's foreign service operates.

Despite these advances, institutional gaps persist. Reports from the Cyber Security Authority [18] highlight challenges such as limited cybersecurity expertise, inconsistent implementation of security standards across public institutions, and insufficient coordination between security agencies. Ghana's foreign service, which increasingly relies on digital communication tools for consular services and diplomatic correspondence, operates within this broader national context.

Diplomatic missions face additional constraints, including outdated ICT infrastructure, limited budgets for cybersecurity upgrades, and reliance on third-party service providers for internet and technical support. Moreover, the absence of a dedicated cyber diplomacy strategy means that Ghana engages in international cyber governance on a largely ad hoc basis. Addressing these gaps requires a holistic understanding of both domestic policy frameworks and regional dynamics influencing digital security.

2.5. Theoretical/Conceptual Framework

This study is guided by the Information Security Governance (ISG) framework, which emphasizes the integration of leadership, organizational structures, risk management processes, and accountability mechanisms to safeguard information assets [19]. ISG is appropriate for analyzing cyber diplomacy because it links technical security measures with institutional decision-making, an essential consideration for foreign services that operate across diverse geopolitical and technical environments. The framework also highlights the role of strategic alignment, ensuring that cybersecurity policies support broader organizational objectives [20]. Applying ISG to Ghana's foreign service allows the study to evaluate how governance structures, legal frameworks, and operational practices collectively influence cyber diplomacy capacity and data security resilience.

3. Methodology

This chapter delineates the methodological framework employed to investigate the interplay between cyber diplomacy and data security within Ghana's Foreign Service. The research was guided by four specific objectives: to assess the current institutional and policy framework for cyber diplomacy in Ghana's Ministry of Foreign Affairs and Regional Integration (MFA); to identify the specific data security vulnerabilities faced by Ghana's diplomatic missions abroad; to analyze the alignment of Ghana's national cyber posture with regional (ECOWAS) and continental (AU) cyber norms; and to propose a strategic framework for enhancing cyber resilience in Ghana's foreign policy operations. A rigorous, qualitative approach was adopted to ensure a deep, contextual understanding of these complex issues. The methodology was meticulously designed to ensure the authenticity, validity, and ethical integrity of the findings.

3.1. Research Design

This study employed a mixed-methods research design, integrating both qualitative and quantitative approaches to provide a comprehensive understanding of

Ghana's cyber diplomacy landscape. Although the qualitative component, consisting of document analysis and semi-structured expert interviews, formed the foundation for exploring policy context, institutional capacity, and practitioner experiences, the study also incorporated quantitative survey data to capture measurable patterns, stakeholder perceptions, and prevalence-based insights.

The mixed-methods approach was chosen because neither a solely qualitative nor purely quantitative design could adequately address the multifaceted nature of the topic. The qualitative strand offered depth, allowing the study to explore the contextual and operational realities embedded in policy documents and expert viewpoints. In parallel, the quantitative strand contributed breadth by systematically capturing numerical trends that strengthened the evidence base and supported generalizability.

Using these two complementary strands enabled triangulation, where insights from interviews and document analysis were compared with survey findings to validate patterns and enrich interpretation. This integrated design ultimately improved the robustness of the study, ensuring that the research objectives were addressed from both an analytical and experiential perspective.

3.2. Data Sources

The research drew upon a diverse range of primary and secondary data sources, each carefully selected to address a specific research objective. To assess Ghana's institutional framework, key policy documents were analyzed, including the Ghana National Cybersecurity Policy & Strategy (2021) and the Data Protection Act, 2012 (Act 843) [21]. For identifying data security vulnerabilities, annual reports and public advisories from the Cyber Security Authority (CSA) of Ghana and internal (non-classified) MFA procedural memoranda were scrutinized. To analyze international alignment, foundational texts such as the African Union Convention on Cyber Security and Personal Data Protection (2014) and the relevant ECOWAS Directive on Fighting Cyber Crime were examined. Finally, to inform the strategic framework, a robust body of academic literature on cyber diplomacy and digital foreign policy, including works by scholars like Mihr (2022) and Tikk & Kerttunen (2020), was synthesized. This multi-source strategy ensured a comprehensive and evidence-based inquiry [22] [23].

3.3. Data Analysis Strategy

The data analysis followed a mixed-methods, objective-driven approach that integrated thematic, comparative, and quantitative analyses. Each research objective was paired with a specific analytical strategy to ensure coherence between the study design, empirical evidence, and the structure of the results.

Objective 1: Assessing the Current State of Cyber Diplomacy

A combined descriptive statistical analysis of survey data and thematic analysis of interview transcripts and policy documents was conducted. Survey responses from diplomatic missions were quantified to identify patterns in communication practices, infrastructure status, and staff preparedness. Qualitative themes from interviews and documents were used to contextualize these patterns and explain underlying institutional dynamics.

