MINISTRY OF
COMMUNICATIONS &
DIGITALISATION

NATIONAL
CYBER SECURITY
AWARENESS MONTH
2021

REPORT

GHANA'S CYBERSECURITY ACT 2020

ITS IMPLICATIONS AND THE ROLE OF STAKEHOLDERS

A Safer Digital Ghana

TABLE OF CONTENTS

i ACKNOWLEDGEMENT

ii ACRONYMS

iii EXECUTIVE SUMMARY

v **GHANA'S CYBERSECURITY GOVERNANCE** – Leadership

vi **NATIONAL CYBER SECURITY TECHNICAL WORKING GROUP** (NCSTWG)

01 **OFFICIAL LAUNCH OF THE NATIONAL CYBER SECURITY AWARENESS MONTH (NCSAM) 2021, A DIRECTIVE FOR THE PROTECTION OF CRITICAL INFORMATION INFRASTRUCTURE (CII) AND THE CYBER SECURITY AUTHORITY (CSA).**

13 **WORKSHOP ON THE CYBERSECURITY ACT, 2020 (ACT 1038)** and the Directive for the Protection of Critical Information Infrastructure (CII)

17 **WORKSHOP ON LAW ENFORCEMENT AGENCY TRAINING STRATEGIES**

19 **WORKSHOP ON THE INTEGRATION OF EUROPEAN CYBERCRIME TRAINING AND EDUCATION GROUP TRAINING MATERIALS**

21 **FORUM ON THE CYBERSECURITY ACT, 2020 (ACT 1038)** for Cybersecurity Service Providers and Professionals

22 **OPENING REMARKS**
Dr. Albert Antwi-Boasiako
Ag. Director-General,
Cyber Security Authority (CSA)

23 **KEYNOTE ADDRESS**
Hon. Ursula Owusu-Ekuful, Minister for Communications and Digitalisation (MOCD)

24 **PRESENTATION**
Safeguarding the Gains of Digitalisation In Ghana – The National Information Technology Agency's (NITA) Role as the ICT Regulator by Mr. Richard Okyere-Fosu, Director-General, NITA

25 **PANEL DISCUSSION & MESSAGE FROM SPONSORS**

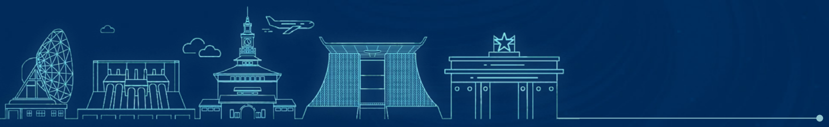


TABLE OF CONTENTS

27 **MULTI-STAKEHOLDER WORKSHOP ON** Global Internet Forum To Counter Terrorism (GIFCT), Tech Against Terrorism (TAT) and Cyber Security Authority (CSA)

28 **PRESENTATION** State of Play-Expert Researchers and Government threat assessment

30 **WORKSHOP ON IMPACT OF THE NEW CYBERSECURITY ACT, 2020 (ACT 1038)** on Computer Emergency Response Team (CERT) Operations

32 **MULTI-STAKEHOLDER WORKSHOP** The Streamlining of Procedures for MLA enhanced by the Second Additional Protocol related to Cybercrime and Electronic Evidence

36 **SPECIALISED COURSE** on the International Cooperation for Prosecutors And Judges

39 **FORUM** Women in Technology and Cybersecurity

43 **CLOSING REMARKS** Hon. Ama Pomaa Boateng, Deputy Minister for Communications and Digitalisation

44 **HIGH-LEVEL & REGIONAL ENGAGEMENTS ON THE CYBERSECURITY ACT, 2020 (ACT 1038)**

46 **NCCE UNDERGOES TRAINING ON THE CYBERSECURITY ACT, 2020 (ACT 1038);** Fake News

47 **WORKSHOP ON THE CYBERSECURITY ACT, 2020 (ACT 1038)** for the Criminal Justice Sector

