National Cyber Security Policy and Strategy of Ghana: A Qualitative Analysis

[Name]

TABLE OF CONTENTS

Abstract

In today's society, cyberspace has become unavoidable due to its virtual dimension and global access. Many countries' national and international communities strive to put maximum effort into developing Cyber Security Policies and Strategies. This research proposal addresses the National Cyber Security policy and strategy in Ghana. The cyber menace in Ghana has turned into cyber fraud exceptionally. Due to inadequate laws on cybercrime, cybercriminals continue to fraud unsuspected internet users for a large amount of money. There is a critical need to address all factors and conditions of cyberspace to fulfil cyber security through a constructive security policy. The need for strategies and procedures implemented by the government officials as the authoritative intervention is mandatory in getting rid of this issue prevailing in Ghana.

1. Introduction

Several nations have developed and published a National Cyber Security Strategy and Policy to overcome the global threats associated with cyberspace. The main aim of this research is to address the issues associated with cyber security policy and strategy in Ghana and what security measures and policies are developed on the national level (Azmi, 2016). The proposal initiates with a contextual background of the topic, followed by the aims and objectives of the research. The identification of problems, along with the study's rationale, is given afterwards. To study the impact, empirical studies are examined. In the last section, methodology implementation and conclusion are discussed.

1.1 *Background*

Recently, a number of cyber-attacks occurred in Ghana, including defacing various government websites (Mensah, 2019). These have had a denting effect on Ghana's cyber security

image. This study primarily indicates the weak elements of cyberinfrastructure and policies in the country and how they should be resolved.

The introduction of new innovative technologies has made cyberspace more vulnerable. All these increasing crimes have created the need for state officials to implement laws, boundaries, and principles. This cyber-attack issue has been the voice of many individuals, and adequate cyber tools are demanded to protect data (Baezner and Robin, 2018).

Many countries address their cyber risk issues through flexible and dynamic cyber strategies that help them detect the root cause and change the emerging environment. A similar approach is required in the developing nation of Ghana, where independent strategies are not implemented accurately (Tibben, 2016). The research under discussion suggests the tools and applications that help to reduce cyber threats and possible precautions in the information technology field.

1.2 *Research aims and Objectives*

- To examine the National Cyber Security Policy and Strategy in Ghana.
- To examine the strengths and limitations of these Policies and Strategies
- To identify potential risks and consequences due to cyber-attacks.
- To examine cyberspace security measures and strategies.
- To suggest new dimensions for cyber security policy and strategy in Ghana.

1.3 *Research Problem*

The focal problem identified for this study is the weak efforts and policies that do not fulfil the cyber security requirements. Also, cyberspace has advanced with time, and security

issues are emerging rapidly. Strong strategies and implementations are required in a country like Ghana where information technology is still developing (Affum, 2019).

1.4 Rationale of the Study

The study significantly underlines the cyberspace issues prevalent in Ghana, where information technology measures have not grown much. The cyber sector of Ghana has gone through more fraud than developments, which signifies the lack of security policies and implementation (Shafqat, 2016). The study addresses all aspects of cyberspace security and applies a multi-stakeholder concept to fight against cyber crimes.

1.5 Significance of the Study

This study will contribute to creating awareness for the proactive measure in securing cyberspace. It will also assist in pinpointing the risks involved in cyber-attacks. Certain tools and measures will also be highlighted to help improve cyber security in Ghana. These will require the implementation of new cyber security policy and strategy in Ghana. It is because there are a lot of cyberspace threats to the IT infrastructure in the future, which previously such attacks have led to serious consequences and loss of confidential and important data (Adu and Adjei, 2018).

1.6 Structure of the Study

The fundamental research focuses on the cyber-attacks on Ghana's IT infrastructure, which have exploited many governmental websites resulting in the loss of official data. The main structure of the study is to be followed throughout the counteracting to reduce such events and improve the whole environment of cyber security by introducing certain policies and awareness creation. Due to the crimes in the cyberspace of Ghana, new methods and novel ideas must be adapted as the current policies are not properly implemented and are worth enough to resolve this issue.

2. Literature Review

2.1 Definition of NCSS

National Cyber Security Strategy is primarily defined as the implementation of rules to protect the infrastructure of information technology, specifically from intrusion, unauthorized access and cybercrimes (Masood, 2016). There is a need for the effective use of technologies and devices to enhance security and protect data so that the data owner experiences no exploitation while the data controllers are all accounted for in the national cyber security policy and strategy in Ghana (Adu and Adjei, 2018). Ill management of cyberspace and inadequate measures for data protection leads to serious data losses.