Objective 2: Identifying Data Security Challenges

A multi-layered vulnerability analysis was employed. Survey data were examined to quantify the prevalence of technical weaknesses such as outdated systems, weak authentication, and inadequate encryption. A deductive coding framework, based on common cyber-risk categories, was applied to interview data and MFA/ICT audit documents to identify human-factor risks, organizational lapses, and exposure to external threats.

Objective 3: Evaluating Institutional and Policy Gaps

A thematic policy and institutional analysis were conducted by reviewing the National Cybersecurity Strategy, MFA ICT guidelines, and the Data Protection Act. Codes were developed to capture gaps related to staffing, coordination structures, compliance mechanisms, and policy sufficiency. These themes were compared with insights from interviews and survey results to determine the extent to which institutional requirements for cyber diplomacy are unmet.

Objective 4: Comparative Benchmarking

A comparative analysis was carried out using regional and international standards as reference points. AU and ECOWAS cybersecurity frameworks, EU cyber diplomacy guidelines, and best-practice models from Estonia and Rwanda were systematically compared with Ghana's current practices. Key differences were identified across areas such as institutional capacity, secure communication protocols, training systems, and inter-agency coordination. This synthesis helped generate actionable recommendations grounded in global best practice.

The integration of these analytical techniques allowed for triangulation across data sources, ensured internal consistency, and provided the evidential basis for the four major themes presented in the Findings and Discussion section.

3.4. Ethical Considerations

Throughout the research, the highest ethical standards were upheld. Informed consent was obtained from all interview participants, who were assured of their anonymity and the confidentiality of their responses. The study strictly avoided soliciting or using any classified or sensitive government information. All data collected from documents was in the public domain or accessed through official, authorized channels. Direct quotations from interviews were used only with explicit permission, and all data has been stored securely on password-protected devices to prevent unauthorized access, ensuring the integrity of the research and the protection of all participants.

4. Findings and Discussion

4.1. Current State of Cyber Diplomacy in Ghana

To assess the current state of cyber diplomacy in Ghana, a mixed-methods approach was employed, including a document review of 15 official MFA and cybersecurity policy documents, structured interviews with seven senior MFA officials, and a survey of 18 Ghanaian diplomatic missions. The aim was to generate an empirical understanding of how cyber diplomacy is operationalized and the extent of preparedness in digital diplomatic communications.

The survey results indicated that 13 out of 18 missions (72%) rely primarily on standard email systems without end-to-end encryption, while only 5 missions had implemented secure messaging platforms, such as encrypted chat or virtual private networks (VPNs). Notably, 10 embassies (56%) reported using outdated ICT infrastructure, including legacy servers and operating systems, which significantly increase vulnerability to cyberattacks. This quantitative evidence reflects a limited institutionalization of cyber diplomacy tools and practices across Ghana's foreign service.

Interviews with MFA officials further revealed that awareness of cyber diplomacy is growing but remains fragmented. Of the seven officials interviewed, five reported having no formal training in cyber diplomacy, and only two had participated in international workshops on digital foreign policy. One official noted: "We are aware of global cyber norms, but integrating them into our daily diplomatic operations is still a challenge due to limited technical support and resources." This qualitative evidence aligns with the survey findings and highlights the gap between awareness and practical implementation.

A document analysis of the National Cybersecurity Strategy (2020-2025) and related MFA policy documents revealed only a single explicit reference to diplomatic engagement in cyberspace, primarily emphasizing participation in international cyber norms discussions rather than operational measures. Similarly, analysis of MFA ICT guidelines shows that while security protocols exist for internal communication, there is no standardized framework for embassies to manage sensitive or classified information in a secure digital environment. This lack of formalized procedures reflects a nascent stage of cyber diplomacy in Ghana.

Comparative examination of regional engagement shows that Ghana participates in African Union (AU) cybersecurity workshops and ECOWAS cross-border cyber norm initiatives, but the level of active implementation within missions is limited. Only 3 of the 18 missions (17%) reported coordinating with domestic cybersecurity authorities for incident reporting or threat intelligence. This evidence a disconnect between international engagement and domestic operational capacity, further underscoring the underdeveloped state of cyber diplomacy practices.

The results also highlighted the human factor as a critical component. Among diplomatic staff surveyed, 64% reported limited understanding of secure communication protocols, which increases the risk of inadvertent data leaks. Additionally, only 2 missions had dedicated IT personnel trained in cybersecurity, indicating that institutional capacity is insufficient to support comprehensive cyber diplomacy.

The findings indicate that Ghana's cyber diplomacy is partially developed but not operationally integrated across its foreign missions. Evidence shows that the majority of embassies rely on vulnerable ICT systems, training is limited, and formalized guidelines are sparse. While Ghana demonstrates intent to engage internationally, operational implementation at the mission level remains weak. These results directly support Objective 1, confirming that the current state of cyber diplomacy is nascent, fragmented, and in need of structured capacity-building to ensure that Ghana can participate effectively in global cyber governance while safeguarding diplomatic communications.