48 **WORKSHOP ON THE NEW CYBERSECURITY ACT, 2020 (ACT 1038)** for Government Chief Executive Officers

49 **REGIONAL ENGAGEMENTS**

52 **HIGH-LEVEL ENGAGEMENTS ON THE NEW CYBERSECURITY ACT, 2020 (ACT 1038)** with the Ghana Journalists' Association (GJA)

53 **CONCLUSION**

54 **RECOMMENDATION**

55 **PHOTO GALLERY**

64 **PARTNERS & ORGANISING PARTNERS**

65 **SPONSORS & MEDIA PARTNERS**

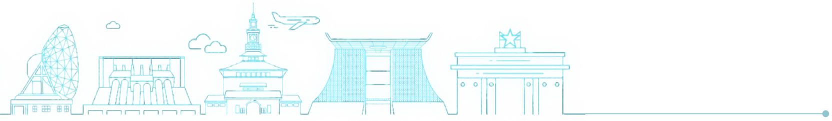
ACKNOWLEDGEMENT

Hon. Mrs. Ursula Owusu-Ekuful
Minister for Communications and Digitalisation

The progress and accolades of Ghana's Cybersecurity development chalked at the local and international scene is largely owed to the political commitment from the occupant of the highest office of the country, His Excellency Nana Addo Dankwa Akufo-Addo which led to the passage of the Cybersecurity Act, 2020 (Act 1038) by the 7th Parliament of the Republic of Ghana and subsequent assention into law by the President on December 29, 2020. This provision effectively led to the establishment of the Cyber Security Authority (CSA) with the mandate to regulate cybersecurity activities in the country; to promote the development of cybersecurity in the country and to provide for related matters. The Minister for Communications and Digitalisation (MoCD), Hon. Ursula Owusu-Ekuful expresses gratitude to the President for his vision, dedication and leadership exhibited towards securing Ghana's digital ecosystem through priority and strategic investments in cybersecurity. The Ministry also wishes to thank His Excellency, the Vice President, Dr. Alhaji Mahamudu Bawumia for his commitment to prioritising the Digital Ghana Agenda which is massively complimented by proactive cybersecurity initiatives for a secured cyberspace.

Appreciation goes to the various roles played by Members of the National Cyber Security Inter-Ministerial Advisory Council (NCSIAC) in providing policy direction to the country's cybersecurity development. Members of the National Cyber Security Technical Working Group (NCSTWG) are duly acknowledged for their efforts and hard work in providing technical advice on the country's cybersecurity agenda. An extension of gratitude goes to the event Planning Committee and the various sub-committees for the excellent work in organising the National Cyber Security Awareness Month (NCSAM) 2021.

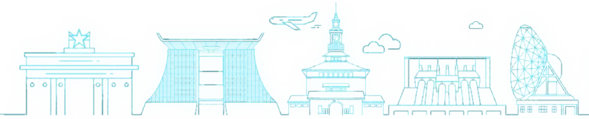
The Ministry of Communications and Digitalisation (MoCD) is much grateful to the various sponsors and international partners for their support and commitment by way of investments in the country's cybersecurity cause. The Ministry highly commends individuals, civil society institutions, businesses, academia, government and non-government organisations for their participation in the month-long event which has significantly contributed to capacity building and awareness creation on cybercrime trends and improving Ghana's cybersecurity among Children, the Public, Businesses, and Government for a Safer Digital Ghana.