2.2 Factors that Influence the Development of NCSS

Each country's particular characteristics and procedures affect the development of security policies that address the public. The prominent factors that influence developing security strategy and policy include the interest of stakeholders, economic priorities and potential resources to utilize for the implementation (Haddad, 2019). These components are significant to make an impact and overcoming the critical occurrences of cyber-attacks.

The National Vice President National Information Technology and Communication Authority of Ghana experienced the loss of official data because of hackers in 2015. All this happens because the companies who control these sites are not very concerned about safeguarding the data, which is a big factor in national cyber security (Africa Cyber Report, 2016). Similarly, the governmental agents of the economy's actions towards this are way below what they should be. All these factors make cyberspace less secure and more prone to cybercrimes and attacks (Adu and Adjei, 2018).

2.3 National Strategies and National Cyber Security Strategies

According to NATO, there are 63 official cyber strategies, some of which have also released their second versions to address cyberspace threats (Binder, 2019). A National Cyber Security Strategy is a common simple document in most nations facing similar cyber issues and managing them accordingly. To analyse the similarities that are still the same or not, a new tendency or logical step is expected from many nations. They may assess the similarities and resolve the issues by considering possible guidelines and policies applied respectively in all countries. However, no specific global solutions are projected to help countries develop their NCCSs (Affum, 2019).

In the UK, breaching cyberspace security costs the individual 3.14 million pounds (Ashford, 2015). The high cost of breaking the laws and accessing confidential data is a good strategy to overcome this issue. Even though there have been strategies in African countries for high-cost penalties for the person who breaches cyberspace, a lack of implementation and proper checks and balances leads to a higher ratio of cyber-attacks in African countries (Adu and Adjei, 2018).

The US government has established several policies that have helped the economy combat cybercrimes. The data was collected from all states of the United States, and the risks profile related to cyberspace were developed. A cyber security bill was passed by keenly looking at the risks involved (Alexander et al., 2019).

2.4 National Cyber Security Policy and Strategy of Ghana

There had been some Acts were passed by the government of Ghana for the protection of data. Electronic Protection Act, 2008 and Data Protection Act, 2012 were passed to improve

security and enhance data management in cyberspace. The data protection Act 2012 had some policies for the people who were in charge of controlling data, such as to keep up the transparency of the given data, risks involved to the personal data, and ensure protection by keeping in mind the identified risk to the personal data (Adu and Adjei, 2018).

The electronic protection act also laid rules and regulations for a well-managed, secured and safe environment for all data stakeholders. Some acts were considered a crime, such as falsely trying to take information and access to data, unauthorised access to records or devices, unfair means of getting electronic money transfer etc. All these policies are there, but Ghana is still not able to properly manage and protect the data, which indicates the inadequate implementation of policies because rules and regulations are there. Still, no focus is on applying those legislations (Africa Cyber Report, 2016).

Along with the strategies and policies being implemented by the Ghana government, there needs to be aware because people in Ghana have very limited knowledge about cyberspace security, which has tremendously led to various crimes and attacks in this area (de Bruijn and Janssen, 2017). The training which is to be given to the people controlling data is the most cost-effective method for making the data more protected and safe (Adu and Adjei, 2018) because it does not cost much to train people rather than implementing policies and spending on devices to protect data in the cyberspace.

3. Methodology

3.1 Research Philosophy

The current research will be based on the research philosophy of interpretivism, where the objective of the study is maintained, and it involves one-on-one interaction with the people,

which helps in letting them know about the mindset of the people (Packard, 2017). The approach of Interpretivism philosophy captures the views of the researcher or the applicants of the study and thus provides comprehensive information regarding the research problem. This research philosophy is utilised here as it provides assumptions and perspectives on various points, and the aim of the study is fulfilled from multiple points of view (Jebreen, 2012).

The NCSSs are highly structured documents and require a range of data for review and development in further implementation. Due to this, interpretivism is best suited to understand the mind of people through interaction.