4.2. Data Security Challenges in Ghana's Foreign Service

The analysis of data security challenges within Ghana's foreign service combined survey responses from 18 embassies, interviews with 7 MFA officials, and examination of internal ICT audits. This approach allowed identification of both technical vulnerabilities and human/organizational weaknesses that compromise the security of diplomatic communications. The foundational data from the embassy survey is presented in Table 1.

Table 1. Embassy ICT infrastructure survey (N = 18 Missions).

Variable	Indicator	Frequency (n)	Percentage (%)
Primary communication method	Standard email (unencrypted)	13	72%
	Encrypted messaging/VPN	5	28%
ICT hardware condition	Outdated/legacy systems	10	56%
Multi-factor authentication (MFA)	Missions using MFA	6	33%
End-to-end encryption	Missions using E2E tools	5	28%
VPN configuration	Misconfigured/partially configured	8	44%
Cyber training received	Staff with cyber hygiene training	6	36%
Dedicated cybersecurity staff	Missions with trained IT experts	2	11%
Cyber incident response plan	Missions with formal IR plans	2	11%

4.2.1. Technical Vulnerabilities

Survey data revealed that 11 out of 18 embassies (61%) still operate on outdated server systems, which are no longer supported with security patches (Table 1). These legacy systems expose missions to malware, ransomware, and unauthorized access. In addition, only 6 missions (33%) employ multi-factor authentication (MFA) for email and system access, leaving the majority reliant on single-password logins. One IT officer commented during interviews: "We have strong passwords, but without MFA, a single breach could compromise the entire embassy network."

Furthermore, encrypted communication tools are inconsistently applied. Only

5 missions reported using end-to-end encryption for internal messaging and document transfer. The survey also revealed that remote access to embassy systems via VPNs is inadequately configured in 8 missions (44%), increasing vulnerability to external cyber intrusions. These findings suggest that technical safeguards are fragmented and unevenly implemented, heightening exposure to cyberattacks.

4.2.2. Human and Organizational Factors

Human behaviour emerged as one of the most significant contributors to cyber vulnerabilities within Ghana's foreign service. Survey data shows that 64% of diplomatic staff lack adequate knowledge of basic cyber hygiene, particularly in areas such as recognising phishing attempts, handling sensitive documents securely, and applying strong authentication practices. Interviews consistently reinforced this finding, with key themes detailed in Table 2. One senior diplomat explained that staff "largely rely on informal, ad hoc guidance from IT support when something goes wrong," noting that no structured or recurring training programme exists to standardise secure communication practices across missions.

Table 2. Summary of interview themes (n = 7 MFA Officials).

Theme Code	Description	Frequency (mentions)	Example Extract
T1: Limited cyber diplomacy training	Officials have limited exposure to cyber diplomacy capacity building.	12	"We have no structured training. Most of us learn informally."
T2: Resource and personnel constraints	Lack of IT staff, outdated systems, insufficient funds.	10	"Even when there is awareness, we simply don't have the staff."
T3: Absence of policy directives	No mission-level standards or guidelines for cybersecurity.	14	"We don't have embassy-specific cybersecurity protocols."
T4: Weak coordination with CSA/NITA	Missions operate in isolation from domestic cybersecurity bodies.	8	"We almost never coordinate with CSA unless something serious happens."
T5: Growing awareness but weak implementation	Officials know cyber matters are important but tools are lacking.	11	"We are aware of global cyber norms, but integrating them remains a challenge."

Interview narratives provided concrete examples of the kinds of human errors that frequently occur. Several officers admitted to opening unsolicited emails that appeared to come from partner embassies, later identified as spoofed messages designed to harvest login credentials. In another mission, staff reported routinely downloading attachments onto shared computers, increasing the likelihood that sensitive documents could be accessed by unauthorized individuals. A number of diplomats also acknowledged the persistent practice of printing classified correspondence and leaving documents temporarily unattended during busy periods, especially when preparing briefing materials for high-level meetings. These examples illustrate how everyday habits, rather than sophisticated attacks, often create the biggest openings for cyber compromise.

Organizational shortcomings compound these human vulnerabilities. Document analysis revealed that only 2 out of 18 missions have a documented incident response plan, and even in those cases, the procedures are not regularly tested or reviewed. Cyber incident reporting remains largely informal, with several interviewees noting that staff are often unsure whom to contact after detecting suspicious activity. As a result, minor intrusions or attempted breaches go unreported, increasing the likelihood of repeated exploitation. These findings align with broader regional observations that West African diplomatic institutions frequently lack standardized structures for managing cyber threats in a timely and coordinated manner. The process of identifying these vulnerabilities is further illustrated in Table 3.

Table 3. Coding matrix for vulnerability identification.

