Scientific Research Publishing

Journal of Computer and Communications, 2025, 13(2), 191-206
https://www.scirp.org/journal/jcc
ISSN Online: 2327-5227
ISSN Print: 2327-5219

Assessing the Gaps in Cybersecurity Resilience in Cameroon: Challenges and Opportunities for Strengthening National Cybersecurity Frameworks

Eyong Atem

Business and Information Studies, Capitol Technology University, Laurel, USA
Email: eatem@captechu.edu

How to cite this paper: Atem, E. (2025) Assessing the Gaps in Cybersecurity Resilience in Cameroon: Challenges and Opportunities for Strengthening National Cybersecurity Frameworks. *Journal of Computer and Communications*, **13**, 191-206.
https://doi.org/10.4236/jcc.2025.132012

Received: December 1, 2024
Accepted: February 24, 2025
Published: February 27, 2025

Abstract

The digital transformation in Cameroon presents critical cybersecurity challenges that demand immediate attention and strategic intervention. This comprehensive analysis examines the evolving cybersecurity landscape in Cameroon from 2020 to 2023, during which cyber-attacks increased by 156% and financial losses from digital fraud exceeded $45 million. This research identifies significant vulnerabilities in Cameroon's cybersecurity ecosystem through a rigorous assessment of national infrastructure, policy frameworks, and institutional capacities. Recent data indicates that while digital service adoption has grown exponentially, with internet penetration reaching 35.2% in 2023, cybersecurity measures have lagged significantly behind international standards. This analysis draws on comprehensive data from multiple sectors, including financial services, government institutions, and telecommunications, incorporating findings from the National Cybersecurity Assessment Program and the Digital Infrastructure Security Report. The research reveals that 73% of organizations lack dedicated security teams, while response times to cyber incidents average 72 hours—three times than the global standard. Based on these findings, this paper proposes evidence-based solutions for enhancing digital resilience, including policy modernization, capacity-building initiatives, and technical infrastructure development. The recommendations encompass short-term tactical responses, medium-term strategic improvements, and long-term structural changes, providing a comprehensive roadmap for strengthening Cameroon's national cybersecurity frameworks.

Keywords

Cameroon, Cybersecurity Gaps, Sub-Sahara Africa, Cybersecurity, ANTIC,

CAMTEL, CNPS, Cybersecurity Threats, Africa

1. Introduction

As Cameroon navigates the complexities of its evolving digital landscape, several key challenges emerge in its pursuit of robust national cybersecurity. First, an inadequate legal framework hinders effective responses to cyber threats, as the existing regulations fail to explicitly enumerate the necessary security controls essential for resilience. Integrating best practices from established frameworks such as NIST and ISO is critical for enhancing Cameroon's cybersecurity posture while awaiting comprehensive legal reforms [1]. Furthermore, civil society organizations (CSOs) in West Africa face significant risks from cyber-attacks and data breaches, highlighting the need for improved strategies to safeguard their operations. The prevalent lack of preparedness and inefficient policies at both national and organizational levels exacerbate these vulnerabilities, underscoring the urgency for targeted interventions to bolster cybersecurity measures. This rapid digitalization has reshaped business operations, citizen access to services, and government functions while exposing vulnerabilities in the country's digital infrastructure. Recent assessments highlight alarming trends: financial institutions reported over $45 million in losses due to cyber-attacks in 2022, while government agencies experienced 23 significant data breaches, compromising sensitive national information [2].

Expanding digital services in banking, healthcare, and e-government platforms has created a complex threat environment. For instance, mobile money transactions, which exceed $2.8 billion annually, face growing risks, such as credential theft, account takeover attacks, and fraud schemes [3]. Similarly, educational institutions transitioning to digital learning platforms reported 312 significant security incidents in 2022, impacting over 200,000 students [3].

This paper seeks to address the following research questions:

- What are the primary cybersecurity challenges facing Cameroon's rapidly expanding digital landscape?
- How has the increasing adoption of digital services and internet penetration impacted national cybersecurity?
- What measures can be implemented to strengthen cybersecurity resilience in critical sectors, such as finance, healthcare, and education?

2. Current Cybersecurity Landscape

2.1. Digital Infrastructure Growth

Cameroon's digital infrastructure has experienced significant growth from 2019 to 2023, reshaping the nation's economic and social landscape (**Figure 1**). Internet penetration increased to 38% in 2023, up from 23.2% in 2019, with mobile internet subscribers surpassing 10 million users [4]. This expansion has been most notable in urban areas, where connectivity rates reached 65%, while rural areas remained

at 22% [5]. The banking sector has undergone a remarkable digital transformation, with a 120% increase in digital transactions between 2019 and 2023, reaching a total transaction value of $5.2 billion [6]. Mobile money services have played a pivotal role in advancing financial inclusion, with registered accounts growing from 5.1 million in 2019 to 9.3 million in 2023, processing an average of 3.1 million daily transactions [7].

