REPUBLIC
OF GHANA

www.csa.gov.gh

NATIONAL CYBERSECURITY POLICY & STRATEGY

A Secure and Resilient Digital Ghana

contents

Foreword 3

Preface 4

Statement 5

Introduction 6

1.0 Background & Situational Analysis 8

1.1 Cybercrime & Cybersecurity Defined 9

1.2 Global Perspective 10

1.3 Ghana's Cybersecurity Landscape 12

1.4 Ghana's Cyberspace Threat Actors 16

1.5 Opportunities 20

2.0 Vision 21

3.0 Mission 21

4.0 Institutional Framework 22

4.1 National Cybersecurity Governance 23

4.2 Cyber Security Authority (CSA) 23

4.3 Joint Cybersecurity Committee (JCC) 23

Part One - National Cybersecurity Policy 26

5.0 Policy Statements 27

5.0.1 Policy Statement I – Legal Measures 27

5.0.2 Policy Statement II – Technical Measures 27

5.0.3 Policy Statement III – Organisational Measures 28

5.0.4 Policy Statement IV – Capacity Building 28

5.0.5 Policy Statement V – Cooperation 28

Part Two - National Cybersecurity Strategy 29

6.0 Strategic Imperatives 30

6.0.1 Build a Resilient Digital Ecosystem 32

6.0.1.1 Strategic Objectives 32
6.0.1.2 Strategic Initiatives & Implementation Plan 33
6.0.2 Secure Digital Infrastructure 35
6.0.2.1 Strategic Objectives 35
6.0.2.2 Strategic Initiatives & Implementation Plan 36
6.0.3 Develop National Capacity 38
6.0.3.1 Strategic Objectives 38
6.0.3.2 Strategic Initiatives & Implementation Plan 39
6.0.4 Deter Cybercrime 45
6.0.4.1 Strategic Objectives 45
6.0.4.2 Strategic Initiatives & Implementation Plan 46
6.0.5 Strengthen Cooperation 49
6.0.5.1 Strategic Objectives 49
6.0.5.2 Strategic Initiatives & Implementation Plan 50
7.0 Implementation 54
8.0 Monitoring and Evaluation 55
9.0 Funding for National Cybersecurity 58
10.0 Conclusion: Cybersecurity Beyond 2027 58
11.0 Acknowledgement 59
12.0 Annex 1: Acronyms 60
13.0 Annex 2: Glossary 62

foreword

Ghana's socio-economic development is inherently underpinned by digitalisation. Our Cybersecurity Policy and Strategy highlight the relevance of Ghana's digitalisation evolution to Ghana's short, medium and long term economic and social development. To sustain the above model of development, the need to scale up Ghana's cybersecurity readiness is paramount. Around the world, security is one of the hallmarks of a strong economy and a prerequisite for the maintenance of its sovereignty. For decades, Ghana has been considered one of Africa's safest nations due to its prioritisation of democratic development, economic growth, peace and security. However, in recent years and with the advent of ICT, security challenges have become more complex with changing trends particularly during the COVID-19 era where there has been an increased dependency on technology. The resulting cyber insecurity from the development of ICT has exposed our country to a number of cyber-attacks that have been recorded over the past years.

The Government has therefore prioritised the need to secure the country's digital journey with the same resolve that is used to secure our physical borders to keep the people of Ghana safe. In this regard, the Government has introduced the Cybersecurity Act, 2020 (Act 1038) to regulate cybersecurity activities and promote cybersecurity development in the country. The Act which was passed by the 7th Parliament is expected to provide a legal basis for our cybersecurity development and further improve our response to the escalating phenomenon of cybercrime. It is our aim to ensure that all Children, the Public, Businesses and Government are protected from cyber-related attacks. It is to this end, that the National Cyber Security Centre was established in 2018 to oversee Ghana's cybersecurity development. One of the tasks mandated to the Centre was to implement a National Cybersecurity Policy and Strategy document to act as a framework for a secure and resilient digital Ghana. Although we acknowledge that Ghana's digital ecosystem cannot be insulated from attacks, however, our cyber resiliency will be defined by our ability to detect, prevent, protect and recover from any form of cyber-attack on our critical information infrastructure. It is in this regard that the National Cybersecurity Policy and Strategy essentially seeks to provide a roadmap for providing a national policy direction and strategic implementation plan to mitigating the effects of cyberattacks and deterring cybercriminals.

This is very important because Ghana's critical information infrastructure comprising systems that run the financial, energy, telecommunication/ICT, defence, health, and other government sectors, are at the heart of Ghana's network-centric based economy. These sectors are heavily dependent on ICT Infrastructure and our sustained economic continuity is very much dependent on these critical systems. Successful attacks against these systems could undermine our country's socio-economic survival, compromise our national security, affect public health and safety, and undermine our sovereignty as a nation in a very significant manner. However, if these sectors can thrive, they will act as a catalyst towards achieving the Sustainable Development Goals (SDGs). As a result, Government believes that together with citizens as key stakeholders, this document will serve as a blueprint to contribute significantly to the development of a multifaceted cybersecurity ecosystem, coupled with a robust and digitally-driven economy.

Ghana's digitalisation initiatives are matched with sustained cybersecurity efforts to enable our country to achieve the full digital dividends associated with current and future developments in ICT.

H.E. Nana Addo Dankwa Akufo-Addo
President of the Republic of Ghana

preface

Ghana's economy has witnessed significant improvement in the use and reliance on digital technology over the years which has accelerated with the advent of the COVID-19 pandemic. Although this has been an immeasurable advantage to development, the scale of digitalisation and connectivity has resulted in a number of cybersecurity breaches that threaten the digital safety of Children, the Public, Businesses and the Government at large. As Ghana continues to embark and expand on digitalisation initiatives, cyber-attacks targeting our digital ecosystem are expected to increase with resulting consequences that could undermine our modest developmental efforts.

To protect our critical information infrastructure and to safeguard our country's developing digital ecosystem, the government, through the Ministry of Communications and Digitalisation, has introduced the National Cybersecurity Policy and Strategy (NCPS) to complement the implementation of the Cybersecurity Act, 2020 (Act 1038). The Strategy provides an implementation plan to the policy statements (Legal measures, Technical measures, Organisational measures, Capacity Building, and Cooperation) of the Policy. The Strategy revolves around five intersecting strategic imperatives which are Secure Digital Infrastructure, Deter Cybercrime, Develop National Capacity, Build a Resilient Digital Economy and Strengthen Cybersecurity Cooperation.

The Ministry of Communications and Digitalisation working in collaboration with the Governing Board of the Cyber Security Authority (CSA) and the Joint Cybersecurity Committee (JCC), introduced this document to equip the Government with the tools needed to address issues of cybercrime. The NCPS has been developed through constructive engagements with relevant stakeholders including corporate entities, civil society organisation, academic and research institutions, international partners and the general public at large.

This document does not only address ways the Government can combat cybercrime but also puts in place measures to equip citizens with the requisite tools to ensure that they do not fall prey to cyber-attacks. To combat cybercrime, a joint effort is required between the private and the public sector. As co-owners of this document, I invite all of you to consider this National Cybersecurity Policy and Strategy as our reference point towards a secure and resilient digital Ghana.

Mrs. Ursula Owusu-Ekuful (MP)
Minister for Communications and Digitalisation
Republic of Ghana

statement

Our world today has changed, with digitalisation presenting both opportunities and risks to businesses, societies and nations. With the increasing dependency on networks and digital systems for socio-economic developments, malicious actors are focusing on undermining the Confidentiality, Integrity and Availability of these infrastructures, thereby exposing the entire digital ecosystem to harm.

Cyber threats are global in nature but their manifestations are localised. Consequently, Ghana is not immune from such threats. The existential threats from cyber-attacks has led to the recognition of the need for a national strategy to prevent potential cyber-attacks if possible and to prepare for eventual attacks should they happen.

The adoption of this National Cybersecurity Policy and Strategy (NCPS) itself represents a strategic response to both existing and anticipated cyber threats which could undermine Ghana's gains in digitalisation. The strategy provides unambiguous focus and direction to guide the development of Ghana's cybersecurity for the next five years (2023 to 2027).

The Cyber Security Authority as the national agency responsible for cybersecurity matters in the country is mindful of its mandate as the lead agency for the implementation of the NCPS. Whilst the CSA recognises its lead responsibility with respect to the implementation of this national strategy, the multi-dimensional nature of cybersecurity requires a multi-sectoral response.

It is however important to note that, the collective responsibility required to implement this national strategy is recognised by the Cybersecurity Act, 2020 (Act 1038). The establishment of the Joint Cybersecurity Committee (JCC) (Section 13) and the creation of the Industry Forum (Section 81) are the two primary vehicles through which the collective responsibilities of all stakeholders can be exercised for effective implementation of the NCPS. Our goal of preventing cyber-attacks against Ghana's digital infrastructure is the same; we only have differentiated responsibilities, reflecting in our various mandates – as public sector agencies and as private sector actors.

The government of the day is only an enabler for cybersecurity development. The NCPS represents the most important enabling intervention to guide the thinking and actions of all stakeholders as we work to minimise the risks and to secure the benefits of a trusted digital environment for individuals, businesses and the state.

The CSA is looking forward to working with all of you – our implementing partners, to achieve a secure and resilient digital ecosystem for the benefit of everyone.

Dr. Albert Antwi-Boasiako
Director-General, Cyber Security Authority
Republic of Ghana

Introduction

Digitalisation has been a significant determinant of economic development and developing economies continue to experience its benefits. The benefits of digitalisation are seen in increased foreign direct investment, economic productivity and job creation, among others. The digitalisation drive of the Government is underpinned by an ICT-enabled economy that manifests across all its sectors consistent with pillar 9 (Industry, Innovation and Infrastructure) of the United Nations' Sustainable Development Goals (SDGs). Strong cybersecurity, and thereby the protection of the confidentiality, integrity and availability of ICT infrastructure and data, is increasingly important to ensure that individuals are able to exercise their human rights, including the rights to freedom of expression, and the right to privacy.

The internet has evolved from being solely an information-exchange platform to becoming the backbone of modern businesses, critical services, infrastructure and social networks. Although the reliance on digital infrastructure is growing globally, technology remains inherently vulnerable. The confidentiality, integrity, and availability of ICT infrastructure are challenged by rapidly evolving cyber threats and their complexity. It has been established that individuals and organised groups within nations are increasingly resorting to cyber-attacks not only to gain information but to compromise infrastructure and disrupt services.

As the economy grows and scales up connectivity as part of the Government's digitalisation agenda, the country will become susceptible to attacks by cybercriminals. These attacks can disrupt socio-economic activity on a large scale. Thus, it is imperative for the government to put in place an overreaching policy and strategy that protects Children, the Public, Businesses and Government.

The Policy which provides a direction to the country's cybersecurity development directs the national course in five pillars termed policy statements which are Legal measures, Technical measures, Organisational measures, Capacity Building, and Cooperation. The policy statements which is consistent with ITU's Global Cybersecurity Agenda guideline for cybersecurity development is aimed at enhancing confidence, trust and security in the ICT architecture of Ghana.

The Strategy serves as an implementation tool to articulate the purpose of the Policy statements which are to *Build a Resilient Digital Ecosystem, Secure Digital Infrastructure, Develop National Capacity, Deter Cybercrime and Strengthen Cooperation*. These strategic imperatives provide clear strategic objectives and initiatives with their corresponding descriptions, timelines and relevant stakeholders required to implement the strategic imperatives for a secure and resilient digital Ghana.

The National Cybersecurity Policy and Strategy is developed to direct the national course of our cybersecurity development over a five-year period from 2023 to 2027.

Background & Situational Analysis

1.0 Background & Situational Analysis

1.1 Cybercrime & Cybersecurity Defined

Over the years, there has been a digital revolution that has produced great innovation and technological advancement across the globe. According to statistics carried out by Statista, the digital population worldwide as of January 2021, had about 4.66 billion active internet users, of which 4.2 billion were social media users. The increase in the accessibility, popularity and convenience of digital communication has resulted in massive dependence on the internet and computer systems. These developments have also created opportunities for malicious actors to undermine the confidentiality, integrity and availability of computer systems and the data contained therein. Strong cybersecurity, and thereby the protection of the confidentiality, integrity and availability of ICT infrastructure and data, is increasingly important to ensure that individuals are able to exercise their human rights, including the rights to freedom of expression, and the right to privacy, especially online.

Cybercrimes include both cyber-dependent and cyber-enabled crimes. Cyber- dependent crimes are those which can only be committed through the use of ICT devices, and where the devices are both the tool for committing the crime, and the target of the crime. Cyber-enabled crimes are traditional crimes that can be increased in scale or reach by the use of computers, computer networks or other ICTs. The United Nations Office on Drugs and Crimes (UNODC) also describes cybercrime as a criminal act, of which the target is computer information.

The technology for cybercrime has become widely available. The rate of internet penetration especially in the developing world is increasing and the profile of computer and internet users have become diverse. These developments have created opportunities for the perpetuation of crime in the cyberspace. Cybercrime has evolved from its traditional forms into a complex criminal reality involving ICT-dependent networks and systems. This has led to cyber-attacks including sophisticated ones on the Critical Information Infrastructure (CII) of nations. Cyber-attacks have also raised data protection concerns leading to the development of data protection legislation across the globe.

According to the International Telecommunication Union (ITU), Cybersecurity is defined as the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, trainings, best practices, assurance and technologies that can be used to protect the cyber environment of organisations and user's assets. Cybersecurity is an integrated domain comprising technology, people, and processes with the aim of achieving a secured cyber environment.