Vulnerability Category	Codes Identified	Number of Occurrences
Phishing Risks	P1, P2, P3	16
Insecure Communications	C1, C2	11
Insider Threats	I1, I2	7
Third-Party Vendor Risks	V1, V2	5
Obsolete Systems	O1	10

To mitigate these risks, the following realistic and actionable interventions are recommended:

1) Introduce Mandatory Annual Cyber Hygiene Training

- Create a structured training schedule covering phishing recognition, secure communication, password practices, and safe document handling.
- Use short scenario-based modules tailored to common embassy tasks to ensure relevance.

2) Implement Routine Phishing Simulations

- Conduct quarterly phishing-test campaigns to measure susceptibility and provide targeted follow-up training for staff who fall for simulated attacks.

3) Standardize Secure Document-Handling Practices

- Enforce clear rules on printing, sharing, and disposing of sensitive material.
- Provide lockable storage and encourage "clean desk" policies to minimize accidental exposure.

4) Establish a Formal Cyber Incident Reporting Chain

- Introduce a simple, embassy-wide reporting protocol that identifies responsible officers and outlines steps for escalation to headquarters and national agencies.

5) Adopt a Minimum Baseline of Cyber Governance Across Missions

- Require all missions to maintain a basic incident response plan aligned with national cybersecurity standards.

- Conduct periodic compliance checks to ensure consistency.

6) Create a Digital Ambassador or Cyber Focal Point Role in Every Mission

- Designate at least one trained staff member to coordinate cybersecurity matters, liaise with the Cyber Security Authority (CSA), and ensure that policies are implemented in practice.

Together, these measures directly address the human and organizational weaknesses identified in the findings. Strengthening human capabilities and institutional processes will significantly reduce the risk of breaches arising from everyday errors, enhancing the overall resilience of Ghana's foreign service.

4.2.3. External Threats

Evidence from both survey responses and public reports indicates exposure to targeted cyber threats. For example, Ghanaian diplomatic missions in high-risk regions reported receiving suspicious emails linked to known phishing campaigns targeting diplomatic networks. A summary of self-reported incidents is captured in Table 4. Additionally, interviews revealed concerns over espionage attempts, with two officials noting attempted intrusions via compromised software updates. These threats underscore the reality that Ghanaian embassies are not only vulnerable to generic cyber risks but also to geopolitically motivated attacks.

Table 4. External threat incidents reported (self-reported by embassies).

Category	Number of Missions Reporting	Example Incident
Suspicious phishing attempts	9	Emails imitating MFA headquarters
Attempted credential compromise	5	Login attempts from foreign IPs
Suspicious software update attempts	2	Compromised firmware patches
Malware alerts	4	Legacy servers detecting ransomware signatures
Unreported minor incidents	7	Staff admitting incidents were "handled locally"

4.2.4. Policy and Coordination Gaps

Document analysis of the Data Protection Act (2012) and MFA ICT guidelines shows limited guidance on embassy-level data security, a gap further analyzed in Table 5. Only 3 missions reported active coordination with domestic cybersecurity authorities (CSA or NITA) for threat intelligence, leaving most missions isolated. The lack of a structured, nation-wide cyber incident reporting mechanism reduces the ability to respond effectively to cyber threats.

Table 5. Document analysis matrix.

Document	Provision Relevant to Cyber Diplomacy	Evidence Extract	Relevance
Ghana National Cybersecurity Policy & Strategy (2021)	Only one section references "international cooperation in cyberspace."	"Ghana will engage with partners to shape norms."	Shows limited operational detail for embassies.
MFA ICT Guidelines	Password rules, basic IT hygiene.	No section on incident response, embassy secure communication.	Confirms policy gaps.
Data Protection Act (2012)	General data privacy obligations.	No embassy-specific classification procedures.	Demonstrates absence of diplomatic-tier directives.
AU Cybersecurity Convention (2014)	Mandates harmonized reporting.	"Member states shall adopt national CSIRTs."	Ghanaian missions not aligned; only 17% coordinate with CSA.
ECOWAS Directive on Fighting Cyber Crime	Requires standardized reporting and secure communication measures.	Ghana lacks embassy-level implementation.	Supports Objective 3.

4.2.5. Summary of Evidence

The consolidated evidence, including data from Table 1, indicates that Ghana's foreign service faces multi-dimensional data security challenges.

- Outdated systems: 61% of embassies still use unsupported servers.
- Weak authentication: 67% of missions lack MFA.
- Encryption gaps: Only 5 missions use end-to-end encrypted communication.
- Training gaps: 64% of staff report insufficient cyber hygiene knowledge.
- Incident management gaps: Only 2 missions have formal incident response plans.
- Limited coordination: Only 3 missions coordinate with domestic cybersecurity agencies.

The evidence indicates that Ghana's foreign service faces multi-dimensional data security challenges. Technical vulnerabilities, human factors, and organizational weaknesses converge to create a high-risk environment. These findings directly address Objective 2 (as coded in Table 3), highlighting that effective cybersecurity in diplomatic operations requires not only robust technical solutions but also systematic staff training, standardized protocols, and enhanced coordination with domestic and international cybersecurity agencies. Without addressing these gaps, Ghana's diplomatic communications remain susceptible to intrusion, espionage, and potential compromise of sensitive information, undermining both national security and international trust.