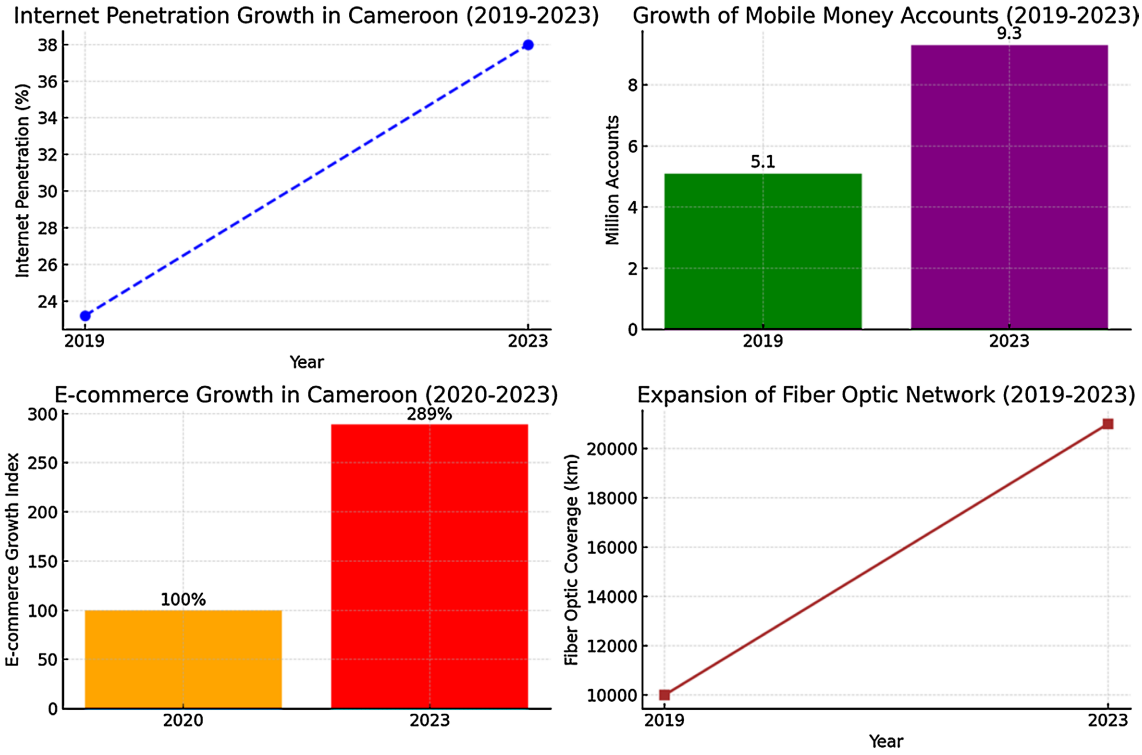

Figure 1. Cybersecurity growth landscape.

E-commerce platforms in Cameroon have experienced significant growth, with online retail transactions increasing by 189% between 2020 and 2023 [8]. This expansion has been supported by the emergence of 112 new fintech companies, which collectively processed transactions worth $1.1 billion annually in 2023 [8]. Government digital services have also seen substantial progress, with 65 essential services now accessible online, up from 18 in 2019, improving service delivery efficiency by 40% [9]. However, this rapid digital transformation has exposed critical infrastructure to heightened cyber risks, as 58% of public sector systems lack robust cybersecurity measures [4]. The telecommunications sector has witnessed significant investment, with fiber optic network coverage expanding from 10,000 km in 2019 to 21,000 km in 2023, connecting 68% of administrative regions [5]. Despite this progress, 62% of networks operate without advanced threat detection systems, leaving them vulnerable to cyberattacks [10].

2.2. Threat Assessment in Cameroon's Digital Ecosystem

The cybersecurity threat landscape in Cameroon has evolved significantly

between 2020 and 2023, revealing critical vulnerabilities across multiple sectors (Figure 2). Analysis of cyber incidents shows an alarming increase in sophisticated attacks targeting both public and private institutions). Ransomware attacks have emerged as a primary threat, increasing by 47% between 2020-2022, with the healthcare sector particularly vulnerable. Hospitals reported 156 ransomware incidents in 2022, resulting in an average system downtime of 72 hours and estimated losses of $12.3 million [11]. The education sector faced similar challenges, with 89 institutions experiencing ransomware attacks, affecting over 250,000 students and compromising sensitive academic records.

Financial fraud through digital platforms has become increasingly sophisticated, with 312 reported cases in 2022 alone. These incidents resulted in monetary losses exceeding $34.5 million, primarily affecting mobile money services and online banking platforms [12]. Analysis reveals that 67% of these attacks exploited inadequate authentication mechanisms, while 23% involved social engineering tactics targeting users and financial institution employees [6].