ACRONYMS

CSA	Cyber Security Authority
MoCD	Ministry of Communications and Digitalisation
NCSIAC	National Cyber Security Inter-Ministerial Advisory Council
NCSAM	National Cyber Security Awareness Month
CII	Critical Information Infrastructure
CERTs	Computer Emergency Response Teams
CBAC	Capacity Building and Awareness Creation
COP	Child Online Protection
ECOWAS	Economic Community of West African States
GJA	Ghana Journalists' Association
SIGA	State Interests and Governance Authority
REGSEC	Regional Security Councils
NCCE	National Commission for Civic Education
NCSTWG	National Cyber Security Technical Working Group
NCA	National Communications Authority
NCA-CERT	NCA Computer Emergency Response Team
ITU	International Telecommunication Union
UNICEF	United Nations International Children's Emergency Fund
JCC	Joint Cybersecurity Committee
GCI	Global Cybersecurity Index
ICT	Information and Communications Technology
GARNET	Ghanaian Academic and Research Network
GWCL	Ghana Water Company Limited
NAS	National Ambulance Service
NADMO	National Disaster Management Organisation
NPRA	National Pensions Regulatory Authority
SOC	Security Operations Centre
ECG	Electricity Company of Ghana
BPA	Bui Power Authority
BOST	Bulk Oil Storage and Transportation Company Limited
NPA	National Petroleum Authority
GCAA	Ghana Civil Aviation Authority

GMA	Ghana Maritime Authority
CoE	Council of Europe
CID	Criminal Investigations Department
BNI	Bureau for National Investigations
EOCO	Economic and Organised Crime Office
NIB	National Intelligence Bureau
INTERPOL	International Criminal Police Organisation
KAIPTC	Kofi Annan International Peacekeeping and Training Centre
NITA	National Information Technology Agency
GIFCT	Global Internet Forum to Counter Terrorism
PVE	Preventing Violent Extremism
CVE	Countering Violent Extremism
TaT	Tech Against Terrorism
NITA-SOC	National Information Technology Agency Security Operations Centre
ISWA	Islamic State West Africa
TCAP	Terrorist Content Analytics Platform
MLAT	Mutual Legal Assistance Treaty
NSB	National Signals Bureau
MLA	Mutual Legal Assistance
EJCN	European Judicial Cybercrime Network
UNTOC	United Nations Convention against Transnational Organised Crime
UNCAC	United Nations Convention against Corruption
CCPE	Consultative Council of European Prosecutors
EJCN	European Judicial Cybercrime Network
PPP	Public Private Partnerships
DPC	Data Protection Commission
GITTA	Ghana Information Technology and Telecom Awards
GNAT	Ghana National Association of Teachers
GBA	Ghana Bar Association
SOEs	State-Owned Enterprises
GNCCI	Ghana National Chamber of Commerce and Industry



EXECUTIVE SUMMARY

The National Cyber Security Awareness Month (NCSAM) 2021, was organised from October 1-31, 2021 under the theme “Ghana's Cybersecurity Act 2020: Its Implications and the Role of Stakeholders". It was the fifth in the series to be convened since the introduction of the programme by the then National Cyber Security Secretariat, in 2017. A number of workshops, programmes and activities were held across the country as part of the month-long event. The objectives of the 2021 edition were:

- To officially launch the Cyber Security Authority (CSA) to deliver on its mandate by implementing the Cybersecurity Act, 2020 (Act 1038)
- To launch the Critical Information Infrastructure (CII) Directive
- To create awareness on the Cybersecurity Act 2020 (Act 1038) among Ghanaians.
- To build upon the “A Safer Digital Ghana” campaign by creating awareness among children, the public, businesses and the government.
- To create a platform to engage local and international partners and stakeholders to interact and discuss matters related to cybersecurity and cybercrime.

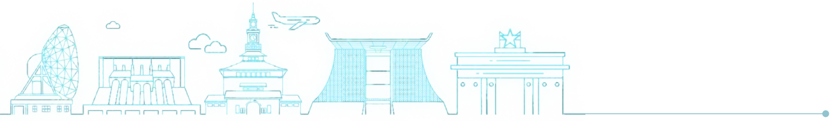
NCSAM 2021 was primarily focused on key areas of Ghana’s cybersecurity development based on Act 1038, including Critical Information Infrastructure (CII) protection, Computer Emergency Response Teams (CERTs), Capacity Building and Awareness Creation (CBAC) and Child Online Protection (COP). The event was also to help Ghana to build upon its foundational cybersecurity pillars, which had been ranked 3rd on the African continent with a rating of 86.69% according to the ITU’s Global Cybersecurity Index report, 2020.