4.3. Institutional and Policy Gaps in Ghana's Foreign Service

An examination of Ghana's foreign service reveals significant institutional and policy gaps that hinder the effective implementation of cyber diplomacy. These findings are interpreted through the Information Security Governance (ISG) framework, which emphasizes strategic alignment, risk management, clearly assigned roles, adequate resourcing, and accountability mechanisms. The data draw on document reviews of MFA ICT guidelines, the National Cybersecurity Strategy 2020-2025, the Data Protection Act 2012, interviews with seven senior MFA officials, and survey responses from 18 Ghanaian embassies. Key themes from interviews are in Table 2, and the document analysis is summarized in Table 3.

4.3.1. Institutional Capacity Gaps (ISG: Roles & Responsibilities, Resourcing)

Survey results show that only 2 missions (11%) have dedicated IT personnel trained in cybersecurity, while the remaining 16 rely on general administrative staff with limited technical expertise (Table 1). From an ISG standpoint, this gap reflects weaknesses in role assignment and resourcing, two foundational governance principles. ISG emphasizes that information security governance is ineffective when critical responsibilities are dispersed among untrained staff or assigned informally without clear mandates.

Interviews reinforced this concern, revealing that although many missions acknowledge growing cyber risks, they lack personnel with the skills needed to implement preventive controls, monitor systems, or respond to incidents. The dependence on non-specialized staff therefore, creates systemic vulnerabilities and indicates that current operational practices are not aligned with ISG expectations regarding technical competence and capacity sufficiency.

A related weakness is the absence of formal cybersecurity committees or cyber focal points in 72% of missions. Cyber focal points refer to individuals formally designated to oversee cybersecurity-related responsibilities within a mission, including coordinating security procedures, liaising with national cybersecurity agencies, monitoring compliance with policies, and ensuring timely reporting of incidents. From an ISG perspective, failing to establish such accountability roles undermines the creation of structured oversight mechanisms. Without clear custodianship, security practices become inconsistent, informal, and difficult to enforce across missions.

4.3.2. Policy Framework Gaps (ISG: Strategic Alignment & Policy Direction)

Document analysis revealed that national policies provide high-level guidance but lack operational directives tailored to diplomatic environments (Table 5). From an ISG standpoint, this represents a misalignment between organizational strategy and policy implementation. ISG principles require that policies be actionable, context-specific, and linked to strategic objectives, in this case, securing diplomatic communication systems and supporting cyber diplomacy missions.

The MFA ICT guidelines offer only generic system-use instructions and do not include protocols for secure communication, incident reporting, or data classification. As a result, 83% of surveyed missions perceive existing policies as insufficient. Specific evidence extracts highlighting these gaps are compiled in **Table 6**. This weakens the ISG requirement that policy frameworks must drive consistent behaviour across the organization.

Table 6. Evidence extracts for policy gaps.

Gap Category	Evidence	Source
No standardized incident response	Only 2 missions have IR plans	Survey data
Weak staff training	64% lack training	Survey data
Poor coordination	3 missions coordinate with CSA/NITA	Survey data
Policy insufficiency	83% report guidelines inadequate	Interviews & survey
Lack of cyber focal points	72% of missions have none	Survey

Interviews further revealed that cyber diplomacy has not been formally integrated into MFA strategic planning. This absence breaks the ISG principle of strategic alignment, which ensures that cybersecurity priorities reinforce the core mission of the institution.

4.3.3. Coordination and Compliance Issues (ISG: Monitoring, External Integration)

Only 3 of the 18 missions reported active engagement with CSA or NITA (**Table 1**). This limited coordination undermines ISG's emphasis on risk management and compliance monitoring, where organizations must continuously assess threats, share intelligence, and coordinate with relevant national agencies.

Missions often operate in isolation from national cybersecurity efforts, reducing situational awareness and delaying mitigation. The absence of monitoring mechanisms also means missions cannot evaluate whether security practices meet required standards, another direct violation of ISG principles.

Unmitigated phishing attempts in 2022 highlight how the lack of coordinated risk monitoring materially increases the exposure of diplomatic operations to cyber threats.

4.3.4. Training and Awareness Gaps (ISG: Culture, Competency Development)

ISG underscores the importance of a security-aware organizational culture supported by ongoing capacity development. Yet 64% of embassy staff had never received cybersecurity or cyber diplomacy training, and only two missions conducted periodic workshops.

Interviews confirmed that limited training leads to inconsistent protocol adherence, even where technical tools are available. This demonstrates a weak security culture, which ISG identifies as a critical governance determinant of long-term resilience.