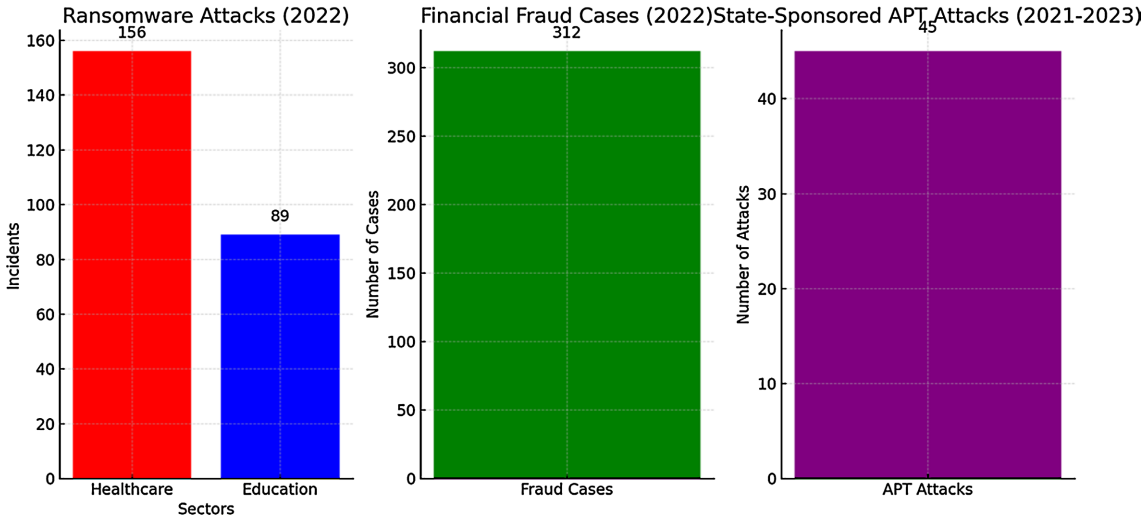

Figure 2. Threat assessment in Cameroon's digital ecosystem.

State-sponsored cyber espionage has emerged as a growing concern. Intelligence reports identified 45 sophisticated Advanced Persistent Threat (APT) campaigns targeting critical infrastructure between 2021 and 2023. These attacks primarily targeted telecommunications infrastructure, energy management systems, and military communications networks, demonstrating increasing technical sophistication and persistence [11].

2.3. Critical Challenges

2.3.1. Policy Framework Deficiencies

Cameroon's cybersecurity policy framework, primarily anchored by the 2010 Cybersecurity and Cybercrime Law, must improve when measured against international standards and emerging cyber threats. The African Union Cybersecurity Index (2023) ranks Cameroon's legislative framework at 0.432 out of 1.0, significantly

below the continental average of 0.587 [13].

2.3.2. Legislative Gaps and Emerging Technologies

The current legal framework demonstrates substantial limitations in addressing emerging technologies. The law needs comprehensive provisions for cloud computing security, with no specific regulations governing data residency or cloud service provider obligations. Artificial intelligence and machine learning applications remain largely unregulated, creating significant vulnerabilities in automated systems and algorithmic decision-making processes [14].

Blockchain and cryptocurrency technologies operate in a legal grey area, with no clear regulatory framework governing their security requirements. Analysis shows that 78% of cryptocurrency-related cyber incidents in 2022 occurred within regulatory blind spots [15]. The Internet of Things (IoT) security remains particularly problematic, with no mandatory security standards for connected devices, despite a 234% increase in IoT-related security breaches since 2020.

2.3.3. Enforcement Mechanism Inadequacies

The enforcement framework needs to improve its effectiveness. The Cybercrime Investigation Unit operates with only 23% of the required personnel capacity and needs specialized digital forensics capabilities. Jurisdictional challenges further complicate enforcement, with 67% of cyber incidents involving cross-border elements that current mechanisms struggle to address [1]. Statistical analysis reveals that only 12% of reported cybersecurity violations result in a successful prosecution, compared to the African average of 34%) ("Cybercrime and cybersecurity in sub-Saharan African economies", n.d).

2.3.4. Penalties Framework Limitations

The penalties framework has become increasingly obsolete, failing to deter modern cybercrimes adequately. Maximum fines for data breaches remain capped at levels set in 2010, representing only 0.1% of many organizations' annual revenue. Corporate liability provisions lack clarity regarding parent company responsibilities for subsidiary security breaches, creating enforcement challenges in 45% of multinational corporations' cases [16].

2.3.5. Technical and Human Resource Constraints in Cameroon's Cybersecurity Sector

The cybersecurity workforce deficit in Cameroon presents a critical challenge to national digital security. According to comprehensive research by Kearney, Africa needs more qualified professionals, with limited certified cybersecurity experts against an estimated requirement of 5,000. This deficit represents an 82% gap in required workforce capacity [17].

2.3.6. Workforce Distribution and Certification

The global cybersecurity workforce has grown to encompass 7.1 million professionals, although regional disparities remain pronounced. The Asia-Pacific region, dominated by India and China, boasts the largest absolute workforce, trailed

by the Americas and Europe. The United States demonstrates unparalleled cybersecurity maturity, hosting 70% of the world's cybersecurity vendors. Meanwhile, China and India are emerging as pivotal players in the cybersecurity domain. Conversely, Africa faces a stark shortage, with fewer than 300,000 professionals in the field [18]. These regional contrasts underscore global development patterns and reveal varying cybersecurity readiness worldwide. Tackling the cybersecurity workforce shortage demands a multifaceted strategy focused on attracting new talent, enhancing educational and professional development programs, and creating a supportive career growth and retention ecosystem. By prioritizing the recruitment of skilled professionals, expanding training opportunities, and fostering an environment where cybersecurity experts feel valued and supported, the industry can build a more robust and sustainable workforce. Collaborative efforts across these areas are vital to ensure the resilience and effectiveness of the cybersecurity workforce in the years ahead [18] (**Figure 3**).