According to a research commissioned by the Ministry of Communications and Digitalisation and conducted by the World Bank in collaboration with the Global Cyber Security Capacity Centre (GCSCC) of the University of Oxford, Ghana's cybersecurity development is currently at the Formative Stage. The purpose of this Policy and Strategy is to provide a national direction and implementation plan towards enhancing the security of our digital ecosystem. The Policy and Strategy on cybersecurity, therefore, revolves around technology, processes and most importantly people, towards a secure and resilient digital Ghana.

1.2 Global Perspective

The use of information and communication technology has seen tremendous growth over the years. The GSM Association (GSMA) reported in their 2019 annual report (The Mobile Economy) that about half the world's population (3.8 billion) use mobile internet. It further estimates that by the year 2025, mobile devices connected to the internet are expected to be 5 billion. Internet of Things (IoT) connections were stated to be 12 billion and estimated to increase to 24.6 billion connections by 2025 in the same report.

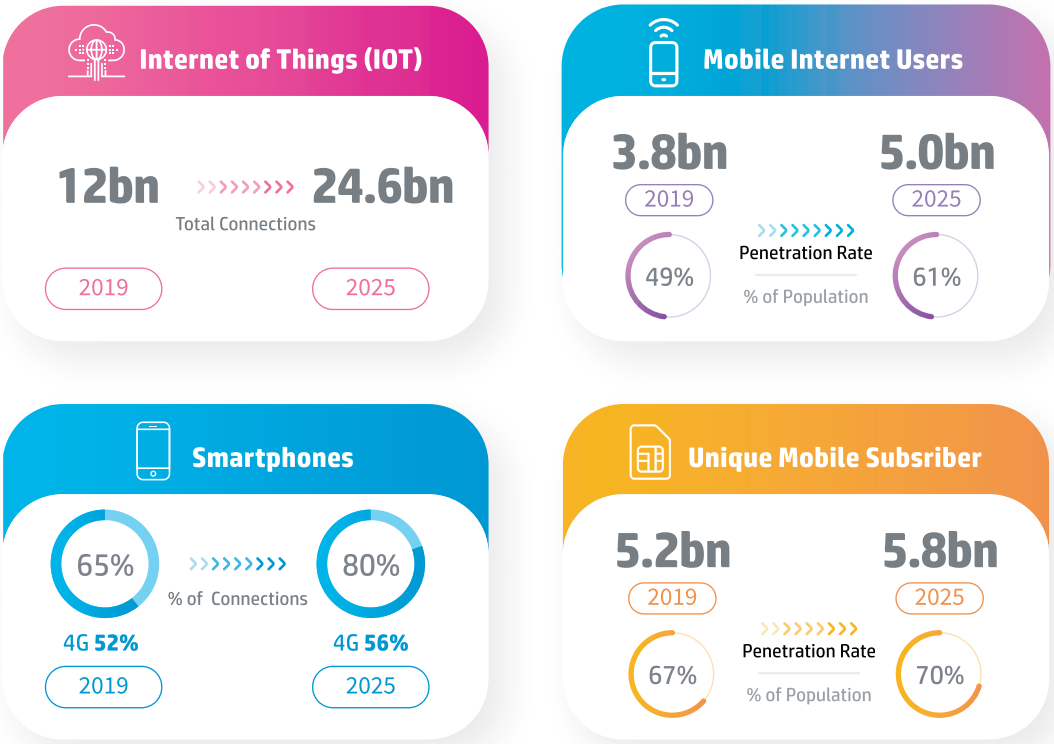


Figure 1: *Statistics on Global Internet usage*

The world is experiencing a rapid emergence of technology tools and systems in recent times underpinning global socio-economic development. For instance, there is an increased utilisation of various digital platforms, especially during this era of COVID-19, to facilitate and coordinate the activities of Governments, businesses and individuals globally. Cyber-attacks, therefore, have become increasingly frequent, dynamic, complex and highly impactful due to this development. The World Economic Forum (WEF) in its 2021 Global Risks Report indicated that dependence on cloud computing jumped by a third in 2020. Network operators also registered as much as a 70% increase in the demand for internet and mobile data services. Video-conferencing also sky-

rocketed by 700% in 2020, according to the report. This further establishes the increased reliance on technology for socio-economic development. This phenomenon is however accompanied by a surge in cybercrime activities across the globe.

Cybersecurity has therefore dominated the global discourse on security because of the increasing reliance of countries on ICT networks and systems. The global economy has become network-centric and attacks targeting national critical infrastructure could affect it. The WannaCry ransomware attack is an example of how a single cybersecurity incident could have a global reach. The Bangladesh bank heist involving more than 80 million United States dollars is an example of the vulnerability of our financial system to cyber-attacks. The cyber-attack which shut down the Ukrainian power infrastructure is another example of the global cybersecurity risk and the need for coordinated national, regional and international action to mitigate the growing threat.

According to INTERPOL, cybercrime has become the topmost threat facing countries due to its association with other forms of crimes. Evidence has established the use of cyberspace for money laundering, drug trafficking, human trafficking and terrorist-related activities among others. As many countries, especially in the developing world, are adopting electronic voting systems, there are real dangers that cyber-attacks could undermine the democratic developments of countries that are seeking to consolidate their young democracies of which elections are key elements. Increasingly, the nexus between cybercrime and national security challenges are manifesting on a daily basis within Ghana's cybersecurity ecosystem. The cyber domain has therefore become an active field not only for opportunistic cybercriminals and hackers but for organised crime and state-sponsored actors. These developments require a paradigm shift, both in policy and strategy, to face the threat. The INTERPOL indicated in its August 2020 report on Cybercrime: COVID-19 Impact that the global health crisis occasioned a sharp increase in cybercriminal activities related to COVID-19. According to information provided by the private sector partners of INTERPOL, about 1million spam emails, 750 malware-related incidents and 50,000 malicious URLs, all related to COVID-19 were detected between January and April 24, 2020.

In view of the above developments and as part of response strategies, countries have adopted cybersecurity policies and strategies as well as relevant legislation to mitigate the threats. In addition, many countries have set-up Computer Emergency Response Teams (CERTs) and Security Operations Centres (SOCs) to manage cybersecurity incidents. Harmonisation of cybercrime and cybersecurity legislations has also been identified as one of the response strategies to address the global threats. The Convention on Cybercrime, also known as the Budapest Convention, has seen a surge of its membership to more than 65 countries as of March 2021 with Ghana becoming the 62nd state party to the Convention. The African Union adopted the African Union Convention on Cyber Security and Personal Data Protection in 2014 to support member states to improve their cybersecurity on the continent. The ECOWAS Commission has adopted a number of regional directives and instruments including the Directive on Cybercrime (Directive C/DIR. 1/08/11), Regional Cybersecurity and Cybercrime Strategy and the Regional Policy on Critical Information Infrastructure to support member states to respond to existing and emerging cybercrime and cybersecurity challenges.

1.3 Ghana's Cybersecurity Landscape

The vision of the Government of the Republic of Ghana is to develop its economy Beyond Aid through digitalisation. This vision is underpinned by the United Nations Sustainable Development Goals (SDGs) which envisages a world where every country enjoys inclusive and sustainable economic growth and decent work for all. Over the past couple of years, this vision of the government has manifested in several digitalisation initiatives. These include the implementation of the National Property Addressing System (NPAS), the National Identification System (NIS), Mobile Money Financial Interoperability System, the Paperless Ports, the e-Justice System, e-Procurement System and a number of e-government initiatives. The private sector, led by the financial sector including the fintech industry and the tech community, is actively driving the country's digitalisation agenda, which is being fuelled by the continuous growth in the use of mobile devices, according to recent statistics from the National Communications Authority.

Further to these developments, Ghana's Critical Information Infrastructure (CII) is inherently dependent on ICT. Thus, the survival of the economy and its critical systems such as the financial system, energy, telecommunications system, defence and government services are dependent on the ability of the government to protect and secure these critical information assets. Successful attacks against any of these CII could significantly undermine the economic survival of the country. Attacks targeting some of the critical systems have been recorded including successful cyber-attacks against critical financial systems and databases.

According to recent statistics, Ghana has over 15.7 million people (50% of population) connected to the internet and the digitalisation of all sectors of our economy coupled with electronic payment systems have transformed the way we live and work. The impact of any attack on these services would seriously impact businesses and Ghanaians in general. When critical databases and information Infrastructure are hacked by unauthorised persons, the information can be used to perpetuate an attack against an individual, a business or the state which puts the nation at risk.

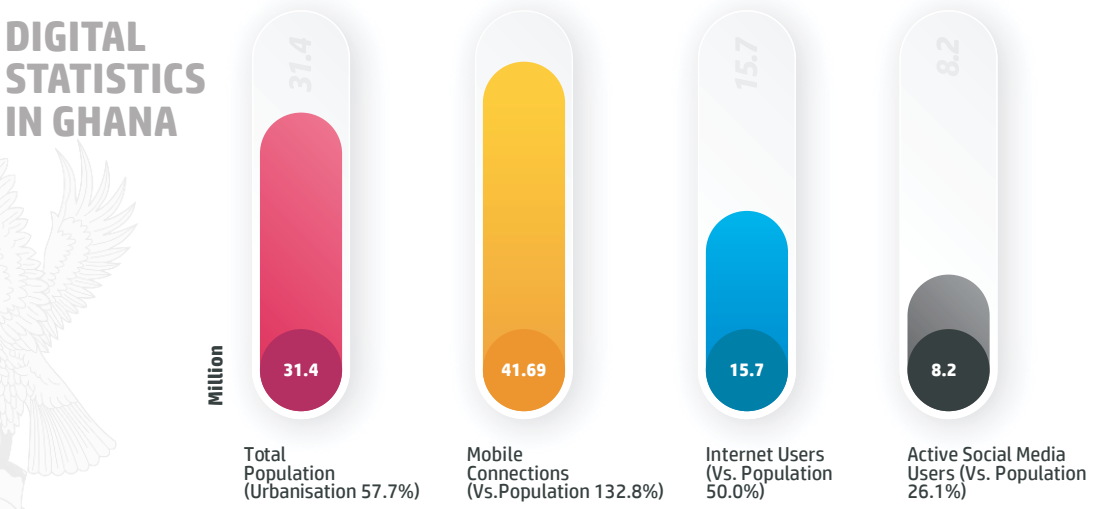


Figure 2: Statistics of Ghana's Internet Users

In recent times, there have been specific attacks targeting government websites and internal networks by malicious internal and external actors. The growing use of social media for impersonation in Ghana at large could undermine the trust in Ghana's cyberspace. The advent of mobile money services in Ghana's financial space has also led to the rise of financially-motivated scams with mobile money fraud accounting for the most common form of consumer fraud according to an analysis conducted by the Cyber Security Authority (CSA). Access to the internet and digital technologies by children and young people have also increased their risks of abuse and exploitation on the internet with a number of reported cases, according to a report commissioned by UNICEF. These examples of cybercrimes and cyber-attacks have also impacted on the privacy of people in Ghana, raising serious data protection concerns. Consequently, a review of Ghana's existing National Cybersecurity Policy and Strategy has become imperative in order to enhance the national response to these escalating cyber threats.

A cybersecurity maturity study commissioned by the Ministry of Communications and Digitalisation and conducted by the Global Cyber Security Capacity Centre (GCSCC) of the University of Oxford in collaboration with the World Bank in 2018, described Ghana's cybersecurity maturity level at a formative stage based on the Cybersecurity Capacity Maturity Model (CMM) for Nations adopted for the study.

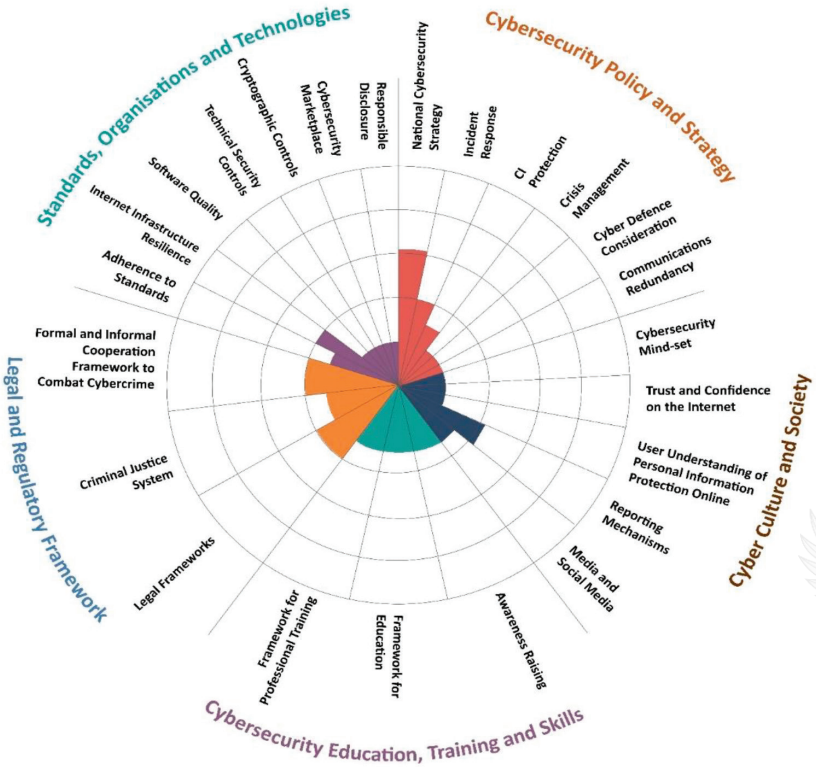


Figure 3: *The State of Ghana's Cybersecurity as depicted by the CMM Assessment*

Findings from the assessment evidenced the implementation of a number of initiatives by the Government. These include the adoption of a National Cybersecurity Institutional Framework (NCIF), the appointment of a National Cybersecurity Advisor to advise the Ministry on the implementation of national cybersecurity programmes, capacity building for the criminal justice sector through the GLACY+ Project, the inauguration of the National Cyber Security Inter-Ministerial Advisory Council (NCSIAC) and the National Cyber Security Technical Working Group (NCSTWG) in 2017, and the establishment of the National Cyber Security Centre (NCSC) in 2018 to coordinate national cybersecurity activities, amongst other initiatives.