The event brought together stakeholders from government and private sectors, civil society, the international community, academia, the media and members of the public to brainstorm on cybercrime and cybersecurity issues and how to collaborate to successfully implement the Act. Activities were conducted in a hybrid format, comprising physical engagements (under strict COVID-19 protocols) and the utilisation of available virtual platforms. It involved thought ttleadership sessions, high-level events, workshops, lectures, demonstrations, training sessions, and media engagements.

The first major event was the formal launch of the NCSAM 2021, the Cyber Security Authority (CSA), and the Critical Information Infrastructure (CII) Directive on Friday, October 1, 2021, at the 2nd floor of the NCA Tower in Accra by the Minister for Communications and Digitalisation, Hon. Mrs Ursula Owusu-Ekuful. She also unveiled the Authority’s logo together with the Minister of Energy, Hon. Dr. Mathew Opoku Prempeh on the 3rd Floor of the NCA Tower. Key stakeholders from government and non-government institutions including CII owners, partners, the media fraternity, and Ghana's cybersecurity international partners participated in the event.

Consequently, the Industry Forum with Cybersecurity Service Providers and Professionals was held on October 11, 2021. The highly patronised event was an opportunity for the players in the industry to appreciate the provisions of the Cybersecurity Act, 2020 that have direct bearing on their profession and the industry at large. The discussions centered on among other things, the establishment of an Industry Forum as provided for in Section 81 of the Act and the need for all Cybersecurity professionals and practitioners to be accredited and licensed by the CSA as mandated by Section 57 of Act 1038.

The Forum on Women in Technology and Cybersecurity was another flagship and highly inspiring event held on October 25, 2021. This event, moderated by the Minister for Communications and Digitalisation, Hon. Mrs. Ursula Owusu-Ekuful, provided a platform for women who had



excelled in the area of technology and cyber security to share their experiences and to challenge other ladies to persevere into the technology and cybersecurity space. The panel for the discussions was composed of Mrs. Patricia Obo-Nai, Chief Executive Officer, Vodafone Ghana, Ms. Folake Olagunju, Programmes Officer, Internet and Cybersecurity, Economic Community of West African States (ECOWAS), Ms. Farida Bedwei, CTO Logiciel, Ms. Adoma Peprah, Country Manager, VISA Ghana, and Mrs. Lucy Quist, Managing Director, Morgan Stanley.

The Acting Director-General of the CSA, Dr. Albert Antwi-Boasiako also strategically aligned himself with the events of the month, engaging with a number of stakeholders in different parts of the country. He delivered lectures and presentations to specific groups urging them to see cybersecurity issues as a critical national issue that has effects on national security as well as the social and economic lives of the people. Among the groups he engaged with on the Act were, the Ghana Journalists' Association (GJA), the Chief Executive Officers under the State Interests and Governance Authority (SIGA), Regional Security Councils (REGSEC), the National Commission for Civic Education (NCCE), the Ghana Bar Association (GBA), the members of the Ghana National Chamber of Commerce and Industry (GNCCI). Dr. Antwi-Boasiako also engaged with resource persons to train personnel from the Criminal Justice Sector on the Act in both Accra and Kumasi.

In all the thought-leadership sessions, workshops, lectures, demonstrations, training sessions, and media engagements, there were lots of engagements and interactions on the Cybersecurity Act, 2020 (Act 1038) and the need for all stakeholders to appreciate how it affects them.