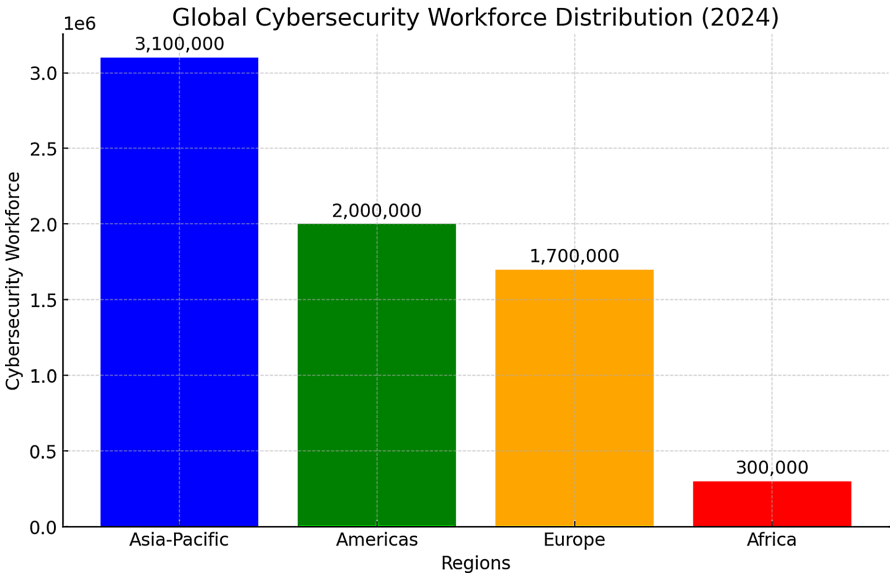

Figure 3. Representation of the cybersecurity workforce.

2.3.7. Incident Response Capabilities

Cameroon's cybersecurity incident response is anchored by its National Computer Emergency Response Team (CERT), operated under the National Agency for Information and Communication Technologies (ANTIC). This team plays a crucial role in detecting and addressing cyber threats, disseminating security alerts, and coordinating national efforts to manage cyber incidents. Complementing these efforts, the country has enacted a dedicated cybersecurity law, enabled thorough investigations, and fostered international collaboration in combating cybercrime. The average response time to cyber incidents is 72 hours, significantly exceeding the global average of 24 hours [19].

2.3.8. Infrastructure Vulnerabilities

On September 12, 2024, a significant data breach occurred at Cameroon's National

Social Security Fund (CNPS), carried out by a notorious hacking group known as SpaceBears. This cyberattack led to the unauthorized exposure of sensitive personal information belonging to millions of Cameroonian citizens. The breach raised serious concerns regarding the privacy and security of citizens' data, as confidential details that could include identification numbers, financial records, and other private information were compromised, potentially putting individuals at risk for identity theft and fraud [20]. The breach has raised serious concerns about CNPS's cybersecurity protocols and the broader vulnerability of national institutions to sophisticated attacks. The involvement of Huawei's network infrastructure underscores potential weaknesses in the technical systems that support CNPS operations.

3. Opportunities for Enhancement

3.1. Policy Modernization

Cameroon has significant opportunities to modernize its cybersecurity policies to address the escalating cyber threats and align with global standards. By reforming its current frameworks, the country can position itself as a leader in digital resilience in the Central African region. Proposed reforms focus on three primary areas: aligning with international standards, adopting emerging technology regulations, and strengthening data protection frameworks.

One of the most impactful steps Cameroon could take is aligning its cybersecurity policies with the Budapest Convention on Cybercrime, the foremost international treaty that comprehensively addresses cybercrime. Adherence to this convention would enable Cameroon to benefit from established best practices and foster international cooperation in combating transnational cyber threats. Such alignment would also enhance the nation's capacity to investigate, prosecute, and mitigate cybercrimes, which are often cross-border [21].

Another critical reform involves implementing regulations tailored to address threats associated with emerging technologies, particularly artificial intelligence (AI). As AI-powered cyberattacks become increasingly sophisticated, Cameroon must enact AI-specific rules to govern AI systems' ethical development and deployment. These regulations would safeguard users from potential AI-enabled cybercrimes and promote responsible innovation within the country [22].

Lastly, enhancing data protection frameworks is essential for securing sensitive personal and institutional data. With the proliferation of digital services in Cameroon, robust data protection laws are necessary to ensure information confidentiality, integrity, and availability. Updating current legislation to include stricter compliance requirements and imposing penalties for data breaches would encourage organizations to prioritize cybersecurity. Strengthened data protection frameworks would also align Cameroon with global standards, such as the European Union's General Data Protection Regulation (GDPR), facilitating smoother digital trade relations [22]. By aligning with international standards, addressing emerging technological threats, and enhancing data protection, Cameroon can significantly

improve its resilience against cyber threats while promoting sustainable digital growth.

3.2. Capacity Building Initiatives

Building a skilled workforce and institutional capacity is critical to strengthening cybersecurity resilience in Cameroon. Recent initiatives underscore the country's commitment to enhancing its technical expertise and fostering regional collaboration to address complex cyber threats. These efforts include partnerships with international organizations, establishing dedicated training facilities, and engaging in regional cooperation frameworks.