Ratification of the African Union Convention on Cybersecurity and Personal Data Protection (Malabo Convention), the Convention on Cybercrime (Budapest Convention) and the ECOWAS Regional Cybersecurity and Cybercrime Strategy and the Regional Critical Infrastructure Protection Policy has further enhanced Ghana's credibility in the fight against cybercrime through international cooperation. The establishment of the National Cyber Security Centre (NCSC) in 2018 to coordinate national cybersecurity programmes and the development of the Computer Emergency Response Teams (CERTs) are other initiatives that have put Ghana on a modest path towards a secure and resilient digital Ghana.

Ghana, in 2017 took a number of steps towards institutionalizing its cybersecurity development. Critical among these steps is the establishment of a multi-sectoral institutional framework with responsibility for national cybersecurity development.

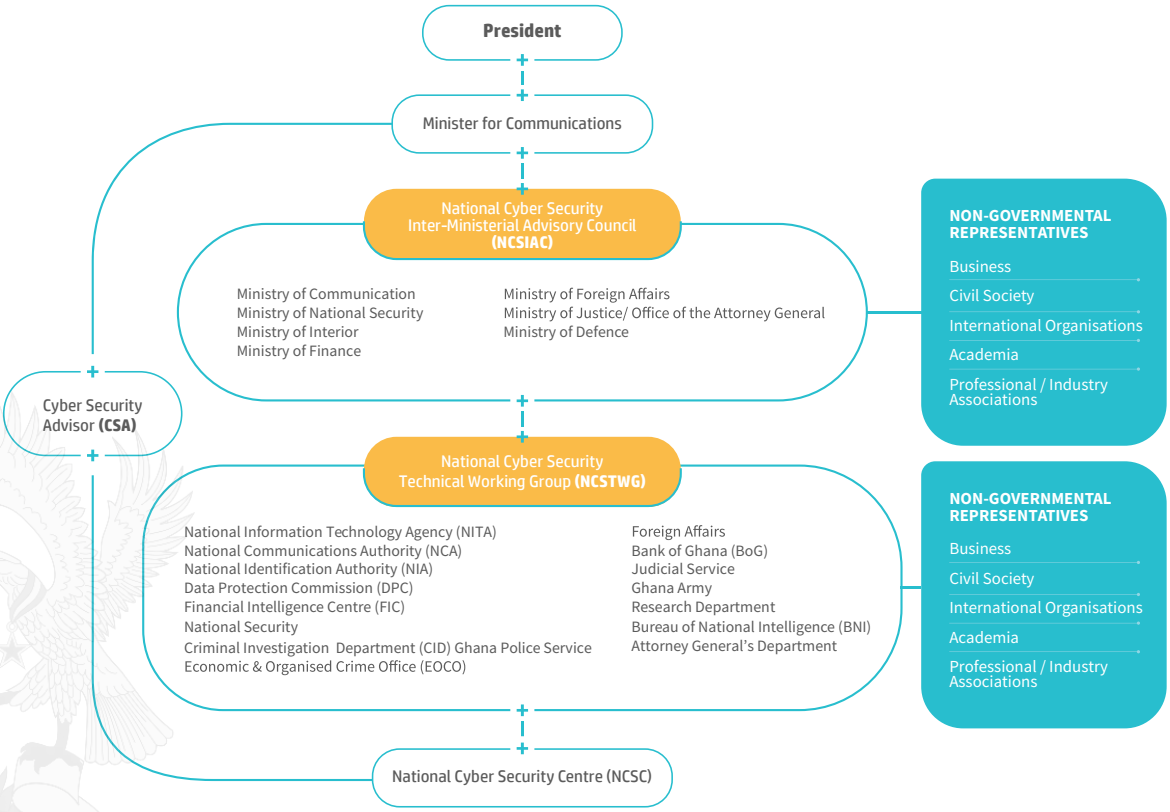


Figure 4: *Ghana's Foundational Cybersecurity Institutional Framework*

The institutional framework consisted of the National Cyber Security Inter-Ministerial Advisory Council (NCSIAC), the National Cyber Security Technical Working Group (NCSTWG) and the National Cyber Security Centre (NCSC). The NCSIAC comprised sector Ministers from relevant Ministries with a mandate to provide strategic and policy direction and guidance on matters pertaining to Ghana's national cybersecurity. The NCSTWG comprised of representatives of relevant government agencies and private sector representatives that are directly involved in cybercrime and cybersecurity activities. The NCSTG was set-up as a technical and operational coordinating body, under the direction of the National Cyber Security Centre, which was set-up under the Ministry of Communications at the time to coordinate national cybersecurity activities both in government and with the private sector.

The engagement of the above stakeholders of Ghana's cybersecurity architecture contributed to the development of a number of strategic interventions in Ghana's formative cybersecurity development. These include the launch of Ghana's National Cybersecurity Awareness Programme dubbed 'A Safer Digital Ghana', the establishment of Sectoral CERTs and SOCs, the launch of the Cybercrime and Cybersecurity Incidents Points of Contact (PoC), accession to the Budapest Convention, ratification of the Malabo Convention, capacity building especially for the criminal justice sector, the development of the Cybersecurity Act, 2020, the establishment of a Digital Forensics Lab for the Police CID and the revision of Ghana's National Cybersecurity Policy & Strategy, among other initiatives and programmes.

The formative development of Ghana's cybersecurity was also supported by a number of Ghana's international partners, including the Council of Europe (through the GLACY+ Project), the European Union, the World Bank, UNICEF, United States Government through the Security Governance Initiative, ITU, the ECOWAS Commission, African Union Commission and the government of the United Kingdom, among other bilateral partners.

This document is a revision of a previous Policy and Strategy document which was first developed in 2011 and adopted in November 2016. The revision was necessitated by the increase of cyber threats, the need for effective institutional and legal arrangements to deal with cybercrime at the national level and the requirements to align Ghana's cybersecurity around international treaties, conventions and best practices to facilitate effective cooperation both at the domestic and international levels.

Despite these modest developments, Ghana's digital ecosystem is inherently vulnerable and exposed to cyber-attacks due to the following:

- Lack of a national cybersecurity risk management framework for the protection of Critical Information Infrastructure (CII) and Government Digitalisation Initiatives (GDIs)
- Weak standardisation and enforcement regime leading to high dependency on sub-standard and in some cases pirated software which has penetrated the supply chain of Ghana's digital ecosystem.
- High number of unemployed youth with ICT skills. Some of whom are actively engaged in cybercrime.
- The influx of other nationals from the sub-region, some of whom are actively engaged in cybercrime in Ghana.

- Weak response to cybercrime cases by the criminal justice sector resulting in the inability to prosecute cybercrime perpetrators to serve as a deterrent to would-be perpetrators.
- Insufficient training and relevant skillset to address cybersecurity needs in various institutions especially in the public sector
- Lack of public's trust in state agencies capability and willingness to fight cybercrime.
- General lack of cybersecurity awareness among the people in Ghana, compounded by low digital literacy of a significant number of end-users.
- Inadequate cybersecurity measures to protect small and medium enterprises.
- General lack of cybersecurity capacity across all levels of Ghana's digital ecosystem.

These vulnerabilities in addition to the emerging complexity and sophistication of cyber-attacks expose the public, businesses and government to serious cyber risks.

1.4 Ghana's Cyberspace Threat Actors

Cybersecurity has dominated the global discourse on security because of the increasing reliance of countries on ICT infrastructure. The global economy has become network-centric and attacks targeting national critical systems could affect the global economy. Critical examples of how an attack could cripple businesses and disrupt national systems include the WannaCry ransomware attack affecting corporations and halting their operations, the Bangladesh bank heist in which USD 80 Million was stolen and the shutdown of the Ukrainian power plant. In July 2019, a major electricity supplier in Johannesburg, South Africa, suffered a ransomware attack leaving residents without power for several hours. Similarly, Uganda's Mobile Money System experienced a cyber-attack in October 2020 resulting in a shutdown of the system for several hours with an estimated loss of about USD 3 Million. The effect of these attacks calls for coordinated national, regional and international action to mitigate the growing threat.

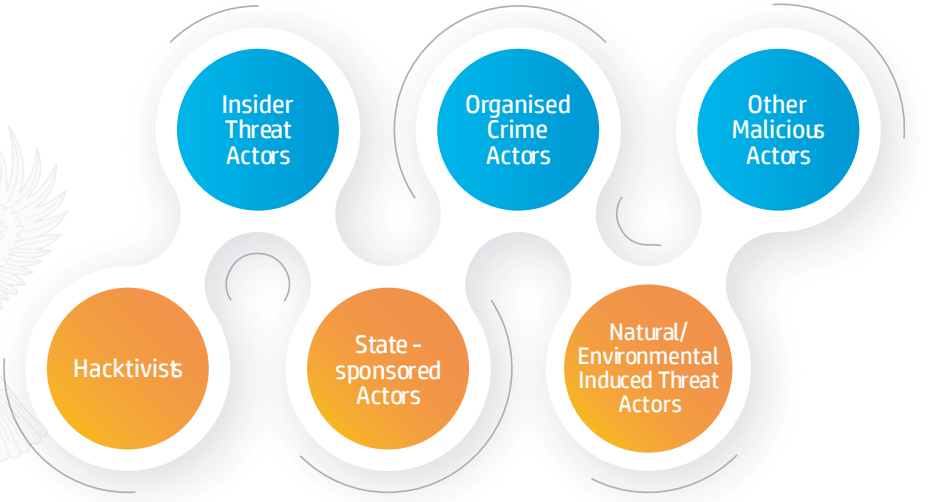


Figure 5: *Global Cyberspace Threat Actors*

Globally, Africa is the second-largest continent in terms of geographic area with a population of a little over 1.2 billion people and internet penetration of 35.2%. Although governments across the world recognise digital transformation as a power to accelerate the prosperity and wellbeing of people, the digital world has also provided an opportunity for malicious actors to undermine or thwart the gains from digitalisation.

A number of cyber-attacks and cybersecurity breaches have been reported globally. Malware, crypto and denial of service attacks, hacking, fraud and insider threats are some of the common cyber-attacks reported globally. The number of state-sponsored espionage and cyber-oriented organised groups engaging in activities geared towards compromising public and private sector networks has increased tremendously. Increasingly, the cyber dimension has been established to be ever-present in most serious and transnational crimes including terrorism, money laundering, drug trafficking, human trafficking and other crimes with national security implications.

The growing use of digital services and the business it generates have become potential targets for cybercriminals. As a nation, there is the need to address cybersecurity challenges to reap the full dividends of the emerging digital economy. Generally, the cyber threat landscape with its associated actors Ghana faces is no different from the international community. Ghana has experienced different types of cybercrimes including cyber-dependent and cyber-enabled crimes. These include website defacement, hacking into protected systems and databases, ransomware attacks, identity theft, SIM box fraud, child online threats and general cyber-related frauds, among others. These crimes have had not only financial or economic impacts on the country but also social and political repercussions.

→ Hacktivists

Hacktivists (hackers and activists), who are politically, socially and ideologically motivated are on the rise. They employ the same tools and tactics as typical hackers. Their tactics can range from spreading messages through simple website defacement or exploitation or launch a Distributed Denial of Service (DDoS) attack to bring down entire networks. Unlike normal hackers, hacktivists do not always work alone. Hacktivists can also work as part of a coordinated group or organisation. These groups can range in size from a few friends to an entire decentralised network of hackers around the world.

→ Insider Threat Actors

Insider threats with or without malicious intent remain a cyber risk to organisations especially in the financial sector in Ghana. Malicious insiders, who are trusted employees of an organisation and have access to critical systems and data, pose the greatest threat. They can cause financial and reputational damage through the theft of sensitive data and intellectual property. They can also pose a destructive cyber threat if they use their privileged knowledge, or access, to facilitate, or launch, an attack to disrupt or degrade critical services on the network of their organisations, or wipe data from the network. These malicious insider threats are mostly aggrieved employees with personality traits of Narcissism (egoistic), Machiavellianism, and Psychopathy often termed as the dark triad. Narcissists engage in such behaviours because they are only concerned about

themselves due to the sense of relevance than other employees, Machiavellians are manipulative and pursue such acts for gains, while psychopaths do that for the thrills, regardless of the risks to themselves or the organisation. Insiders or employees who accidentally cause cyber harm through inadvertent clicking on a phishing email, plugging an infected USB into a computer, or ignoring security procedures and downloading unsafe content from the Internet are often with no malicious intent. Whilst they have no intention of deliberately harming the organisation, their privileged access to systems and data means their actions can cause just as much damage as a malicious insider. These individuals are often the victims of social engineering – they can unwittingly provide access to the networks of their organisation or carry out instructions in good faith that benefit cybercriminals.

→ State-Sponsored Actors

Ghana is conscious of the threat posed by state-affiliated or sponsored actors in the form of a cyber-espionage attack. Attacks of this nature are carried out with a principal focus on the government, defence, finance, energy, and telecommunications, among other critical information infrastructures with a detrimental and devastating impact on national security and a compromise on the sovereignty of the nation. State-affiliated or sponsored actors often have particular objectives aligned with either the political, commercial, or military interests of their country of origin.