GHANA'S CYBERSECURITY GOVERNANCE –

Leadership

President of the Republic of Ghana

H.E. NANA ADDO DANKWA
AKUFO-ADDO

Vice President of the Republic of Ghana

DR. ALHAJI MAHAMUDU
BAWUMIA

Minister for Communications and Digitalisation

HON. MRS. URSULA
OWUSU-EKUFUL

Dep. Minister for Communications and Digitalisation

HON. AMA POMAA
BOATENG

NATIONAL CYBER SECURITY TECHNICAL WORKING GROUP (NCSTWG)

Acting Director-General
Cyber Security Authority (CSA)

DR. ALBERT ANTWI-BOASIAKO

Joe Anokye
National Communications Authority (NCA)

Richard Okyere Fosu
National Information Technology Agency (NITA)

Patricia Adusei-Poku
Data Protection Commission (DPC)

Yvonne Atakora Obuobisa
Office of the Attorney-General & Ministry of Justice

Justice Afia Serwah Asare-Botwe
Judicial Service of Ghana

Lt. Col. Elikem Fiamavle
Ghana Armed Forces (GAF)

ACP Dr. Herbert Gustav Yankson
Criminal Investigations Department (CID)

Kwabena Adu-Boahene
Bureau of National Communications (BNC)

Kofi Boakye
Financial Intelligence Centre (FIC)

John Fummey
Bank of Ghana (BoG)

Nana Osei Tutu
National Security Council Secretariat

Jacob Puplampu
Economic and Organised Crime Office (EOCO)

Eric Akumiah
Ministry of Communications & Digitalisation (MoCD)

Matilda Wilson
National Identification Authority (NIA)

Gen. Nicholas Andoh
Defence Intelligence

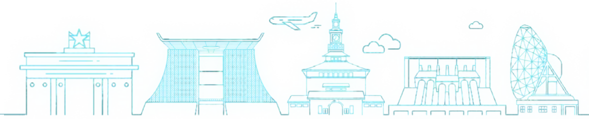
Tim Coleman
Bureau of National Investigations (BNI)

Ken Baiden
Bureau of National Investigations (BNI)

Alexander Yeboah
Research Department

Madam Adisa Yakubu
Ministry of Foreign Affairs & Regional Integration

Nana Kofi Asafu-Aidoo
Ghana Domain Name Registry



OFFICIAL LAUNCH

NATIONAL CYBER SECURITY AWARENESS MONTH (NCSAM) 2021, A DIRECTIVE FOR THE PROTECTION OF CRITICAL INFORMATION INFRASTRUCTURE (CII), AND THE CYBER SECURITY AUTHORITY (CSA)

NATIONAL
CYBER SECURITY
AWARENESS MONTH

BACKGROUND

The 7th Parliament of the Republic of Ghana, on November 06, 2020, passed the historic Cybersecurity Act, 2020 (Act 1038), which was subsequently assented into law by the President H.E. Nana Addo Dankwa Akufo-Addo on December 29, 2020. The Act addresses the gaps in the existing domestic legislation with respect to Ghana's cybersecurity development. The Act provides a legal basis for the establishment of the Cyber Security Authority (CSA) to regulate cybersecurity activities; to protect critical information infrastructure; to provide for the development of the Computer Emergency Response Team (CERT); to promote public awareness and education on cybersecurity matters, and to provide for related matters.

As part of measures to effectively implement Act 1038, the National Cyber Security Centre (NCSC) of the Ministry of Communications and Digitalisation (MoCD) seeks to leverage on the 2021 edition of the annual National Cyber Security Awareness Month (NCSAM) to raise awareness and build capacity on this important development through the theme "Ghana's Cybersecurity Act 2020; Its Implications and the Role of Stakeholders." Therefore NCSAM 2021seeks to engage with relevant stakeholders to deliberate on the Act and its implications, as Ghana seeks to build upon its foundational cybersecurity pillars, which has been ranked 3rd on the African continent with a rating of 86.69% according to the ITU's Global Cybersecurity Index report, 2020.