4.3.5. Evidence Summary (Interpreted Through ISG Principles)

- Roles & staffing: Only 11% of missions have trained IT staff → undermines ISG role clarity and capacity requirements.
- Accountability structures: 72% lack committees/focal points → weak ISG accountability governance.
- Policy direction: 83% believe policies are inadequate → misalignment between strategy and operational policy (Table 6).
- Risk monitoring: Only 17% engage CSA/NITA → violates ISG expectations for continuous risk management.
- Security culture: 64% lack training → breaches ISG competency and awareness principles.

The institutional and policy deficiencies reveal a foreign service that is not strategically aligned, insufficiently resourced, lacking clear accountability, and operating without effective risk management mechanisms, all of which weaken Ghana's cyber diplomacy posture and communication security. These findings satisfy Objective 3 and directly show where ISG expectations are unmet.

4.4. Comparative Insights

To contextualize Ghana's cyber diplomacy and data security practices, a comparative analysis was conducted with selected international and regional actors, including the African Union (AU), ECOWAS, European Union (EU), Estonia, and Rwanda. This approach highlights best practices and benchmarks that can inform strategic improvements in Ghana's foreign service. ey indicators from this comparison are synthesized in Table 7.

Table 7. Regional & international benchmark indicators.

Country/Region	Cyber Diplomacy Integration	Mandatory Training	Embassy-level Secure Systems	Incident Reporting System
Estonia	Fully integrated	Annual, mandatory	100% encryption	Centralized
Rwanda	Integrated into foreign policy	Regular	Standardized	National Cyber Fusion Center
EU	Cyber Diplomacy Toolbox	Structured	Standardized	EU CSIRTs Network
ECOWAS (Nigeria, Senegal)	Formal cyber focal points	Regular	Progressive	ECOWAS Regional CSIRT
Ghana (this study)	Nascent, fragmented	Limited	28% encrypted systems	No standardized system

4.4.1. African Union and ECOWAS

The AU has established the AU Convention on Cybersecurity and Personal Data Protection, which provides guidance for member states on harmonizing cybersecurity policies, including in diplomatic missions [24]. ECOWAS, through its Regional Cybersecurity Framework, mandates that member states adopt standardized reporting and incident response mechanisms. Comparative evidence shows that countries like Nigeria and Senegal actively implement AU guidelines in their diplomatic missions, including formalized cyber focal points and regular training programs. In contrast, only 17% of Ghanaian missions currently coordinate with domestic cybersecurity authorities, indicating a significant gap relative to regional peers (Table 7).

4.4.2. European Union

The EU integrates cyber diplomacy into its foreign policy via the EU Cyber Diplomacy Toolbox, which establishes protocols for threat intelligence sharing, incident response, and diplomatic engagement in cyberspace [25]. EU member states also invest heavily in specialized personnel and training programs. For example, Germany and Estonia maintain dedicated cyber diplomacy units within their foreign ministries, ensuring that technical capacity is embedded in policy processes. Compared to Ghana, where only 11% of missions have trained IT personnel (Table 1), the EU demonstrates the importance of institutionalizing expertise to achieve operational cyber diplomacy.

4.4.3. Estonia

Estonia provides a strong model, having survived significant cyberattacks in 2007 and developed a robust national cyber governance framework. All Estonian embassies employ multi-layered cybersecurity protocols, including mandatory encryption, continuous staff training, and centralized incident reporting [26]. This proactive approach contrasts sharply with Ghana, where 61% of embassies still operate on outdated systems, and formal incident response plans exist in only 2 missions (Table 1 & Table 7).

4.4.4. Rwanda

Rwanda has also prioritized cyber diplomacy and ICT security, embedding cybersecurity specialists within its Ministry of Foreign Affairs and ensuring alignment with the National Cybersecurity Policy (2015). Rwandan diplomats undergo regular training, and embassies maintain standardized secure communication platforms [27]. This level of preparedness provides a practical benchmark for Ghana to emulate, particularly in institutional capacity building and policy operationalization (Table 7).

4.4.5. Synthesis

Comparative evidence demonstrates that effective cyber diplomacy requires institutional integration, specialized personnel, standardized protocols, and continuous training. Ghana's foreign service lags in all these areas, particularly in technical capacity, formal policies, and coordination with national cybersecurity authorities (Table 7). Lessons from Estonia, Rwanda, and EU member states highlight the benefits of centralized planning, proactive risk management, and embedding cyber expertise into diplomatic workflows. Regional frameworks (AU and ECOWAS) provide a pathway for harmonized practices but remain underutilized by Ghanaian missions.

4.5. Implications for Diplomacy and National Security

The findings have direct implications for both diplomatic effectiveness and national security, and these implications become clearer when interpreted through the Information Security Governance (ISG) framework.

ISG highlights that strategic alignment, risk management, performance monitoring, and accountability are prerequisites for secure and resilient information environments. The study's evidence, 72% reliance on unencrypted systems, only 11% trained staff, and 83% reporting inadequate policy guidance, indicates that key ISG governance structures are not in place.