→ Organised Crime Actors

The high reward low-risk nature of cybercrime has made digital platforms/ networks an attractive environment for organised crime actors. Cybercrimes committed by organised crime actors within the country include:

→ Business Email Compromise, where cybercriminals spoof email addresses of employees (usually executives) and send emails that look like they are from a trusted sender to trick victims into revealing confidential information or sending money into specified accounts.

→ Impersonation of public officials, government appointees including Members of Parliament (MP) on various social media platforms to facilitate the commission of online fraud (employment scam, procurement fraud, etc.). These fraudulent profiles/pages, once taken down are created again.

→ Extortion, usually a by-product of a romance scam. The perpetrators deceptively acquire sexual images and videos of their victims and make countless monetary demands. When their victims fail to comply, they threaten to share acquired nude pictures or videos on the internet.

→ Mobile Money (MoMo) fraud where cybercriminals among other modus operandi, social engineer mobile money consumers to unwittingly send money to them, reveal their PIN or other personal information about their mobile money accounts, which can be used to defraud the customer.

→ Online Investment fraud involving cybercriminals who create social media handles and post a fake advertisement of beneficiaries to lure victims. The investments promise unsustainable returns or profits that outpace average market returns without corresponding risks.

As Ghana continues to experience a steady rise in the use of the internet among the populace,

terrorist groups and organisation have also employed the use of the internet to further intensify their activities including recruitment through social media, financing, propaganda, training, incitement to commit acts of terrorism, and the gathering and dissemination of information for terrorist purposes.

Natural/Environmental Induced Threat Actors

Natural disasters including wildfire, landslides, flooding, earthquakes, pandemics and tidal waves, etc. are caused by external natural phenomena and can be very difficult to predict or fully prepare against. They have incredibly far-reaching consequences for the safety and wellbeing of individuals and the country at large. They are force majeure with little or no control over their occurrence. Cybercrime activities escalated during the outbreak of the COVID-19 pandemic globally and Ghana was no exception to its impact, due to the over-reliance on digital platforms and services to survive and provide essential services by Governments, individuals and businesses. The adoption of technology for work, education and other social-related activities during such natural occurrence, in the typical case of the pandemic, further created new opportunities for cybercriminals to exploit vulnerabilities in systems and users.

Other Malicious Actors

Ghana recognises the emerging security risks emanating from the increased adoption of advanced technology including cloud computing, cryptocurrency, artificial intelligence, the Internet of Things (IoT) and their corresponding implications on the user and national security, should there be an attack. Ghana is mindful of the increased adoption of the internet by children worldwide which has contributed to unprecedented growth in online child sexual exploitation and abuse (OCSEA). Tactics and techniques employed by online predators include grooming, stalking, live streaming, coercing and blackmailing children for sexual purposes and the sale of OCSEA materials for profit.

Figure 6: *Ghana's Cyber-attacks Incidents and Trends.*

1.5 Opportunities

Notwithstanding the vulnerabilities identified, the following presents significant opportunities for Ghana to develop and scale up its cybersecurity through the implementation of this strategy:

→ The current development around Ghana's digitalisation initiatives present a rare opportunity to integrate cybersecurity programmes into the initiatives.

→ Known attacks on corporations around the world provide Ghana with insights in order to adopt specific cybersecurity measures to prevent, detect and respond to such potential attacks.

→ Ghana enjoys certain goodwill within the international community. This has translated into a number of cybersecurity collaborations with international partners. This strategy will build upon the current engagements to strengthen such international cooperation towards building a truly resilient digital ecosystem.

→ The modest achievement of Ghana on the cybersecurity front has also attracted interest from many countries including those in the ECOWAS region. These developments necessitate further action to replicate and leverage skills and initiatives to help collaborate, develop and lead cybersecurity development efforts in the sub-region.

→ Most importantly, the current political climate in Ghana is significantly favourable and receptive to cybersecurity development. Ghana's stakeholders in-country, sub-regional and international partners are therefore called upon to come on board to support government efforts towards a secure and resilient digital Ghana.

2.0 Vision

A Secure and Resilient Digital Ghana

3.0 Mission

Our mission is to Build a Resilient Digital Ecosystem, Secure Digital Infrastructure, Develop National Capacity, Deter Cybercrime, and Strengthen Cybersecurity Cooperation.

4.0 Institutional Framework

Effective governance is central to Ghana's cybersecurity development. As a result, Ghana has implemented an effective cybersecurity governance institutional framework for efficient coordination of cybersecurity issues across government and the private sector. Ghana's National Cybersecurity Institutional Framework (NCIF) is underpinned by the following principles:

- Inter-ministerial involvement at strategic and policy levels;
- Inter-agency cooperation as well as private sector involvement at the operational level;
- Sustainability of the governance structure to effectively deliver on Ghana's cybersecurity mandate;
- Partnerships and cooperation with non-governmental actors and Ghana's regional and international partners.

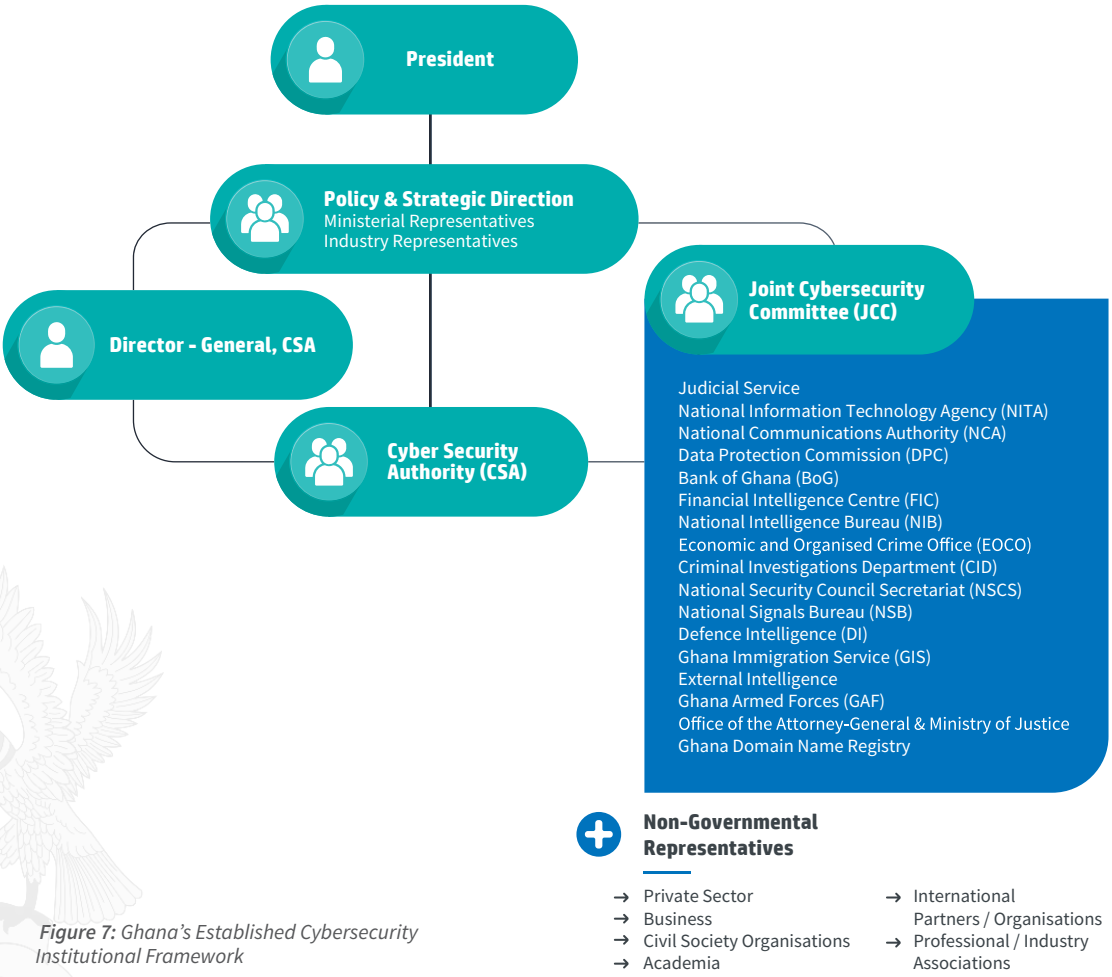


Figure 7: Ghana's Established Cybersecurity Institutional Framework

4.1 National Cybersecurity Governance

The Cybersecurity Act, 2020 (1038) provides the legal framework for Ghana's national cybersecurity governance. The involvement of key government stakeholders and private sector representatives are expressly provided under Section 5 of the Cybersecurity Act, 2020. The governance structure of Ghana's cybersecurity revolves around private-public partnership in the development of cybersecurity strategies and programmes in accordance with Section 81 (Establishment of Industry Forum) of the Act. The private-public partnership for the country's cybersecurity development is emphasised by Article 26(3) of the Malabo Convention which mandates member states to develop a private-public partnership as a model for engagement. Also, the ECOWAS Regional Cybersecurity and Cybercrime Strategy encourage members to pursue active private sector participation in national cybersecurity and cybercrime arrangements. As a member of the ITU, Ghana is required to comply with the Union's recommendation in its Global Cybersecurity Index for members to ensure private-public partnerships in cybersecurity development.

These developments stimulate the private sector involvement in the implementation of the country's strategic cybersecurity initiatives. Key among the initiatives include capacity building and awareness creation for SMEs (small and medium-sized enterprises), coordination on incidence response procedures with the National Computer Emergency Response Team (CERT-Gh), regional cybercrime/cybersecurity sensitisation programmes underpinned by the 'A Safer Digital Ghana's campaign, and research and development in cybersecurity, among others. Ghana's cybersecurity international partners are adequately represented in the governance architecture.

4.2 Cyber Security Authority (CSA)

A Cyber Security Authority (CSA) has been established in accordance with Section 2 of Act 1038 to succeed the National Cyber Security Centre (NCSC), to regulate cybersecurity activities in Ghana. The transition from the NCSC into the CSA is necessitated by the regulatory functions of the Authority expressed in Section 4 of the Act to regulate cybersecurity activities and promote the development of cybersecurity in the country. The CSA oversees the development, implementation, coordination and regulation of cybersecurity across government and non-governmental sectors. The Authority is responsible for critical information infrastructure protection, incident response and coordination, national cybersecurity awareness creation, cybersecurity policy & standardisation, cybersecurity guidance and advisory, international cooperation and Ghana's cybersecurity research & development towards self-reliance.

4.3 Joint Cybersecurity Committee (JCC)

The Joint Cybersecurity Committee (JCC), formerly the National Cyber Security Technical Working Group (NCSTWG), has been established in accordance with Section 13 of Act 1038 mandated to facilitate inter-agency cooperation on cybersecurity at the operational level. The Committee composes of heads or senior representatives of relevant government agencies that are directly and significantly involved in cybercrime and cybersecurity activities at the operational level. Government representation and non-governmental stakeholders including representatives from academia, business, and civil society organisations, constitute the committee.

Table 1: The JCC Representatives & Ghana's Cybersecurity Development in accordance with Section 13(2) of the Cybersecurity Act, 2020 (Act 1038).

Agency/Representative	Role/Functions
Judicial Service	Responsible for adjudication of cases involving cybercrime.
National Information Technology Agency (NITA)	Responsible for Government's IT infrastructure, networks and services.
National Communications Authority (NCA)	Responsible for the regulation of the telecommunications sector.
Data Protection Commission (DPC)	Responsible for data protection and privacy of individuals.
Bank of Ghana (BoG)	Responsible for regulating the financial services sector.
Financial Intelligence Centre (FIC)	Responsible for financial intelligence and countering cyber-based money laundering.
National Intelligence Bureau (NIB)	A national security agency with a mandate on national (internal) intelligence.
Economic and Organised Crime Office (EOCO)	To monitor and investigate economic and organised crime and on the authority of the Attorney-General, prosecute these offences to recover the proceeds of crime and provide for related matters.
Criminal Investigations Department (CID) of the Ghana Police Service	Responsible for cybercrime investigations within the Ghana Police Service.
National Security Council Secretariat (NSCS)	Responsible for security coordination among law enforcement, security and intelligence agencies.

Agency/Representative	Role/Functions
National Signals Bureau (NSB)	The National Signals Bureau is the National Security Agency responsible for monitoring, collecting, analysing and disseminating information from cyberspace and electronic media to counter threats to Ghana's security.
Defence Intelligence	This is a semi-autonomous Intelligence Agency dedicated to the provision of intelligence relevant to the protection and defence of the territorialintegrity of Ghana.
Ghana Immigration Service (GIS)	Responsible for the regulation and monitoring of the entry, residence, employment and exit of foreigners.
External Intelligence	A Foreign Affairs agency with a mandate on external intelligence.
Ghana Armed Forces	Responsible for protecting Ghana's territorial integrity from foreign aggression and maintaining internal security.
Public Prosecutions Division of the Office of the Attorney-General and Ministry of Justice	Responsible for public prosecutions including cybercrime cases.
Ghana Doman Name Registry (GDNR)	Responsible for administering and managing Ghana's domain name space.
Non-Governmental Representatives	Comprising representatives from the Private Sector, Academia & Research Institutions, Civil Society, Professional and Industry Associations and International Organisations.

part 1

National Cybersecurity Policy

Ghana's cybersecurity revolves around five policy statements consistent with the five strategic pillars of the International Telecommunication Union (ITU) Global Cybersecurity Agenda and international best practices. The policy provides a clear and specific national path and direction to the country's cybersecurity development.