OBJECTIVES OF THE NATIONAL CYBER SECURITY

Awareness Month (NCSAM) 2021

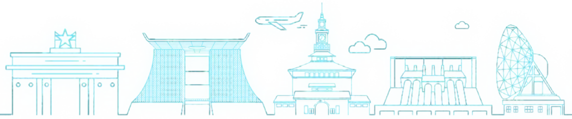
The month-long event aims to:

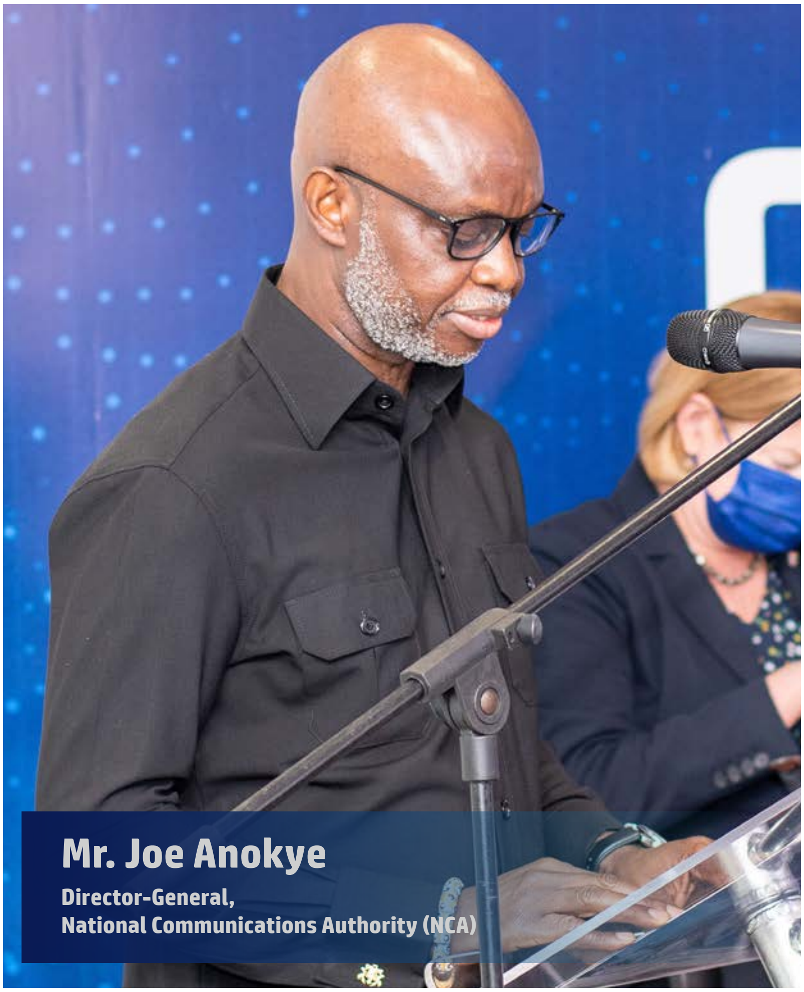
- Officially launch the Cyber Security Authority (CSA) with a mandate to commence its full regulatory mandate.
- Launch the Critical Information Infrastructure (CII) Directive which is designed to protect designated CIIs from cyber-attacks.
- Create awareness on the Cybersecurity Act, 2020 and cybercrime trends while building capacity on cybersecurity among Ghanaians.
- Build upon the Safer Digital Ghana campaign by creating awareness among Children, the Public, Businesses and the Government.
- Create a platform to improve local and international cooperation and partnerships to fight cybercrime and improve cybersecurity, consistent with Act 1038.