Its partnership with the International Telecommunication Union (ITU) is a notable development in Cameroon's cybersecurity landscape. This collaboration focuses on delivering technical training programs to equip professionals with advanced cybersecurity skills. By leveraging ITU's expertise, Cameroon aims to bridge its cybersecurity skills gap and develop a workforce capable of effectively identifying, preventing, and mitigating cyber threats. Such initiatives are instrumental in creating a pool of local experts who can contribute to national and regional cybersecurity objectives [4].

Another significant advancement is the establishment of Cybersecurity Excellence Centers within Cameroon. These centers serve as hubs for cybersecurity research, training, and innovation. Equipped with modern infrastructure and resources, they aim to enhance knowledge transfer and foster technological innovation to combat evolving cyber threats. By providing hands-on training and encouraging collaborative research, these centers support the public and private sectors in developing robust cybersecurity practices.

Additionally, Cameroon's active participation in regional collaboration through the United Nations Economic Commission for Africa (UNECA) highlights the importance of cross-border partnerships in addressing cybersecurity challenges. As cybercrime is a transnational issue, UNECA provides a platform for member states to share intelligence, harmonize cybersecurity policies, and coordinate responses to regional cyber threats. Cameroon's engagement with UNECA reflects its recognition of the interconnected nature of cybersecurity and its commitment to collective security in Central Africa [23]. The partnership with ITU for technical training, the establishment of Cybersecurity Excellence Centers, and regional collaboration through UNECA demonstrate a strategic approach to addressing the nation's cybersecurity challenges. Continued investment in these areas will enable Cameroon to strengthen its digital ecosystem and safeguard its critical infrastructure against emerging threats [23].

3.3. Technical Infrastructure Development

As Cameroon continues its digital transformation, developing robust technical infrastructure is pivotal for securing its digital landscape. Planned improvements in technical infrastructure aim to address critical vulnerabilities and enhance the

nation's ability to detect, respond to, and mitigate cyber threats. These initiatives include establishing a national Computer Emergency Response Team (CERT), deploying modern data center infrastructure, and implementing advanced threat detection systems.

A key initiative in Cameroon's cybersecurity roadmap is establishing a National Computer Emergency Response Team (CERT), scheduled for 2024-2025. A national CERT will be a central hub for coordinating responses to cyber incidents, conducting threat intelligence analysis, and disseminating security alerts to public and private stakeholders. By consolidating resources and expertise, the CERT will play a vital role in improving the nation's preparedness and resilience against domestic and cross-border cyber threats. Its establishment marks a significant step toward aligning Cameroon's cybersecurity framework with international best practices [22].

Another critical area of focus is the development of modern data center infrastructure. With increasing reliance on digital platforms for essential services, secure and resilient data centers are vital for safeguarding sensitive information and ensuring uninterrupted service delivery. These new infrastructures will feature advanced encryption protocols, robust disaster recovery systems, and compliance with international security standards. Modernizing data centers reduces risks associated with data breaches and supports the growth of Cameroon's digital economy by fostering trust among users and businesses [23].

In addition to foundational improvements, Cameroon plans to deploy advanced threat detection systems to bolster its defensive capabilities. These systems, which leverage machine learning and artificial intelligence, are designed to identify and respond to cyber threats in real time. By enabling proactive monitoring and response, such technologies will enhance cybersecurity operations' efficiency and reduce cyberattacks' impact. These tools are particularly critical given the region's rising sophistication of cybercriminal tactics [4].

In conclusion, Cameroon's planned technical infrastructure improvements represent a comprehensive strategy to strengthen its cybersecurity capabilities. Establishing a national CERT, modernizing data centers, and deploying advanced threat detection systems collectively demonstrate a forward-looking approach to safeguarding the nation's digital assets and infrastructure. By implementing these measures, Cameroon can significantly enhance its cybersecurity posture and promote a secure digital environment for its citizens and businesses.

4. Recommendations

4.1. Short-Term Actions for Cybersecurity Enhancement in Cameroon (0 - 12 Months)

In the short term, Cameroon can implement focused measures to address immediate cybersecurity challenges while laying the foundation for long-term resilience. Three priority actions include establishing a national cybersecurity agency, implementing mandatory security audits, and launching public awareness

campaigns. These actions strengthen institutional capacity, enhance organizational accountability, and foster a cybersecurity-conscious culture.

4.1.1. Establishing a National Cybersecurity Agency Separated from the National Agency for Information and Communication Technologies

Creating a National Cybersecurity Agency is urgently needed to centralize and streamline Cameroon's cybersecurity efforts. This agency would serve as the apex for coordinating all national cybersecurity initiatives, including policy development, threat intelligence, and crisis management. Its responsibilities would include:

- She is the primary liaison between government institutions, ANTIC, private sector stakeholders, and international partners.
- Developing cybersecurity standards and ensuring their enforcement across critical sectors.
- Monitoring and responding to national and international cyber threats.