3.2 Research Approach

In any research, there are broad research approaches, either inductive or deductive. In this study, an inductive research approach will be applied. Research is to be carried out where the inferences will be made by observation. The inductive approach is essential for this research as it provides reasoning that works from specific observations to a range of broader theories and generalisations. It is called a bottom-up approach as the conclusions are likely to be based on premises and involve a degree of uncertainty. Inductive arguments are based on observations by developing patterns through a series of hypotheses to propose results for the research questions. Inductive approach is very beneficial as it does not rely on disregarding theories to formulate results and aims to identify the patterns from existing theories to explore the research questions. Thus, learning from experience is fulfilled by attempting this approach (Burney, 2008).

In this study, the relationship of the given variables is investigated from scratch, and no such relationship among the variables has been discussed before (Rahi, 2017). The policies and strategies will be deduced from scratch, and inferences will be made by reasoning regarding the cyber-attacks and crimes prevalent in Ghana.

3.3 Research Design

The study will apply a secondary qualitative research design for measuring and understanding the in-depth reasons for cyberspace issues. Through a qualitative approach, significant security documents, case studies and pre-existed literature will be monitored and investigated in the context of the selected topic. Qualitative research provides a detailed and rich picture of certain research. The approach is identified as a more experiential approach as it captures a range of views and feelings of the target group. Also, the research approach is not bound by limitations; sometimes responses in numbers cannot reveal the detailed answer to the research questions then the qualitative analysis is performed to add context to the research. The approach provides useful insights for any research, and that is why recognised as a more flexible approach (Rahman, 2017).

Moreover, the pre-existed research work of the researchers' will is used to make inferences regarding the data controllers and the people who know about hacking. Additionally, the literature will be used to study current policies and how they can be applied effectively.

3.4 Data Collection Method

Since the research focuses on strategies and policies developed by different nations, the data collection method will be based on secondary data collection. The data for this purpose can be gathered widely through the internet by online journals, newspaper, and reports which has authentic source and a number of official websites which address the issue under discussion. Secondary data analysis is beneficial for this research as it provides a key function to examine an analytical approach to conclude effective results for the research. Furthermore, secondary data analysis can be easily assessed and takes a short time to evaluate by a researcher. It is also cost-

effective, and as it collects data from primary research, it gives exact and authentic information (Cacciattolo, 2015).

The researcher will gain a significant amount of data quickly, which is an advantage of this method. Secondary data will be collected to complete the literature review and help the study's findings. There has already been extensive research in this area because of the prevailing security issues in Ghana for many years especially regarding the cyber Security Policy and Strategy in Ghana.

3.4 Data Analysis Technique

As this research will follow the secondary data method, the technique to analyse this data will be content analysis. The overall theme and understanding of qualitative data are investigated in a content analysis process where critical findings and results are examined.

As discussed in the data collection methods, there has been a lot of research in this area of cyberspace security, which is why the access to data and then the interpretation of that data and providing evidence and reasoning will assist in this study. With the help of content analysis, qualitative data can easily be presented.

3.5 Research Limitations and Ethical Consideration

This study will have certain limitations while conducting the data collection and analysis process. Cyberspace is complex, so obtaining security concerned data at large appears to be a big difficulty. The researcher may have limited authentic information sources due to confidentiality and ethical concerns. Also, the official associations and representatives of National cyber security cannot be disclosed due to confidentiality.

The limitation the researcher will face is the time and money constraints as access to all the important data are not possible in a limited period. Moreover, some articles are not free of cost, which is why financing in this regard can be problematic for the researcher.

The researcher will also have limited access to several articles from journals because many articles are not readily available. Additionally, permission from the cited articles' authors is mandatory, as accessing personal work without their consent is highly unethical. As the research incorporates a secondary data collection method, the need for journal articles is mandatory.

4. Conclusion

There have been a number of technological improvements, but countries are not very concerned about the data's security, especially African countries. Most countries in the world have not developed strict cyber security, which is an alarming situation. The security of cyber is at stake in many developing nations like Ghana. The major differences in approaches of countries and policymakers tend to affect the development of national security strategies for cyberspace. Proper preparation and instructions about the prevalent risks of cyber crimes need to be given to the governing authorities so that the official governments' and local public data can also be secured.

Cybercrimes are more prevalent in African Countries, and awareness is the key determinant to tackle this issue as people in these countries are unaware of the measures and tools to incorporate to protect the data. Moreover, the data protection act and electronic protection act have been passed by the government of Ghana. Still, governmental agents are not entertained by implementing the policies, which leads to cyber-attacks. Therefore, the policies should be implemented, and heavy penalties should be imposed on the people who go against such laws.