5.0 Policy Statements

Figure 8: *The five (5) Policy Statements of Ghana's National Cybersecurity Policy*

5.0.1 Policy Statement I – Legal Measures

Gaps in national legislations make cybercrime a low risk and lucrative venture. Government, through the Office of the Attorney General and Ministry of Justice and relevant agencies, will develop and conduct periodic reviews of Ghana's cybercrime and cybersecurity legislation. The Government will ensure that Ghana's cybercrime and cybersecurity legislation are consistent and interoperable with regional and international laws, treaties and conventions. The Government will ensure that Ghana's legislation on cybercrime and cybersecurity are consistent with the human rights and digital rights of citizens. The Government will progressively build capacity in the criminal justice sector and other relevant national institutions for effective enforcement of cybercrime and cybersecurity legislation.

5.0. 2 Policy Statement II – Technical Measures

Vulnerabilities in hardware and software remain the main contributing factors for cyber-attacks as malicious attacks are increasing in their complexity and sophistication. The Government will implement appropriate technical measures to ensure the security of Ghana's digital ecosystem. Among other technical measures, the Government will set up and operationalise Ghana's Computer Emergency Response Team (CERT) ecosystem, introduce National Cybersecurity Risk Management Framework and standards especially for the Critical Information Infrastructure (CII) in various sectors, mechanisms for Cybersecurity Certification and Accreditations and Child Online Protection (COP).

5.0. 3 Policy Statement III – Organisational Measures

Organisational and institutional arrangements are prerequisites for the effective development of Ghana's national cybersecurity. The Government recognises the importance of a multi-stakeholder approach towards addressing Ghana's cybercrime and cybersecurity challenges. The Government will set up a national cybersecurity institutional framework that integrates governmental and non-governmental cybersecurity stakeholders and ensures accountability among them. The Government will develop its cybersecurity strategy and set-up a national agency responsible for coordinating cybersecurity operations and activities both in government and in collaboration with the private sector.

5.0. 4 Policy Statement IV – Capacity Building

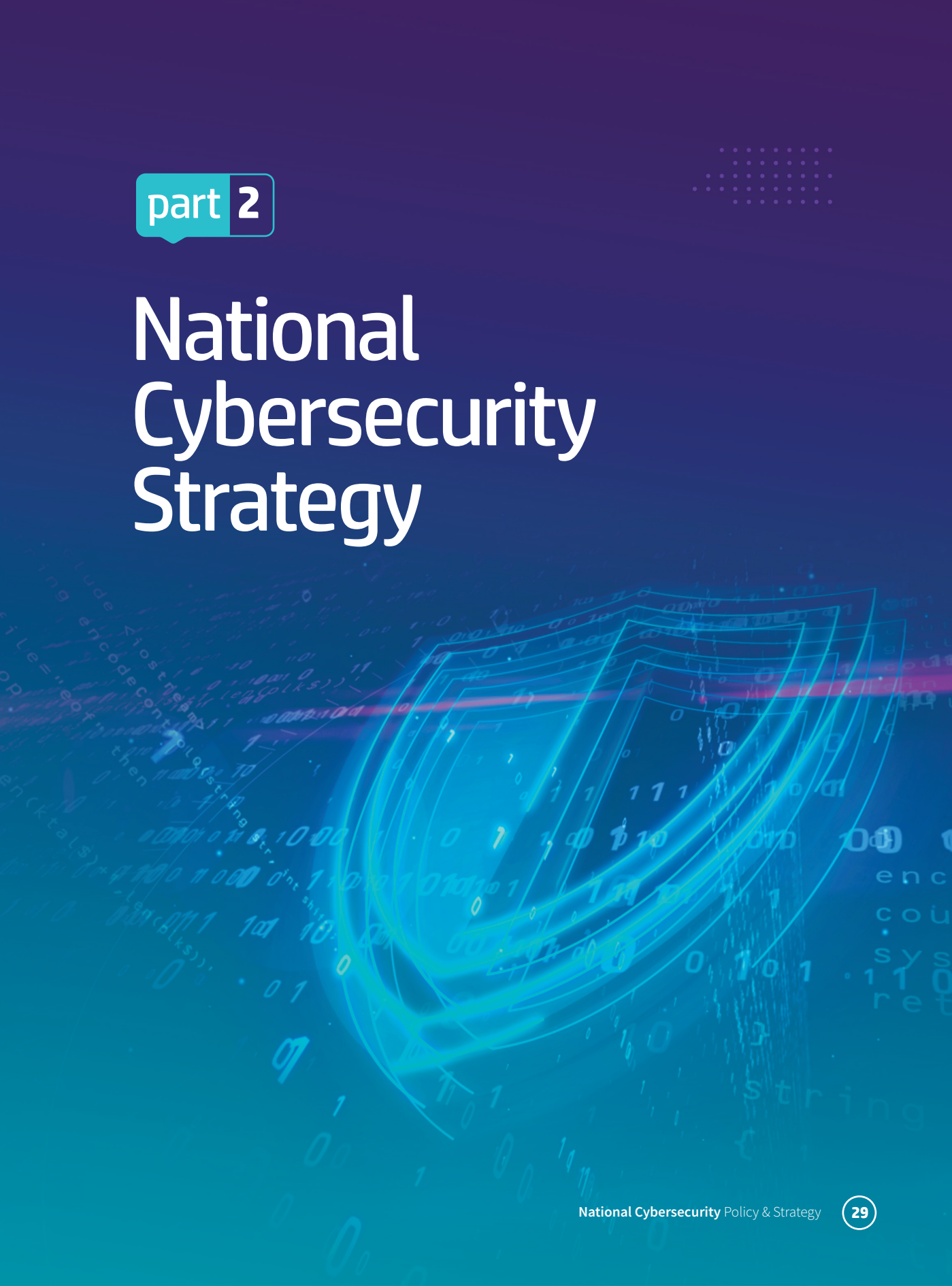
To ensure the sustainable development of Ghana's cybersecurity ecosystem, investment in capacity building efforts remains imperative. The Government will invest available resources to develop, foster and maintain a national cybersecurity culture. The Government will embark on national cybersecurity awareness programmes, support the development and adoption of appropriate cybersecurity standards, invest in cybersecurity education across all levels in order to develop the country's cybersecurity human resource base, prioritise the development of the local cybersecurity industry and invest in research and development towards self-reliance.

5.0. 5 Policy Statement V – Cooperation

Cybercrime and cybersecurity challenges are multidimensional and cross- border. Consequently, the Government will commit to partnerships and cooperation both within Ghana and through regional and international cooperation arrangements. The Government will prioritise inter-ministerial engagements, inter- agency cooperation and public-private partnerships in furtherance of Ghana's cybersecurity cooperation agenda. The Government will actively participate and contribute to international cooperation efforts towards addressing cybercrime and cybersecurity challenges.

part 2

National Cybersecurity Strategy



A National Cybersecurity Strategy has been developed to implement the policies outlined in this document. The Strategy provides an implementation plan covering a number of strategic imperatives expected to guide Ghana's cybersecurity development over the next five years (2023–2027). The strategy focuses on mainstreaming a cybersecurity agenda across government and the private sector, to help prioritise cybersecurity as an important focus area for the government. The strategy establishes the mandate of key cybersecurity government and non-governmental actors and directs the allocation of resources to the emerging and existing cybersecurity matters and priorities.

The strategy is situated within other national developmental and strategic goals as represented below:

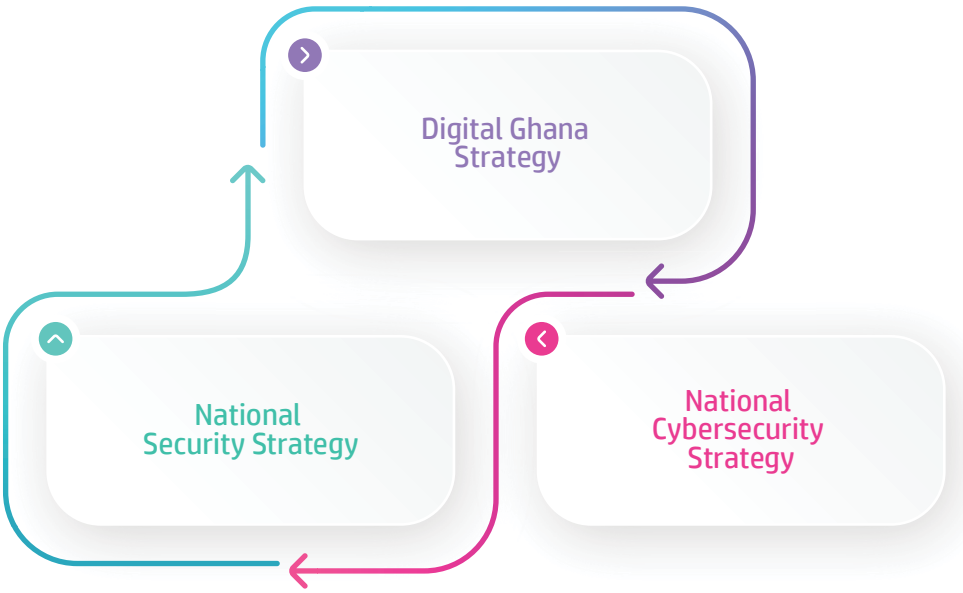


Figure 9: *Ghana's National Cybersecurity Strategy is interlinked with other national developmental goals*

6.0 Strategic Imperatives

The National Cybersecurity Strategy revolves around five strategic imperatives: *Build a Resilient Digital Ecosystem; Secure Digital Infrastructure; Develop National Capacity Deter Cybercrime; and Strengthen Cybersecurity Cooperation.*

These are represented by the diagram below:

Figure 10: *The Five (5) Strategic Imperatives of Ghana's National Cybersecurity Strategy.*

A number of initiatives under each of the imperatives have been identified for implementation in the next five years (2023–2027). An implementation plan covering Short-Term (within 1 year), Medium-Term (between 1 – 3 years) and Long-Term (between 3 – 5 years) is presented to guide the realisation of the strategic initiatives. Each strategic initiative is underpinned by five objectives.

6.0.1 Build a Resilient Digital Ecosystem

The concept of cyber resilience involves timely detection and recovery from cyber incidents when they occur. Ghana will build a resilient digital ecosystem by creating a cybersecurity environment that facilitates the sharing of timely and actionable cybersecurity information for proactive detection of threats in order to ensure the availability of our digital ecosystem. Ghana will pursue and invest in its ability to stay prepared for major cybersecurity incidents.

6.0.1.1 Strategic Objectives

Strategic objectives underlining the strategic imperative are presented below:

1. Ghana will pursue, invest and test our ability to prepare for major attacks in order to build confidence in our entire cybersecurity ecosystem.
2. In order to provide assurance of our cyber resilience, Ghana will implement the necessary national cybersecurity contingency measures and subject them to regular tests and exercises.
3. The general cybersecurity environment will be pursued and scaled up across all sectors in order to raise Ghana's resilience to both the common and pervasive cyber-attacks.
4. Effective coordination is key to achieve cyber resilience. In this regard, Ghana will build an incident response ecosystem that is inclusive, proactive, interactive, trusted, and responsive to our national incident response plan and needs. Measures taken to achieve cyber resilience will comply with the principles of legality and proportionality.
5. Ghana will invest in cybersecurity research and development including security of our internet infrastructure across the public and private sector to ensure continuous resilience of our digital ecosystem.

6.0.1.2 Strategic Initiatives & Implementation Plan

The following constitutes the Strategic Initiatives & Implementation Plan that Ghana seeks to implement towards achieving this Strategic Imperative. Timelines provided constitute short term (1-2 years), medium-term (3-4 years) and long-term (4-5 years), and responsibilities are presented for the various initiatives and actions.

Table 2: Build a Resilient Digital Ecosystem – Strategic Initiatives and Implementation Plan.

S/N	Strategic Initiative	Description of Strategic Initiative	Time Frame	Responsibility/ Stakeholders
1.01	National Cybersecurity Contingency Plan	A cybersecurity contingency plan capable of facilitating our national response to cybersecurity incidents and cyber crisis management. The plan will clearly define the roles and responsibilities of different stakeholders during cybersecurity emergencies and crisis, based on a risk assessment framework which will cover the process of identifying threatsand vulnerabilities and their potential impact, especially on the CII sectors. A review of contingency plans shall be carried out, taking into consideration lessons learnt from cyber exercises.	Short to Medium-term	• CSA • JCC • Sectoral CERTs • Other relevant MDAs • Non- Governmental Stakeholders
1.02	CERT Development	Development of Computer Emergency Response Team (CERT), comprising a National CERT and Sectoral CERTs responsible for incident response and coordination across the public and the private sector. This includes capacity building and information sharing to detect, investigate, analyse and respond to cyber-related incidents. Security Operating Centres (SOCs) shall be established to complement the traditional functions of CERTs. This initiative also involves cooperation with international CERT bodies including ITU, FIRST and AfricaCERT. Cybersecurity exercises shall be conducted to test the readiness and responsiveness of the CERT capabilities. Ghana shall participate in global and regional cybersecurity incident response activities and initiatives.	Short to Medium-term	• CSA • JCC • Sectoral CERTs • Other relevant MDAs • Non- Governmental Stakeholders

S/N	Strategic Initiative	Description of Strategic Initiative	Time Frame	Responsibility/ Stakeholders
1.03	Establish and Operationalise Mechanisms for Incident Reporting	Establish and operationalise Points of Contact to facilitate and coordinate cybercrime and cybersecurity incident reporting. This will include both online and offline mechanisms for incident reporting. Effective coordination and collaboration with the Police CID, service providers and relevant institutions especially with the JCC and private sector shall be facilitated to enhance reporting of cybercrime and cybersecurity incidents.	Short-term	• CSA • JCC • Sectoral CERTs • Other relevant MDAs • Non- Governmental Stakeholders
1.04	Establishment of Cyber Risks Early Warning System	Establishment of an early warning system to help provide situational awareness of the country's cyber threats especially CII-based threats and also advise both the government and the private sector on cybersecurity matters. This will involve an investment in technologies such as analytics, automation, artificial intelligence, and other state-of-the-art security technologies to ensure operational excellence for the timely detection and response to cyber-related incidents. This will promote the continuous improvement of Ghana's cybersecurity early warning system.	Short to Long-term	• CSA • JCC • Sectoral CERTs • Other relevant MDAs • Non- Governmental Stakeholders

6.0.2 Secure Digital Infrastructure

The digital infrastructure of Ghana constitutes Critical Information Infrastructure (CII), Government Digitalisation Initiatives (GDI) and other digital networks and systems in the private sector. These, especially the CII, owned by both the government and the private sector, is of particular importance because any successful cyber-attack on them would have a serious impact on the economic well-being and national security of the country. The digital strength of Ghana resides in its ability to secure these digital Infrastructure which form the backbone of the country's digitalisation developmental goals. These imperatives outline how government and private sector participants intend to work together to manage risks and achieve security and resilient outcomes and also ensure that Ghana's digital infrastructure and assets are protected against cyber- attacks.