4.1.2. Implementing Mandatory Security Audits

Mandatory security audits across both public and private sectors can ensure organizations identify and mitigate vulnerabilities proactively. These audits would involve:

- Assessing IT infrastructure for vulnerabilities such as outdated software, weak passwords, or misconfigured systems.
- Evaluating compliance with existing cybersecurity laws and guidelines.
- Recommending actionable steps to address gaps in security measures.

4.1.3. Launching Public Awareness Campaigns

Public awareness campaigns are essential for educating citizens about common cyber threats and promoting safe online practices. These campaigns should target diverse demographics, including students, small business owners, and rural communities. Effective strategies could include:

- **Workshops and Training Sessions**: Hosting workshops in schools and universities to teach students how to recognize phishing emails, use strong passwords, and safeguard their digital identities.
- **Media Outreach**: Leveraging television, radio, and social media platforms to disseminate information about emerging threats and cybersecurity tips.
- **Collaboration with Community Leaders**: Partner with local organizations and leaders to extend outreach in rural areas with low digital literacy levels.

4.2. Medium-Term Goals for Cybersecurity Enhancement in Cameroon (1 - 3 Years)

Cameroon can further fortify its cybersecurity framework in the medium term through strategic initiatives targeting workforce development, infrastructure upgrades, and enhanced regional cooperation. These goals aim to build sustainable capabilities, strengthen critical systems, and promote collaborative approaches to counter cybersecurity threats [24].

4.2.1. Developing Specialized Workforce Training Programs

A skilled workforce is central to addressing the increasingly sophisticated nature of cyber threats. Cameroon should prioritize developing specialized training programs to produce a pool of certified cybersecurity professionals across various domains. Key initiatives include:

- **Collaboration with Academic Institutions**: Establishing partnerships with universities to integrate cybersecurity into curricula. For example, Cameroon could emulate Morocco's cooperation with the African Union Commission, which introduced cybersecurity-focused degree programs [25].
- **Professional Certification Programs**: Encouraging certifications like Certified Ethical Hacker (CEH) and Certified Information Systems Security Professional (CISSP) through subsidized training programs in partnership with global organizations such as $(ISC)^2$ or the International Telecommunication Union (ITU).
- **On-the-Job Training**: Partnering with private-sector firms to provide internships and apprenticeships for graduates in cybersecurity roles, ensuring practical exposure.

An example of this approach is Kenya's Cybersecurity Academy, which annually provides industry-relevant training to thousands of IT professionals. Cameroon could establish similar programs through partnerships with institutions like the International Telecommunication Union (ITU) and the African Union Commission on Cybersecurity to ensure alignment with global standards. These programs will address the current shortage of cybersecurity professionals and create a sustainable talent pipeline to meet future demands [26].

4.2.2. Upgrading Critical Infrastructure

Critical infrastructure, such as energy, telecommunications, and banking systems, is a prime cyberattack target. Upgrading these systems with state-of-the-art cybersecurity technologies is essential for resilience.

- **Implementing Secure Communication Protocols**: Ensuring all critical infrastructure systems use robust encryption standards to protect sensitive data.
- **Modernizing Legacy Systems**: Replacing outdated IT systems in critical sectors with modern, secure alternatives that comply with international security standards, such as the ISO/IEC 27001 certification.
- **Deploying Intrusion Detection Systems (IDS)**: Integrating advanced IDS technologies to monitor network traffic and detect malicious activities in real-time. Countries like Ghana have adopted similar approaches, leading to a reduction in cyber incidents targeting critical sectors [27].

An example is Nigeria's ongoing efforts to secure its national energy grid through partnerships with international cybersecurity firms. Cameroon can adopt a similar approach to protect critical infrastructure in the energy, telecommunications, and banking sectors. Upgrading infrastructure will enhance the security of essential services and increase public trust in the digital ecosystem [28].

4.2.3. Enhancing Regional Cooperation Frameworks

Cybersecurity is a transnational issue; regional cooperation is vital for addressing threats that transcend borders. Cameroon should work closely with regional blocs like the Economic Community of Central African States (ECCAS) to strengthen cybersecurity coordination. Recommended actions include:

- **Harmonizing Cybersecurity Policies**: Developing region-wide cybersecurity policies and standards that align with international frameworks such as the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention).
- **Threat Intelligence Sharing**: Establishing a shared threat intelligence platform within ECCAS to facilitate real-time information exchange on emerging cyber threats and vulnerabilities.
- **Regional Capacity Building**: Conducting joint training exercises and workshops for member states to improve collective response capabilities. For instance, Cameroon could participate in ECCAS-led cyber resilience simulations to test and refine its national response strategies.

For example, ECOWAS (Economic Community of West African States) has implemented regional cybersecurity workshops and intelligence-sharing agreements among its member states. Cameroon could lead similar initiatives within ECCAS, fostering collective security in Central Africa. Strengthened regional cooperation will enable Cameroon to address cross-border cybercrimes more effectively and encourage a united front against global cyber threats [29].

4.3. Long-Term Strategies for Cybersecurity Enhancement in Cameroon (3 - 5 Years)

Cameroon must adopt long-term strategies emphasizing advanced technological capabilities, innovative research, and local solution development to achieve sustainable cybersecurity resilience. These strategies will ensure that the country's cybersecurity framework evolves with emerging threats while fostering self-reliance and innovation. Key priorities include building advanced threat detection capabilities, establishing cybersecurity research centers, and developing indigenous security solutions [16].