The national cyber security policy and strategy in Ghana must be synchronized with other countries' strategies to sustain the nation’s security. Technology has helped economies, but access to data has been easier and more vulnerable. It is recommended to consider advanced associations of technology and cyber activities supported by cyber security on every platform.

5. Timescale

Task	Week 1	Week 2	Week 3	Week 4	Week 5	Week 6	Week 7	Week 8	Week 9	Week 10
Topic Research										
Proposal										
Chapter: Introduction										
Chapter: Literature Review										
Chapter: Research Methodology										
Chapter: Data Collection										
Chapter: Data analysis										
Conclusion and Recommendation										

References

Adu, K.K. and Adjei, E., 2018. The phenomenon of data loss and cyber security issues in Ghana. *foresight*.

Affum, c.h.r.i.s.t.i.a.n., 2019. *Cybersecurity Practices among Foreign Banks in Ghana* (Doctoral dissertation, University of Ghana).

Africa Cyber Report, 2016. *Achieving Cyber Security Resilience*: Enhancing Visibility and Increasing Awareness. Retrieved from: www.serianu.com (accessed on 5 July, 2017).

Alexander, A., Graham, P., Jackson, E., Johnson, B., Williams, T. and Park, J., 2019, June. An Analysis of Cybersecurity Legislation and Policy Creation on the State Level. In *National Cyber Summit* (pp. 30-43). Springer, Cham.

Ashford, W., 2015. Top 10 cyber crime stories of 2015. *Computer Weekly*.

Azmi, R., Tibben, W. and Win, K.T., 2016. Motives behind Cyber Security Strategy Development: A Literature Review of National Cyber Security Strategy.

Bada, M., Von Solms, B. and Agrafiotis, I., 2019. Reviewing national cybersecurity awareness in Africa: an empirical study.

Bada, M., Von Solms, B. and Agrafiotis, I., 2019. Reviewing National Cybersecurity Awareness for Users and Executives in Africa. *arXiv preprint arXiv:1910.01005*.

Baezner, M. and Robin, P., 2018. *Cyber Sovereignty*. ETH Zurich.

Bansah, E.A., 2018. The threats of using computerized accounting information systems in the banking industry. *Journal of Accounting and Management Information Systems*, *18*(3), pp.440-461.

Burney, A., 2008. Inductive and deductive research approach. *Department of Computer Science, University of Karachi, Pakistan*, p.22.

Cacciattolo, K., 2015. Analysis of the Effectiveness of the Secondary Analysis of Existing Data in Quantitative Techniques. 10.13140/RG.2.1.3368.1123.

Carr, M., 2016. Public-private partnerships in national cyber-security strategies. *International Affairs*, *92*(1), pp.43-62.

De Bruijn, H. and Janssen, M., 2017. Building cybersecurity awareness: The need for evidence-based framing strategies. *Government Information Quarterly*, *34*(1), pp.1-7.

Ennin, D. and Mensah, R.O., 2019. Cybercrime in Ghana and the Reaction of the Law. *JL Pol'y& Globalization*, *84*, p.36.

Haddad, C. and Binder, C., 2019. Governing through cybersecurity: national policy strategies, globalized (in-) security and socio-technical visions of the digital society. *ÖsterreichischeZeitschrift für Soziologie*, *44*(1), pp.115-134.

Jebreen, I., 2012. Using inductive approach as research strategy in requirements engineering. *International Journal of Computer and Information Technology*, *1*(2), pp.162-173.

Mori, S. and Goto, A., 2018. Review of National Cybersecurity Policies. In *PACIS* (p. 335).

Packard, M.D., 2017. Where did interpretivism go in the theory of entrepreneurship?. *Journal of Business Venturing*, *32*(5), pp.536-549.

Rahi, S., 2017. Research design and methods: A systematic review of research paradigms, sampling issues and instruments development. *International Journal of Economics & Management Sciences*, *6*(2), pp.1-5.

Rahman, M.S., 2017. The Advantages and Disadvantages of Using Qualitative and Quantitative Approaches and Methods in Language" Testing and Assessment" Research: A Literature Review. *Journal of Education and Learning*, *6*(1), pp.102-112.

Shafqat, N. and Masood, A., 2016. Comparative analysis of various national cybersecurity strategies. *International Journal of Computer Science and Information Security*, *14*(1), p.129.