6.0.2.1 Strategic Objectives

Strategic objectives underlining the strategic imperative are presented below:

1. Ghana will identify and implement the necessary security mechanisms for the protection of Critical Information Infrastructure (CII) which forms the backbone of our economic well-being.
2. Ghana will identify and develop the necessary security mechanisms towards securing Government Digitalisation Initiatives (GDIs). This is to ensure the security of these initiatives which are being implemented through Ghana's Digital Strategy.
3. Ghana will implement the necessary security mechanisms to secure digital networks, systems and assets in the private sector.
4. Ghana will promote awareness on cyber risks targetting CII as well as GDIs in order to secure these critical digital systems.
5. Ghana will reinforce the security of its digital infrastructure and and will invest in resources to ensure the protection of this critical component of its digital ecosystem.

6.0.2.2 Strategic Initiatives & Implementation Plan

The following constitutes the Strategic Initiatives & Implementation Plan that Ghana seeks to implement towards achieving this Strategic Imperative. Timelines and responsibilities are presented for the various initiatives and actions.

Table 3: Secure Digital Infrastructure – Strategic Initiatives and Implementation Plan.

S/N	Strategic Initiative	Description of Strategic Initiative	Time Frame	Responsibility/ Stakeholders
2.01	Adoption of National Cybersecurity Risk Management Framework for CII & GDIs	This involves the development and implementation of a National Framework that will assist in the risk management of all the CII sectors and GDIs. This initiative shall include the identification and risk assessment of CII sectors and GDIs as well as the development of risk registers for CII and GDIs.	Short to Medium-term	• CSA • JCC • Other relevant MDAs • Non- Governmental Stakeholders
2.02	Implementation of the Cybersecurity Act, 2020 (Act 1038)	The Cybersecurity Act will protect the CII sectors, regulate cybersecurity activities and promote cybersecurity development. The implementation of the Act will also ensure that Ghana's obligations under the international treaties including the African Union Convention on Cyber Security & Personal Data Protection (Malabo Convention), the Convention on Cybercrime (Budapest Convention) and relevant ECOWAS directives.	Short to Long-term	• CSA • JCC • Other relevant MDAs • Non- Governmental Stakeholders
2.03	Establishment of a National Public Key Infrastructure (PKI).	Establish a National Public Key Infrastructure (PKI) to manage digital certificates in a public key cryptography scheme. This would ensure secure electronic transactions. This initiative includes the development of policy aspects of PKI and the adoption of PKI for e-government initiatives. Government and stakeholders will promote PKI in e- commerce development in the private sector.	Short to Medium-term	• CSA • NITA • JCC • Other relevant MDAs • Non- Governmental Stakeholders

S/N	Strategic Initiative	Description of Strategic Initiative	Time Frame	Responsibility/ Stakeholders
2.04	Establishment of Cybersecurity Assurance Programme for CII Sectors and GDI Owners	Establish Cybersecurity Assurance Programmes for CII Sectors and GDIs. Baseline cybersecurity standards for the CII and GDIs and quality assurance framework for CII and GDIs shall be established. This initiative involves security auditing and testing for the CII sectors and GDI owners including regular Vulnerability Assessment and Penetration Testing (VAPT).	Short to Long-term	• CSA • JCC • Other relevant MDAs • Non- Governmental Stakeholders
2.05	Establishment of a Mechanism for Regular Vulnerability Disclosure	Establish a system to regularly identify and disclose vulnerabilities in the CII sectors and GDIs. Mechanisms for information sharing between CII and GDI owners and the Government shall be established including internal and external communication strategies with clear points of contact. This initiative includes establishing the framework for assessing the capability of CII and GDI owners to prevent, detect, identify, respond and recover from cyber-attacks. Cybersecurity exercises to identify vulnerabilities affecting CII and GDIs shall be conducted.	Short to Medium-term	• CSA • JCC • Other relevant MDAs • Non- Governmental Stakeholders
2.06	Establishment of a Central Equipment Identification Register (CEIR)	Establish a technology infrastructure for device registration, SIM registration and verification as an important component of securing Ghana's digital ecosystem. This initiative shall provide for the standardisation of SIM and device registration and strengthen the combat against Sim Box fraud and cybercrime. The technology will have a Central Equipment Identification Management System (CEIMS) to ensure the registration of devices in use on all local networks.	Short to Medium-term	• CSA • NCA • JCC • Other relevant MDAs • Non- Governmental Stakeholders

6.0.3 Develop National Capacity

To establish a digitally safe and secure Ghana, there are key capabilities required to establish and manage effective cybersecurity. These capabilities can be established and developed concurrently through the prioritisation of initiatives. Ghana's national cybersecurity capacity development starts with awareness creation through the development of cybersecurity research and development towards self-reliance and the exportation of cybersecurity products and services in the sub-region. Ghana intends to achieve this strategic imperative through investment in cybersecurity in both the public and the private sector.

6.0.3.1 Strategic Objectives

Strategic objectives underlining the strategic imperatives are presented below:

1. Ghana's cybersecurity culture starts with awareness raising. Awareness will be raised about the need for cybersecurity and responsible behaviour in cyberspace among Children, the Public, Businesses, and Government.

2. Ghana will pursue, develop and implement relevant cybersecurity standards, frameworks and best practices in order to promote a national culture of cybersecurity across the entire digital ecosystem of our country.

3. Cybersecurity is of strategic importance to Ghana's digital economy. A Cybersecurity Fund pursuant to Section 29 of the Cybersecurity Act, 2020 (Act 1038) shall be established to ensure sustainable funding for the development of Ghana's cybersecurity.

4. In order to ensure that Ghana achieves self-reliance in cybersecurity, research and development will be prioritised by actively investing in cybersecurity both in the government and private sector.

5. Ghana seeks to become a cybersecurity hub in the ECOWAS sub-region. Consequently, an active cybersecurity ecosystem will be created through government's collaboration with industry, academia, research institutions and international partners.

6.0.3.2 Strategic Initiatives & Implementation Plan

The following constitutes the Strategic Initiatives & Implementation Plan that Ghana seeks to implement towards achieving this Strategic Imperative. Timelines and responsibilities are presented for the various initiatives and actions.

Table 4: Develop National Capacity – Strategic Initiatives and Implementation Plan.

S/N	Strategic Initiative	Description of Strategic Initiative	Time Frame	Responsibility/ Stakeholders
3.01	Adoption of Cybersecurity Standards &Accreditation Framework	Adoption of standards and enforceable best practice guidance that outline minimum expectations for all elements of cybersecurity. This involves the adoption of a nationally agreed baseline standard for cybersecurity in the public and private sectors. Standards for cybersecurity education, a standard for cybersecurity professional certifications standards and guidance for cybersecurity software and hardware development, among others shall be introduced. Integrating cybersecurity requirements in public contracts and procurements are anticipated under this initiative.	Short to Medium-term	• CSA • JCC • National Accreditation Board (NAB) • Ghana Standards Authority (GSA) • Other relevant MDAs • Non- Governmental Stakeholders
3.02	Child Online Protection (COP) Framework	Development and implementation of a national COP framework based on international standards (ITU, UNICEF, WeProtect, AU, etc.). Through a multi-stakeholder approach, COP guidelines for educators, parents, industry, children and other stakeholders shall be implemented under this initiative. This initiative involves capacity building and awareness creation on child online protection issues.	Short to Long-term	• CSA • JCC • Ministry of Gender, Children and Social Protection • Ministry of Education • International Partners (UNICEF, AU, ITU etc.) • Other relevant MDAs • Non- Governmental Stakeholders

S/N	Strategic Initiative	Description of Strategic Initiative	Time Frame	Responsibility/ Stakeholders
3.03	Implement Ghana's National Cybersecurity Organisational Structure	A multi-stakeholder organisational structure that underpins the implementation of Ghana's National Cybersecurity Strategy. This involves the identification of stakeholders, their roles and responsibilities including operationalising the various sub-working groups of the JCC. This initiative will drive the rationalisation and differentiation of the respective roles of JCC members and other stakeholders to prevent duplication of efforts. Relevant Standard Operating Procedures (SOPs) shall be implemented to ensure efficiency in cybersecurity operational coordination at the national level. The initiative will inform resource allocation for the implementation of the multi-stakeholder organisational structure for cybersecurity and the development of communication mechanisms among stakeholders.	Short to Medium-term	• CSA • JCC • Other relevant MDAs • Non- Governmental Stakeholders
3.04	National Cybersecurity Awareness Programme	Develop a national programme to build capacity and raise awareness on cybercrime and cybersecurity issues and promote a culture of cybersecurity among Ghanaians. This initiative will launch Ghana's national cybersecurity awareness programme dubbed 'A Safer Digital Ghana'. The capacity building and awareness creation efforts will focus on Children, the Public, Business and Government. The Government will engage the media, civil society organisations, NGOs, international partners, etc. on the implementation of the awareness campaign. Relevant monitoring and evaluation framework shall be implemented to measure the implementation of the *Safer Digital Ghana* campaign.	Short to Long-term	• CSA • JCC • Ministry of Education • Ministry of Gender, Children and Social Protection • Ministry of Information • NCCE • Other relevant MDAs • International Partners (UNICEF, AU, ITU etc.) • Non- Governmental Stakeholders

S/N	Strategic Initiative	Description of Strategic Initiative	Time Frame	Responsibility/ Stakeholders
3.05	Development of Cybersecurity Education	Implementing a systematic cybersecurity education across all levels of education in Ghana, including integrating cybersecurity education into the curricular of basic and senior secondary education in Ghana. The initiative also involves integrating cybersecurity education into all tertiary and continuing education programmes and courses in Ghana. Professional cybersecurity education shall also be an important element of this initiative to support the development of Ghana's cybersecurity workforce. Specialised cybersecurity courses for defence, law enforcement and national security agencies shall be introduced through the programmes of the National Cyber Academy.	Short to Long-term	• CSA • JCC • Ministry of Education • Other relevant MDAs • National Accreditation Board (NAB) • Non- Governmental Stakeholders
3.06	Development of Cyber Defensive Capabilities	Development of national capabilities in defensive cybersecurity towards self-reliance. National Cyber Defense Programmes involving law enforcement, intelligence and national security agencies shall be established. Partnerships with cybersecurity research centres at the domestic and international levels shall be established for the development of cyber defensive capabilities. This initiative shall develop national cyber capabilities to protect and defend Ghana's interest in the cyberspace.	Medium to Long-term	• CSA • NSCS • JCC

S/N	Strategic Initiative	Description of Strategic Initiative	Time Frame	Responsibility/ Stakeholders
3.07	Implementation of Data Protection & Digital Right Initiatives	Implementation of national initiatives to ensure enforcement of privacy rights of people in Ghana, together with plans to safeguard digital rights of citizens. Awareness creation on data protection principles, rights and obligations of individuals and data controllers shall be promoted at the national level. Digital rights' campaigns to ensure freedom of users in Ghana in the cyberspace shall be developed through collaboration with Civil Society Organisations.	Short to Long-term	• CSA • JCC • Data Protection Commission • Freedom Online Coalition • Other International Partners • Civil Society Organisations • Other relevant MDAs • Non- Governmental Stakeholders
3.08	Establishment of a Cybersecurity Fund	An establishment of a dedicated fund pursuant to Section 29 of the Cybersecurity Act, 2020 (Act 1038) for the promotion and development of Ghana's cybersecurity. Government shall establish the fund to ensure sustainable financial inflow to support the implementation of Ghana's National Cybersecurity Policy and Strategy. The Fund shall support Ghana's Research and Development activities in cybersecurity. The fund shall also support the development of the local cybersecurity industry and will support Ghana's involvement in the development of regional and international cybersecurity initiatives.	Short-term	• Parliament • Ministry of Finance • CSA • JCC • Non- Governmental Stakeholders

S/N	Strategic Initiative	Description of Strategic Initiative	Time Frame	Responsibility/ Stakeholders
3.09	Development of the Local Cybersecurity Industry	The Government will actively pursue and develop the local cybersecurity industry by promoting relevant investments and public-private partnerships as the development of the local industry constitute an important element of Ghana's goal for cybersecurity resilience. This initiative will promote the development of local talents and skills in cybersecurity among Ghanaians. Consistent with national policy on local contents, the Government will allocate at least 30% of government cybersecurity projects and contracts to qualified and accredited local cybersecurity firms. An annual budget to fund cybersecurity innovative products through competitive bidding by local cybersecurity firms shall be encouraged by the Government. This initiative shall promote Commercialisation of cybersecurity products and solutions through collaboration between government, local firms, Universities and research centres. Ghana will promote the exportation of cybersecurity skills, services and products in the sub-region through this initiative.	Short to Long-term	• CSA • JCC • Private Sector • Other relevant MDAs • Non- Governmental Stakeholders
3.10	Establishment of a National Cyber Academy	Establish a dedicated Cyber Academy to support the development of Ghana's workforce in cybersecurity. This initiative involves training and skills development of public sector officials, law enforcement and national security agencies in cybersecurity. The academy will also support the development of skills and competency in cybersecurity in the non-traditional education sector.	Short to Medium-term	• CSA • JCC • Ministry of Education • National Accreditation Board (NAB) • Other relevant MDAs • Non- Governmental Stakeholders