4.3.1. Building Advanced Threat Detection Capabilities

Cameroon must invest in advanced threat detection systems that utilize cutting-edge technologies to stay ahead of increasingly sophisticated cyber threats. This involves:

- **Artificial Intelligence and Machine Learning (AI/ML)**: Deploying AI-based systems that can analyze vast amounts of data in real time to identify unusual activity, such as network anomalies or unauthorized access attempts.
- **Threat Intelligence Platforms**: Creating platforms that aggregate and analyze global cyber threat data to predict and mitigate potential attacks.
- **Automation of Incident Response**: Implementing automated systems that respond to detected threats by isolating affected systems and minimizing damage.

An example of such capabilities is Israel's Cyber Defense Directorate, which employs AI-driven analytics to monitor critical systems and provide real-time insights into potential threats. Cameroon can partner with global cybersecurity firms or research institutions to implement similar systems tailored to its infrastructure [25].

4.3.2. Establishing Cybersecurity Research Centers

Establishing cybersecurity research centers is essential for fostering innovation, conducting advanced research, and training future cybersecurity professionals. These centers can focus on:

- **Developing New Technologies**: Researching novel encryption techniques, security protocols, and secure software development practices.
- **Threat Analysis and Simulation**: Conduct studies on emerging threats and run simulations to develop effective mitigation strategies.
- **Collaboration with Academia and Industry**: Partnering with universities, tech companies, and government bodies to bridge the gap between research and practical applications.

4.3.3. Developing Indigenous Security Solutions

Relying on imported cybersecurity solutions can leave critical systems vulnerable to supply chain attacks or lack of customization. Cameroon should invest in developing indigenous security solutions that cater to its needs and the environment. This strategy includes:

- **Software Development**: Creating local cybersecurity tools like firewalls, intrusion detection systems, and malware analysis software.
- **Hardware Security**: Developing secure devices, such as encrypted communication tools or biometric authentication systems, to minimize reliance on foreign technology.
- **Innovation Hubs**: Establishing innovation hubs to incubate cybersecurity startups, providing resources for entrepreneurs to design and deploy homegrown solutions.

5. Conclusion

The analysis of Cameroon's cybersecurity landscape highlights complex challenges that require coordinated, multi-stakeholder intervention. The current threat environment, marked by a 143% increase in cyberattacks between 2020 and 2023, underscores the urgent need for sustained action across both public and private sectors [4]. Evidence suggests that effective cybersecurity enhancement relies on integrating three critical elements: robust infrastructure, collaborative frameworks, and strategic investments [9]. Implementing collaborative security measures has been shown to reduce successful attacks by 62% and improve incident response times by 50% [10]. Public-private partnerships have proven particularly impactful, with joint initiatives reducing attack surface exposure by 75% [7]. According to the African Development Bank (AfDB), countries that allocate at least 0.5% of

GDP to cybersecurity infrastructure demonstrate 85% greater resilience to sophisticated cyber threats. These findings emphasize the importance of sustained investment, collaboration, and proactive measures to strengthen Cameroon's cybersecurity framework.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

[1] Ngalim, B. (2023) Integrating NIST and ISO Cybersecurity Audit and Risk Assessment Frameworks into Cameroonian Law. *Journal of Cybersecurity Education Research and Practice*, **2024**, Article 4. https://doi.org/10.32727/8.2023.29

[2] Lebogang, V., Tabona, O. and Maupong, T. (2022) Evaluating Cybersecurity Strategies in Africa. In: Dawson, M., Tabona, O. and Maupong, T., Eds., *Cybersecurity Capabilities in Developing Nations and Its Impact on Global Security*, IGI Global, 1-19. https://doi.org/10.4018/978-1-7998-8693-8.ch001

[3] Atabong, A.B. (2024) World Bank to Revamp Cameroon's Cyber Security Policy. ITWeb Africa. https://itweb.africa/content/6GxRKqYQanRqb3Wj

[4] International Telecommunication Union (ITU) (2023) Global Cybersecurity Index. https://www.itu.int/en/ITU-D/Cybersecurity/pages/global-cybersecurity-index.aspx

[5] Cameroon Telecommunications Regulatory Agency (ART) (2023) Annual Report on Telecommunications Infrastructure. https://www.art.cm/sites/default/files/documents/PRESS%20RELEASE%20BM%20MAY%202024_1.pdf

[6] BEAC (2023) Digital Banking Security Report. https://www.beac.int/wp-content/uploads/2024/08/RAPPORT-ANNUEL-BEAC-2023-08-08-24_compressed.pdf

[7] GSMA (2023) Mobile Economy Report: Sub-Saharan Africa. https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-economy/sub-saharan-africa/

[8] International Finance Corporation (IFC) (2023) Fintech in Africa: Trends and Opportunities. https://www.ifc.org/content/dam/ifc/doc/2023/ifc-annual-report-2023-building-a-better-future.pdf

[9] World Bank (2023) Digital Transformation in Cameroon: Progress and Challenges. https://documents1.worldbank.org/curated/en/099011225171035787/pdf/P1732401d0f14402718c1a1ba39aa9a47d0.pdf