4.5.1. Diplomatic Implications (ISG: Strategic Alignment & Secure Operations)

Weak cybersecurity governance undermines Ghana's ability to conduct diplomacy securely:

- Strategic Misalignment: ISG principles show that cybersecurity must support the core diplomatic mission. But Ghana's policies and training gaps indicate that cyber diplomacy is not yet embedded in MFA strategic planning.
- Operational Risk: The absence of risk-based control, such as encryption, secure protocols, or incident response, makes sensitive diplomatic communication susceptible to interception, influencing negotiation outcomes and eroding trust.
- Credibility Loss: Without ISG-aligned governance, Ghana struggles to meet international expectations for secure diplomatic engagement, weakening its ability to shape cyber norms or participate in digital diplomacy initiatives with confidence.

4.5.2. National Security Implications (ISG: Risk Management & Accountability)

Diplomatic missions often transmit information that affects national defense, foreign policy, and economic negotiations. ISG stresses that such information assets require structured oversight and continuous monitoring.

However:

- The lack of trained personnel undermines risk identification and mitigation.
- Fragmented responsibilities weaken accountability mechanisms.
- Minimal coordination with CSA/NITA interrupts threat intelligence flows.
- Inconsistent communication protocols disable performance monitoring, a key ISG pillar.

These lapses increase the likelihood of espionage, data breaches, and geopolitical manipulation. A compromised diplomatic channel can expose national strategy, foreign engagements, and negotiative positioning.

Comparative insight shows that states such as Estonia, Rwanda, and EU members embed ISG principles directly into foreign ministry operations, through embedded cyber units, enforced standards, clear reporting lines, and structured training. Ghana's departure from these practices signals vulnerabilities that adversaries could exploit.

4.5.3. Conclusion (ISG-Aligned Interpretation)

Without adopting an ISG-grounded governance structure, clear roles, strategic alignment, risk management, and systematic monitoring, Ghana's foreign service will remain exposed to threats that compromise diplomatic integrity and national security. Embedding ISG principles into policy frameworks, capacity-building programs, and cross-agency coordination is therefore essential for Ghana to function as a credible and resilient actor in global cyber diplomacy.

5. Conclusions

The study set out to examine the state of cyber diplomacy and data security challenges within Ghana's foreign service, with a particular focus on vulnerabilities across diplomatic missions, institutional gaps, and the implications for national security. The findings demonstrate that although Ghana has made progress in national cybersecurity through the establishment of the Cyber Security Authority and ongoing regulatory reforms, the foreign service remains significantly underprepared for emerging cyber risks. Empirical evidence from embassy surveys and interviews revealed inadequate ICT infrastructure, inconsistent use of secure communication systems, and a general lack of cyber diplomacy training among foreign service personnel. This limited technical and institutional readiness weakens the ability of Ghanaian missions to protect sensitive diplomatic information or respond effectively to cyber incidents.

In addition, the study found that policy frameworks guiding embassy-level digital operations remain fragmented, with many missions operating without clear protocols for encryption, data handling, or incident reporting. When compared with cyber diplomacy models in regions such as the European Union, and countries such as Estonia and Rwanda, Ghana's foreign service lags behind in institutional coordination and cyber preparedness. This gap exposes the state to potential espionage, data breaches, and disruptions that could undermine bilateral relations or national security interests.

The overall conclusion is that Ghana's cyber diplomacy architecture requires deliberate strengthening. A combination of institutional reforms, technical investments, and strategic policy development is necessary to safeguard the digital components of diplomatic practice. The growing reliance on digital platforms for communication, negotiation, and coordination makes cybersecurity not just a technical requirement, but a foundational element of effective diplomacy. Enhancing cyber capacity within the foreign service will therefore be critical for Ghana's international competitiveness, resilience, and national security posture. The recommendations that follow provide a structured set of actions to address the gaps identified.

6. Recommendations

Ghana's foreign service requires an integrated approach to strengthening cyber diplomacy capacity, combining institutional, technical, and policy-level interventions. The recommendations below directly respond to the vulnerabilities identified across diplomatic missions and draw on best practices from leading cyber diplomacy systems.

6.1. Institutional Reforms

Strengthening Ghana's cyber diplomacy begins with restructuring the institutional foundations of the foreign service. The Ministry of Foreign Affairs should establish a Cyber Diplomacy and Digital Security Unit responsible for coordinating cybersecurity policies, monitoring threats, and liaising with the Cyber Security Authority. Every embassy should designate a cyber focal person trained to oversee digital safety protocols and report incidents promptly. Regular capacity-building programs must be introduced to equip diplomats with digital literacy and threat-awareness skills. Finally, the MFA should integrate cybersecurity responsibilities into performance assessments, ensuring accountability and fostering a culture of secure digital practices across missions.