S/N	Strategic Initiative	Description of Strategic Initiative	Time Frame	Responsibility/ Stakeholders
3.11	Adoption of National Cybersecurity Monitoring and Evaluation (M&E) Framework	Implementation of a national monitoring and evaluation framework to measure the implementation of Ghana's National Cybersecurity development at each stage of the development process. The Government will adopt appropriate metrics and benchmarks for the M&E framework and will deploy atechnology infrastructure to implement the framework.	Short to Long-term	• CSA • JCC • Other relevant MDAs • Non- Governmental Stakeholders
3.12	Cybersecurity Research and Development (R&D)	Develop a roadmap that identifies Ghana's cybersecurity R&D needs and the necessary actions and timelines for implementation. The document which will guide Ghana's cybersecurity R&D development towards self-reliance shall be introduced. Through cybersecurity R&D needs analysis, Government will establish inter-agency and inter-sector coordination on this initiative. Government shall encourage and promote partnerships with the private sector, academia, research institutions and international partners by creating incentives for cybersecurity innovation. A dedicated budget for Ghana's cybersecurity R&D shall be sourced from the Cybersecurity Fund.	Medium to Long-term	• CSA • JCC • Other relevant MDAs • Non- Governmental Stakeholders

6.0.4 Deter Cybercrime

Cybercrime is a threat to Ghana's vision of developing its economy through digitalisation as it has both direct and indirect impacts on Ghana's developmental agenda. Cybercrimes range from cyber-enabled and cyber-dependent crimes. Cybercrime actors include individuals, organised groups as well as state-sponsored. Ghana's response to cybercrime is based on the concept of deterrence. This is by adopting relevant proactive and reactive measures to ensure cybercrime becomes a high-risk venture for perpetrators. The deterrence approach will also culminate in raising the security posture of the digital infrastructure. Ghana will continue to foster global alliances and promote criminal justice response to cybercrimes through the application of both domestic and international laws and treaties.

6.0.4.1 Strategic Objectives

Strategic objectives underlining the strategic imperative are presented below:

1. Ghana will pursue, adopt and implement relevant policies, strategies and legislation to counter both existing and emerging cybercrime trends whiles upholding the rule of law in cyberspace.

2. Ghana will pursue the necessary deterrent actions to minimise the impact of cybercrime on our domestic and global economies.

3. Ghana will equip its law enforcement and criminal justice authorities, to maintain relevant and proportionate capabilities to enforce existing and future cybercrime legislation, consistent with its obligations under international, regional, and national human right laws.

4. Ghana will pursue appropriate offensive and defensive cyber capabilities as part of our medium to long term cybercrime response capabilities to serves as a deterrent to those who intend to undermine the digital life of the citizens, business and government.

5. Ghana will continue to review its legislation to ensure they are relevant, effective and responds to all forms of cybercrime.

6.0.4.2 Strategic Initiatives & Implementation Plan

The following constitutes the Strategic Initiatives & Implementation Plan that Ghana seeks to implement towards achieving this Strategic Imperative. Timelines and responsibilities are presented for the various initiatives and actions.

Table 5: Deter Cybercrime – Strategic Initiatives and Implementation Plan.

S/N	Strategic Initiative	Description of Strategic Initiative	Time Frame	Responsibility/ Stakeholders
4.01	Establishment of National Digital Forensics Laboratory	Establish a National Digital Forensics Laboratory to support law enforcement agencies to carry out cybercrime and cybersecurity investigations. A national lab for law enforcement agencies with cyber forensics technology shall be established. This initiative involves the development of standard operating procedures and relevant guidelines to support cybercrime and cybersecurity investigations as well as digital forensics case management.	Short to Medium-term	• CSA • JCC • NSCS • Law Enforcement and Security Agencies
4.02	Establish Regional Cybercrime Units	Regional Centres to support cybercrime response in the administrative regions of Ghana shall be established. This will include the establishment of dedicated units with relevant cyber forensic capabilities at each of the administrative/law enforcement agencies in the regions of Ghana. The Units will have the expertise to receive complaints, provide first response and forensics response on cybercrime cases. Such Units will however refer complex cybercrime cases and incidents to the National Digital Forensics Lab.	Short to Long-term	• CSA • JCC • Ghana Police/CID • NSCS • Other relevant international partners (INTERPOL, Council of Europe, etc.)

S/N	Strategic Initiative	Description of Strategic Initiative	Time Frame	Responsibility/ Stakeholders
4.03	Establish Cybercrime Prosecutions Division at the Office of the Attorney-General	Establish a cybercrime prosecutions division at the Office of the Attorney-General's Department to facilitate the prosecution of cybercrime cases. This will increase our national response in addressing cybercrime and help improve our institutional structures by engaging the relevant institutions in the fight against cybercrime and provide for other related matters. The division will have expertise with knowledge in cyber law to complement their background in traditional law for effective adjudication of cyber-facilitated crimes.	Short to Long-term	• CSA • JCC • Office of the Attorney-General and Ministry of Justice
4.04	Establish Specialised Courts for Cybercrime	Establish specialised courts for prosecuting cybercrime cases. This will project our national response and commitment to addressing cybercrime by building strong institutions with a mandate on the matter. The specialised courts will have Judges and Officials with expertise in cyber law to appreciate cybercrime and cybersecurity issues for effective adjudication of cyber-facilitated crimes and provide for other matters.	Short to Long-term	• CSA • JCC • Judicial Service • NSCS • Ghana Bar Association
4.05	Review of Evidence Act	A review of Ghana's Evidence Act–1975 (NRCD 323) to provide a clear legal framework for the admissibility of digital evidence. This initiative involves gap analysis on the effectiveness of the current Evidence Act in addressing cybercrime prosecution and adjudications. This initiative will ensure digital evidence is given equal treatment as other traditional forms of evidence in view of the current digitalisation context. Office of the Attorney-General and Ministry of Justice Department working in collaboration with relevant agencies shall lead efforts on the review of the Evidence Act.	Medium-term	• CSA • JCC • Office of the Attorney-General and Ministry of Justice • NSCS • Law Reform Commission • Ghana Police/CID • Ghana Bar Association • Other relevant international partners

S/N	Strategic Initiative	Description of Strategic Initiative	Time Frame	Responsibility/ Stakeholders
4.06	Training for Criminal Justice Sector	Equip the criminal justice sector with the right knowledge, skills and tools to respond, investigate and prosecute cybercriminals. Establishment of institutional capacity building programmes for judges, prosecutors, police personnel and officials from other security agencies. Continuous training for Judges, Prosecutors and Investigators through the integration of cybercrime and digital evidence courses into the curriculum of criminal justice sector training institutions. Training on cybercrime and digital evidence for members of the Ghana Bar Association shall also be implemented as part of this initiative.	Short to Long-term	• CSA • JCC • Other relevant international partners (INTERPOL, Council of Europe, etc.) • Ghana Bar Association • Judicial Training Institute

6.0.5 Strengthen Cooperation

Cybersecurity is not only a cross-cutting issue; it is also a transnational issue. In the past few years, cybersecurity has dominated both economic and security debates at the international level. As a result, Ghana will pursue a free, open, innovative and secure cyberspace as part of its foreign policy. Ghana will pursue relevant actions and strategies that seek to advance this policy direction. The in-country cooperation on cybersecurity through the work of the Joint Cybersecurity Committee (JCC) and other relevant engagements shall be strengthened. Ghana will also lead sub-regional and regional efforts on cybersecurity especially at the ECOWAS and the African Union. The country shall continue to actively engage in international treaties, partnerships and engagements with its partners including the United Nations, the Council of Europe and the Commonwealth to solidify international response against cybercrimes.

6.0.5.1 Strategic Objectives

Strategic objectives underlining the strategic imperative are presented below:

1. Ghana will continue to pursue and strengthen its domestic cooperation mechanisms in addressing cybercrime challenges.
2. Issues of cybersecurity are cross-cutting and trans-sectoral in nature. As a result, Ghana will adopt an inclusive and multi-stakeholder approach at the domestic, regional and international levels in addressing the challenges of cybercrime.
3. Ghana will identify opportunities, leverage on our influence in West Africa and invest in cybersecurity development in the sub-region especially through the ECOWAS.
4. In view of the current development of cybersecurity at the international level, Ghana will promote - as part of its foreign policy - a free, open, innovative, and secure cyberspace; and stakeholder engagement. This is based on the principle that the behaviour of countries in cyberspace is governed by international law.
5. Ghana will pursue and strengthen both formal and informal cooperation mechanisms with governments, international organisations and private sector as part of its policy towards builing a global consensus on responsible behaviour in cyberspace.

6.0.5.2 Strategic Initiatives & Implementation Plan

The following constitutes the Strategic Initiatives & Implementation Plan that Ghana seeks to implement towards achieving this Strategic Imperative. Timelines and responsibilities are presented for the various initiatives and actions.

Table 6: Strengthen Cooperation – Strategic Initiatives and Implementation Plan.

S/N	Strategic Initiative	Description of Strategic Initiative	Time Frame	Responsibility/ Stakeholders
5.01	Cybersecurity Foreign Policy & Initiatives	Ghana will promote cybersecurity development at the sub-regional, regional and international levels through a focused foreign policy engagement underpinned by bilateral and multilateral engagements.Ghana will pursue a free, open, innovative and secure cyberspace for all agenda as part of our foreign policy. In this regard, Ghana will participate in international engagements that seek to further the above goals. Ghana will promote these ideals through active involvement of governmental and non-governmental engagement with the ECOWAS, Africa Union, Commonwealth, United Nations and Freedom Online Coalition (FOC), among others. The Government will support regional and continental initiatives aimed at promoting human rights and the rule of law in the cyberspace.	Short to Long-term	• CSA • Ministry of Foreign Affairs & Regional Integration • JCC • Other relevant international partners
5.02	Adoption and Implementation of International Treaties on Cybercrime & Cybersecurity	Ghana will adopt and implement relevant regional and international treaties on cybercrime and cybersecurity. Implementation of the Convention on Cybercrime (Budapest Convention) and the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention) as well as the ECOWAS Directive on Cybercrime are important components of this initiative. Ghana will also pursue other relevant international cooperation agreements through the ECOWAS, AU, Commonwealth and the United Nations, among others.	Short to Long-term	• CSA • JCC • Ministry of Foreign Affairs & Regional Integration • Office of the Attorney-General and Ministry of Justice • NSCS • Non- Governmental Stakeholders • Other relevant international partners

S/N	Strategic Initiative	Description of Strategic Initiative	Time Frame	Responsibility/ Stakeholders
5.03	Formal Cooperation	Develop a formal agreement with international partners to foster and strengthen cooperation on cybersecurity. Ghana will implement the necessary cooperation arrangements through existing Mutual Legal Assistance provisions and establish a 24/7 point of contact to provide immediate assistance for Mutual Legal Assistance requests. Bilateral engagements and partnerships with other governments and international institutions shall be pursued under this initiative.	Short to Long-term	• CSA • JCC • Ministry of Foreign Affairs & Regional Integration • Other relevant international partners
5.04	Informal Cooperation	As part of strengthening our international relations, Ghana will develop informal relations with relevant international bodies in addressing cybercrime. Ghana will strengthen cooperation with institutions such as AFRIPOL, EUROPOL and INTERPOL in the fight against cybercrime. Ghana will work closely with the international community and regional partners to strengthen platforms and procedures for cyber incident reporting and response. Ghana will Participate in international forums and conferences on cybercrime including internet governance forum and UN-led discussions among others.	Short to Long-term	• CSA • JCC • Other relevant international partners
5.05	Domestic Cooperation	This initiative involves coordinated engagements between government and key cybersecurity actors in promoting national cybersecurity development. This involves the development and operationalisation of the JCC Charter. Regular engagements between Government and Academia, Businesses, Civil Society Organisations, local representatives of international bodies, professional associations and industry will be pursued.	Short to Medium-term	• CSA • JCC • Non- Governmental Stakeholders

S/N	Strategic Initiative	Description of Strategic Initiative	Time Frame	Responsibility/ Stakeholders
5.06	Tech & Cyber Diplomacy	Ghana will pursue cooperation with multinational technology providers and other relevant players in the technology space through Cyber Diplomacy. In view of this, Ghana will support and contribute to international discussions and multi-stakeholder engagements involving tech giants aimed at promoting the responsible use of the cyberspace, especially in relation to the role of tech giants in achieving Ghana's cybersecurity.	Short to Long-term	• CSA • Ministry of Foreign Affairs & Regional Integration • JCC • Multinational Tech Firms (Facebook, Google, etc.) • Other relevant international partners

Implementation

7.0 Implementation of the National Cybersecurity Policy & Strategy

The National Cybersecurity Policy and Strategy which drives our cybersecurity agenda is considered a significant determinant to the sustainable operations of the country's digitalisation initiatives. Consistent with best practice approach to cybersecurity development, monitoring and evaluation constitute a key factor for the effective implementation of cybersecurity initiatives. This informs the Government's prioritisation and allocation of resources and investments in crucial areas of development. Due to this, the government has prioritised the investment in a digital solution with components and features capable of monitoring and evaluating the implementation status of the strategic initiatives at each stage of our cybersecurity journey. Our implementation plan for the next five years revolves around the five key strategic imperatives which aim to BUILD a resilient digital ecosystem, SECURE the country's digital infrastructure, DEVELOP national capacity, DETER the country from cybercrime and STRENGTHEN cybersecurity cooperation at the domestic and international levels, all underpinned by the policy statements. A digital solution will provide a progress report and gap analysis of work being done in our cybersecurity arena with respect to the implementation of the National Cybersecurity Policy and Strategy (NCPS).