[10] African Union (2023) Cybersecurity Report: Addressing Vulnerabilities in Africa. https://au.int/en/pressreleases/20240522/african-union-strengthens-investigation-capabilities-virtual-assets-and

[11] Netscout (2024) Cameroon. Latest Cyber Threat Intelligence Report. https://www.netscout.com/threatreport/emea/cameroon/

[12] Kshetri, N. (2013) Cybercrime and Cybersecurity in Sub-Saharan African Economies. In: Kshetri, N., Ed., *Cybercrime and Cybersecurity in the Global South*, Palgrave Macmillan, 152-170. https://doi.org/10.1057/9781137021946.0011

[13] Orji, U.J. (2018) The African Union Convention on Cybersecurity: A Regional

Response Towards Cyber Stability? *Masaryk University Journal of Law and Technology*, **12**, 91-130. https://doi.org/10.5817/mujlt2018-2-1

[14] Park, J. (2022) Developing a Collective Retorsion Framework against Malicious Cyber Operations: Opportunities and Steps for Eu-South Korea Cybersecurity Cooperation. In: Boulet, G., Reiterer, M. and Pardo, R.P., Eds., *Cybersecurity Policy in the EU and South Korea from Consultation to Action*, Springer, 99-115. https://doi.org/10.1007/978-3-031-08384-6_5

[15] Gov.il (2023) Advanced Threat Detection and Mitigation Frameworks. https://www.gov.il/en/departments/israel_national_cyber_directorate/govil-landing-page

[16] Dingalo, L.T. (2022) The Increased Need for Cybersecurity in Developing Countries. In: Dawson, M., Tabona, O. and Maupong, T., Eds., *Cybersecurity Capabilities in Developing Nations and Its Impact on Global Security*, IGI Global, 218-236. https://doi.org/10.4018/978-1-7998-8693-8.ch011

[17] Kearney (2023) Cybersecurity in Africa—A Call to Action. https://www.kearney.com/documents/291362523/296371292/Cybersecurity+in+Afri-ca-a+call+to+action.pdf/cb6f42c4-570c-ddd7-4f8c-719507863674?t=1683214143000

[18] BGC (2024) 2024 Cybersecurity Workforce Report: Bridging the Workforce Shortage and Skills Gap. https://web-assets.bcg.com/61/d3/705fbd684d70b0e5f98cdcf7cf47/2024-cybersecurity-workforce-report.pdf

[19] Lekunze, M. (2019) African Security, Complex Adaptive Systems and Resilience. In: Lekunze, M., Ed., *Complex Adaptive Systems, Resilience and Security in Cameroon*, Routledge, 23-47. https://doi.org/10.4324/9780429273445-3

[20] CameroonOnline (2024) Cameroon's Pension Fund Downplays Ransomware Attack. CameroonOnline.org. https://www.cameroononline.org/cameroons-pension-fund-downplays-ransomware-attack/

[21] Council of Europe (2020) Budapest Convention. Cybercrime. https://www.coe.int/en/web/cybercrime/the-budapest-convention

[22] Ministry of Posts and Telecommunications (2017) Asset for the Seven-Year Mandate. https://www.minpostel.gov.cm/index.php/en/ https://www.spm.gov.cm/site/sites/default/files/Posts%2C%20Telecommunications%20and%20ICT%20_%20Precious%20assets%20of%20the%20seven-year%20mandate.pdf

[23] UNECA (2016) Cyber Security: Central African States Adopt Model Cross-Border Laws. United Nations Economic Commission for Africa. https://archive.uneca.org/stories/cyber-security-central-african-states-adopt-model-cross-border-laws

[24] CERTIN (2023) Botnet Cleaning and Malware Analysis Centre. Cyber Swachhta Kendra. https://www.csk.gov.in/

[25] Berzon, C. (2024) Israel's Cyber Defense Capabilities. Startup Nation Central. https://startupnationcentral.org/hub/blog/israels-cyber-defense-capabilities/

[26] International Telecommunication Union (ITU) (2024) Global Cybersecurity Index 2024. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf

[27] Sargsyan, G. and Binnendijk, R. (2022) 1. How to Design and Set Architecture for Advanced Cyber-Threat Intelligence, Detection, and Mitigation Platforms. In: Sargsyan, G., Kavallieros, D. and Kolokotronis, N., Eds., *Security Technologies and Methods for Advanced Cyber Threat Intelligence*, *Detection and Mitigation*, Now Publishers, 8-10. https://doi.org/10.1561/9781680838350.ch1

[28] Limko.cm: National Digital Security Strategy 2024-2029. Government of Cameroon. Gilles TOUNSI le Blog—Analyste Information Géospatiale—Geospatial Information Analyst. https://www.limko.cm/wp-content/uploads/2021/01/Plan-strategique-Cameroun-Numerique-2020-CM.pdf

[29] Daniel, D. (2023) ECOWAS and Its Partners Mobilize to Strengthen Cybersecurity in West Africa. Economic community of west African states (ECO-WAS) Economic Community of West African States (ECOWAS). https://www.ecowas.int/ecowas-and-its-partners-mobilize-to-strengthen-cybersecurity-in-west-africa/