6.2. Technical Cybersecurity Interventions

Embassies must transition from outdated infrastructure to secure, modern systems. This includes immediate deployment of end-to-end encrypted communication platforms, multi-factor authentication, and standardized secure email services across all missions. Servers and network hardware in foreign missions should be upgraded, with remote monitoring conducted by MFA headquarters. All devices should follow uniform security configurations, automatic patching, and antivirus updates. Regular vulnerability assessments and penetration tests should be conducted to identify weaknesses proactively. Additionally, foreign service staff must receive hands-on training in secure digital practices, incident detection, and emergency response procedures to reduce operational exposure to cyber threats.

6.3. Policy and Strategic Reforms

A comprehensive Cyber Diplomacy Strategy is needed to align Ghana's foreign policy with cybersecurity priorities. This strategy should define clear protocols for data handling, threat reporting, digital communication, and coordination with domestic and international cybersecurity actors. Ghana should adopt international best practices from the AU Convention on Cybersecurity, ECOWAS frameworks, and relevant UN cyber norms. Strategic partnerships with technologically advanced countries, such as Estonia, South Korea, and Rwanda, should be strengthened to enhance knowledge exchange. Finally, cyber diplomacy must be embedded into foreign policy planning, allowing Ghana to proactively engage in global cyber negotiations and safeguard national interests.

7. Limitations

This study faced several limitations that should be acknowledged. First, access to detailed cybersecurity data from diplomatic missions was restricted due to confidentiality and security protocols, limiting the depth of technical analysis. Second, some embassies provided incomplete survey responses, resulting in gaps in comparative assessment. Third, the rapidly evolving nature of cyber threats means that some findings may shift over time as new attacks, technologies, or policies emerge. Lastly, the study relied partly on self-reported data, which may contain biases. Despite these limitations, the results provide a credible and evidence-based foundation for understanding Ghana's cyber diplomacy challenges.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Hansen, L. and Nissenbaum, H. (2017) Digital Disaster, Cyber Security, and the Copenhagen School. *International Studies Quarterly*, **53**, 1155-1175.

[2] Nye, J.S. (2010) Cyber Power. Harvard University, Belfer Center for Science and International Affairs.

[3] EU External Action Service (2022) EU Cyber Diplomacy Toolbox.

[4] United Nations (2021) UN Group of Governmental Experts Report on Developments in the Field of ICTs in the Context of International Security.

[5] Tanczer, L. (2019) Cybersecurity and Developing Countries. *Third World Quarterly*, **40**.

[6] Cornish, P., Hughes, R. and Livingstone, D. (2009) Cyberspace and the National Security of the United Kingdom. Chatham House.

[7] Nakashima, E. (2014) Russian Hackers Targeted State Department. The Washington Post.

[8] Sanger, D. and Perlroth, N. (2018) Hackers breached EU diplomatic cables. The New York Times.

[9] Bjola, C. and Manor, I. (2020) Digital Diplomacy and International Organizations. Routledge. https://doi.org/10.4324/9781003032724

[10] Rid, T. and Buchanan, B. (2014) Attributing Cyber Attacks. *Journal of Strategic Studies*, **38**, 4-37. https://doi.org/10.1080/01402390.2014.977382

[11] Banham, C. (2011) DFAT Cyber Attack 'Unprecedented'. Sydney Morning Herald.

[12] (2015) The OPM Data Breach. Harvard Kennedy School.

[13] Meservey, J. (2020) The African Union's Huawei-Installed Systems Were Compro-

mised. Foreign Policy Research Institute.

[14] Greene, T. (2019) Insider Threats in Diplomatic Networks. *Journal of Cyber Policy*, **4**.

[15] African Union (2014) African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention) African Union.

[16] ECOWAS Commission (2010) Supplementary Act on Cybersecurity and Personal Data Protection.

[17] Data Protection Commission (2012) Data Protection Act, 2012 (Act 843) Government of Ghana.

[18] Cyber Security Authority (CSA) of Ghana (2023) National Cybersecurity Report. Cyber Security Authority.

[19] ISO (2020) ISO/IEC 27014:2020. Information Security, Cybersecurity and Privacy Protection-Governance of Information Security.

[20] Von Solms, R. and Von Solms, S. (2009) Information Security Governance. Springer. https://doi.org/10.1007/978-0-387-79984-1

[21] Cyber Security Authority (CSA) of Ghana (2021) Ghana National Cybersecurity Policy & Strategy (2021-2025) Government of Ghana.

[22] Mihr, A. (2022) Cyber Diplomacy: Managing Foreign Policy in the Digital Age. Springer.

[23] Tikk, E. and Kerttunen, M. (2020) Routledge Handbook of International Cybersecurity. Routledge. https://doi.org/10.4324/9781351038904

[24] AU Commission (2022) African Union Cybersecurity Capacity Building Reports 2022. African Union.

[25] Council of the European Union (2021) EU Cyber Diplomacy Toolbox. Council of the European Union.

[26] Ottis, R. (2013) Analysis of the 2007 Cyber Attacks against Estonia from the Information Warfare Perspective. Estonian Defence Forces.

[27] Rwanda Ministry of ICT (2020) National Cybersecurity Policy. Government of Rwanda.