Purpose

The digital solution to facilitate the implementation of the NCPS is being deployed as a monitoring and evaluation mechanism to determine the progress status yearly over the five-year implementation period of the specific initiatives of the Strategy. The solution is meant to measure the rate, impact, successes and challenges associated with the implementation of the Cybersecurity Strategy. The technology shall inform in the feasibility study of targets set to achieve the strategic initiatives as well as provide gap analysis involved in the implementation of the NCPS. It shall assess the impact of the implementation on the Ghanaian digital economy based on the objectives set for each of the strategic imperatives, the successes achieved in the implementation and the challenges to guide implementation of programmes and activities.

8.0 Monitoring and Evaluation

Our Monitoring & Evaluation (M&E) Approach

To measure the rate, impact, successes and challenges associated with the implementation of this strategy, the government will implement Monitoring and Evaluation (M&E). The M&E mechanisms to be implemented shall measure the rate of the realisation of the strategy based on the timelines stated. It shall assess the impact of the implementation on the Ghanaian digital economy based on the objectives set for each of the Strategic Imperatives, the successes achieved in the implementation as well as the challenges to guide future implementation of programmes and activities. A number of mechanisms shall be adopted as part of the M&E:

- Development of evidence-based M&E metrics to measure the impact of the strategy against its objectives.
- Deployment of a software solution (digital platform) to measure the rate of implementation, both in the public and the private sector, taking into consideration all sectoral programmes and initiatives.
- Collating and analysing cybercrime reports from CERT-GH and law enforcement agencies to ascertain the frequency and magnitude of cybercrime trends in the country.
- Conduct cybersecurity assessment on key institutions to establish their capabilities in addressing cybersecurity issues.
- Implement a gap analysis framework to measure cybersecurity awareness of personnel to determine areas of needed improvement.
- Conduct surveys to measure the impact, successes and challenges associated with the implementation of specific strategic initiatives and programmes.
- Administer institutional capacity assessment questionnaire to assess the readiness of the sectors in detecting, responding and addressing cybersecurity issues.
- Workshops and conference reports will be produced and analysed to determine the strength of collaborations.

Success Indicators

The success in the implementation of this strategy is based on specific deliverables and measurable results to the public, businesses, the government and the international community. The following provide insights into the success indicators:

Success Indicators - Build a Resilient Cyber Ecosystem

- Evidence of cybersecurity incident reporting to CERT-GH and other Sectoral CERTs by the public and businesses.
- Improved capability for cybersecurity incident monitoring and prevention across all sectors.
- Improved response to cybersecurity incidents, demonstrated by the ability to quickly restore digital services and systems after successful cyber-attacks.
- Improved understanding of cybercrimes and cybersecurity incidents as well as the ability to quantify losses arising from cybersecurity breaches.

Success Indicators - Secure our Digital Infrastructure

- Strengthened digital infrastructure with high resilience to cyber-attacks, evidenced partly by recorded failed attacks.
- Reduced impact of cyber-attacks and duration required to recover from such attacks against our Critical Information Infrastructure (CII) and Government Digitalisation Initiatives (GDIs)
- Better understanding of threats targeting CII and GDIs as well as the entire digital ecosystem.
- Increased trust in Ghana's digital ecosystem, evidenced partly by public confidence in the use of digital services.

Success Indicators - Develop National Capacity

- An improved and developed culture of cybersecurity, evidenced in knowledge and awareness of cyber risks as well as, the actions to be taken regarding cybersecurity, by Children, the Public, Businesses and Government.
- Evidence of coordinated and integrated cybersecurity education across all levels especially in the formal education sector.
- Increase in investment in cybersecurity by the Ministries, Departments & Agencies (MDAs) and private sectors, including regular budget allocations for cybersecurity.
- Evidence of adoption and enforcement of nationally-approved cybersecurity standards, guidelines and best practices across all sectors.
- Improved ability to measure the impact of cybercrimes and cybersecurity incidents, including financial costs to the Ghanaian economy.
- Evidence of the growth of the local cybersecurity ecosystem including development of domestic workforce through partnerships between government and local firms, academia and international partners.

Success Indicators -Deter Cybercrime

- Improvement in law enforcement capability to detect, investigate and prosecute cybercrimes in a reasonable timeframe.
- A higher proportion of incidents being reported to authorities due to increased public awareness, trust and cooperation with state institutions responsible for cybercrime prevention and response.
- New skill set, tools and strategies to detect, monitor and disrupt activities of cybercriminals especially by organized cybercrime networks.
- Effective legal framework, enforcement capabilities to investigate cybercrime cases and an increase in the number of arrests and conviction of cybercriminals to serve as deterrent to would-be offenders.
- Increase in the level of public trust in law enforcement and criminal justice authorities in responding to cybercrimes.

Success Indicators - Strengthen Cooperation

- Improved and coordinated response to cybercrime and cybersecurity issues, indicated by effective, structured engagements by members of the National Cyber Security Technical Working Group.
- Improved cooperation with international partners to investigate and prosecute cybercrime cases including joint investigation actions.
- Active involvement and contributions of Ghanaian public sector officials and private sector subject matter experts in cybersecurity discussions at the international level.
- Improvement in the number of cybersecurity related engagements being championed by Ghana, both in the public and private sectors, in the West African sub region.
- Ghana's ability to strengthen international consensus on legal regulations and responsible behaviour in cyberspace by promoting the benefits of a free, open, innovative and secure cyberspace; stakeholder engagement; and the principle that state behaviour in cyberspace is governed by international law. Increase in Ghanaian participation and organisation of international cybersecurity exercises, trainings and capacity building programmes.

9.0 Funding For National Cybersecurity

In accordance with Sections 29 to 34 of the Cybersecurity Act,2020 (Act 1038), the establishment of a reliable domestic source of funding is imperative to provide guaranteed funding for the country's cybersecurity development and to protect Ghana's investment in digital transformation, consistent with international best practices. Sustained funding is required to be able to implement the Act and the revised National Cybersecurity Policy and Strategy. The National Cybersecurity Policy and Strategy identifies various initiatives and programmes of activities that will require financial resources to implement. The Ministry of Communications and Digitalisation in collaboration with relevant Ministries and Agencies will define the budget for short term, medium-term and long term strategic national cybersecurity goals.

Ghana's economic prosperity is inherently linked to Confidentiality, Integrity and Availability of the country's Critical Information Infrastructure (CII) and the entire national cyber ecosystem. Consequently, the Government will create a sustainable national budget for cybersecurity. Thus, a Cybersecurity Fund pursuant to the Act shall be established to support the implementation of this policy and to facilitate cybersecurity research and innovation towards self-reliance in pursuance of a Safer Digital Ghana.

10.0 Conclusion: Cybersecurity Beyond 2027

The policy direction and the strategic initiatives outlined in this document are designed to address the cybersecurity challenges in the next five years. While some of the policies and initiatives are completely achievable within the timeframes allocated, given the allocation of the right resources, the formulation and implementation of other policies and initiatives respectively are likely to go beyond 2027. Consequently, the government will continue to monitor the implementation of this policy and strategy, prioritise specific initiatives based on national needs analysis to ensure prudent allocation of resources.

11.0 Acknowledgement

The development of this document will not have been possible without the commitment and collaboration of a number of key stakeholders. Appreciation goes to the Sector Minister, Hon Ursula Owusu-Ekuful, for her exceptional leadership in championing Ghana's cybersecurity development. Our gratitude to Members of the Governing Board of the Cyber Security Authority (CSA) which was established by H.E. Nana Addo Dankwa Akufo-Addo for providing policy direction to the country's cybersecurity development. Members of the Joint Cybersecurity Committee (JCC), led by the Head of the Cyber Security Authority (CSA) Dr. Albert Antwi-Boasiako, are duly acknowledged for their lead roles, collaborative efforts and contributions towards the development of the policy and strategy.

The Ministry of Communications and Digitalisation also expresses its appreciation to Members of the Parliamentary Select Committee on Communications for their valuable contributions to the development of the document. The Ministry is also grateful to Ghana's cybersecurity development partners including the ECOWAS Commission, the African Union Commission, the World Bank, International Telecommunications Union, the Council of Europe, the European Union, UNICEF, Freedom Online Coalition, the United States Government through the Security Governance Initiative (SGI) and the Government of the United Kingdom for their support and valuable contributions.

Ghana's domestic stakeholders continue to play critical roles in the development of national interventions to mitigate cybercrime and cybersecurity. A number of non-governmental stakeholders comprising representatives from industry, academia, professional associations and civil society groups contributed to the review of the document. The Ministry is indebted to all these institutions for their continuous commitment towards improving Ghana's cybersecurity readiness.

The Ministry of Communications and Digitalisation expresses its appreciation to all the staff of the National Cyber Security Centre for leading the development of this important production towards a secure and resilient Digital Ghana. Finally, the Ministry is grateful to the Ghanaian public – both at home and abroad for their keen interest and contributions towards the adoption of a new National Cybersecurity Policy and Strategy which seeks to guide our cybersecurity development for the next five years.

12.0 Annex 1: Acronyms

Table 7: Table of Abbreviations and Description.

Abbreviation	Description
AFRIPOL	African Criminal Police Organisation
AU	African Union
BoG	Bank of Ghana
CERTs	Computer Emergency Response Teams
CID	Criminal Investigations Department
CMM	Cybersecurity Capacity Maturity Model
CII	Critical Information Infrastructure
COP	Child Online Protection
CSA	Cyber Security Authority
DI	Defence Intelligence
DDoS	Distributed Denial-of-Service
DoS	Denial-of-Service
EUROPOL	European Criminal Police Organisation
FOC	Freedom Online Coalition
GCI	Global Cybersecurity Index
GCSCC	Global Cyber Security Capacity Centre
GLACY+	Global Action on Cybercrime Extended
GSA	Ghana Standards Authority
ICT	Information Communication Technology
INTERPOL	International Criminal Police Organisation
IT	Information Technology
ITU	International Telecommunications Union
JCC	Joint Cybersecurity Committee
MDAs	Ministries, Departments & Agencies
M&E	Monitoring and Evaluation
NAB	National Accreditation Board
NCA	National Communications Authority
NCCE	National Commission for Civic Education
NCIF	National Cybersecurity Institutional Framework
NCSC	National Cyber Security Centre
NCSIAC	National Cyber Security Inter-Ministerial Advisory Council

Abbreviation	Description
NCPS	National Cybersecurity Policy and Strategy
NGOs	Non-Governmental Organisations
NIB	National Intelligence Bureau
NIS	National Identification System
NITA	National Information Technology Agency
NPAS	National Property Addressing System
NBS	National Signals Bureau
NSCS	National Security Council Secretariat
OCSEA	Online Child Sexual Exploitation and Abuse
PKI	Public Key Infrastructure
R&D	Research and Development
SDGs	Sustainable Development Goals
SOCs	Security Operations Centres
SOPs	Standard Operating Procedures
UN	United Nations
UNCTAD	United Nations Conference for Trade and Development
UNICEF	United National International Children Emergency Fund
UNODC	United Nations Office on Drugs & Crime

13.0 Annex 2: Glossary Of Terms

Cyberattack → A deliberate attempt to damage, disrupt, or gain unauthorised access to a computer, computer system or electronic communication network.

Cybercrime → Include both cyber-dependent and cyber-enabled crimes.

Cyber-dependent crimes → Crimes committed through the use of ICT devices, and where the devices are both the tool for committing the crime, and the target of the crime.

Cyber-enabled crimes → Traditional crimes which can be increased in scale or reach by the use of computers, computer networks or other ICTs.

Cybersecurity → The state in which a computer or computer system is protected from unauthorised access or attack for the purpose of ensuring that

a. the computer or computer system continues to be available and operational;
b. the integrity of the computer or computer system is maintained; and
c. the integrity and confidentiality of information stored in, processed by or transmitted through the computer or computer system is maintained.

Cyberspace → The interdependent network of information technology infrastructure that includes the internet, telecommunications networks, computer systems, internet-connected devices and embedded processors and controller.

Identity Theft → The deliberate use of someone else's identity, usually as a method to gain access, financial advantage or gain other benefits in the other person's name.

Malware → Malware is any software intentionally designed to cause damage to a computer, server, client, or computer network.

MDAs → Consists of Government Ministries, Departments and Agencies.

National CERT → A Computer Emergency Response Team responsible for facilitating and coordinating incident response procedures at the national level.

Non-Governmental Actors → Comprises of the Private Sector, Academia & Research Institutions, Civil Society, Professional and Industry Associations and International Organisations.

Ransomware → Malicious software that denies the user access to their files, computer or device and in some cases threatens to publish user's private data unless a ransom is paid.

Risk → The potential that a threat will exploit a vulnerability of an information system and cause harm.

Safeguard → A reducing measure that acts to detect, prevent, or minimise loss associated with the occurrence of a specific threat or category of threats.

Sectoral CERT → A Computer Emergency Response Team responsible for facilitating and coordinating incident response procedures at the sectoral level.

Social Engineering → The psychological manipulation of people into performing actions or divulging confidential information.

Vulnerability → Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

REPUBLIC
OF GHANA