EXPECTED OUTCOME

The month-long event is expected to:

- Establish the Cyber Security Authority (CSA) to commence the implementation of the provisions of Act 1038 to protect Ghana's developing digital ecosystem.
- Establish and implement protection mechanisms for all designated Critical Information
- Infrastructure (CII) based on the guidelines outlined in the CII Directive.
- Improve awareness on the Cybersecurity Act among key stakeholders and the Ghanaian public at large.
- Increase awareness of the cybercrime /cybersecurity incidents reporting Points of Contact (PoC) to facilitate reporting of cybercrime and cybersecurity incidents.
- Strengthen formal and informal cooperation at local and international levels on cybercrime /cybersecurityrelated matters to effectively implement Act 1038.





Mr. Joe Anokye

Director-General,
National Communications Authority (NCA)

WELCOME REMARKS

The Director-General of the National Communications Authority (NCA), Mr. Joe Anokye in his welcome remarks at the event indicated that the theme “Ghana’s Cybersecurity, Act 2020: Its Implications and the Role of Stakeholders” was timely, as it “reinforces our collective commitment in ensuring Ghana’s cybersecurity development.”

He added that, globally, the telecommunications sector has contributed immensely to socio-economic development, and the consideration of the sector as a critical information infrastructure sector for nations is therefore not by coincidence.

Mr. Anokye further informed the gathering that the NCA has been actively involved as one of the key public institutions leading digital transformation efforts in the country and has played an integral role in the processes leading to the current development of Ghana’s cybersecurity. “Before the establishment of the National Cybersecurity Secretariat at the then Ministry of Communications in July 2017, the NCA took the necessary steps to implement Ghana’s National Cybersecurity Policy and Strategy through collaborative engagements with the Council of Europe’s GLACY+ Project and other relevant domestic institutions. Subsequently, the NCA established a Cybersecurity Division within the Authority, responsible for cybersecurity activities emanating from the telecommunications sector. These efforts contributed to Ghana’s accession to the Convention on Cybercrime, also known as the Budapest Convention.

The NCA in the year 2018 also established the NCA Computer Emergency Response Team (NCA-CERT), responsible for coordinating cybercrime/cybersecurity incident response in the telecommunications sector. The establishment of the NCA-CERT has been instrumental in Ghana’s cybersecurity incident response efforts as the NCA-CERT constitutes one of the active Sectoral CERTs currently operating within Ghana’s CERT ecosystem. All these critical contributions have culminated in Ghana’s impressive score in the latest International Telecommunication Union (ITU)’s Global Cybersecurity Index which raised Ghana’s cybersecurity profile from 32.6% in 2017 to 86.69% as of December 2020”.

In view of the strong political will and commitment of the sector minister to Ghana’s cybersecurity development, the NCA also committed to providing financial and logistical support to the then National Cyber Security Centre since its establishment. As the Director-General of the NCA, he was pleased to note that, NCA’s support to the National Cyber Security Centre has delivered measurable results by improving the overall cybersecurity posture of the country. He expressed pride to be associated with the success story of our beloved country under the leadership of H.E. Nana Addo Dankwa Akufo-Addo.

He elaborated the NCA’s continuous commitment to Ghana’s cybersecurity development, pledged to take care of the newly established Cyber Security Authority as a kid brother or sister by providing institutional guidance and other forms of support as they carry out their important mandate as provided in Act 1038.

Dr. Albert Antwi-Boasiako

Ag. Director-General,
Cyber Security Authority (CSA)

OPENING REMARKS

Dr. Albert Antwi-Boasiako, the Ag. Director-General of the established Cyber Security Authority (CSA), delivered his opening remarks detailing the journey of the previous body, the National Cyber Security Centre (NCSC) while acknowledging the contribution and efforts of all the key stakeholders to the country's cybersecurity journey.

He indicated that, with the passage of Ghana's landmark Cybersecurity Act, 2020 (Act 1038) by the 7th Parliament in November 2020 and its assent by H.E Nana Addo Dankwa Akufo-Addo, on December 29, 2020, Ghana joined the list of countries in which the rule of law is firmly being applied in the cyberspace; with the aim of mitigating the growing cyber insecurity. TTHence, the theme for the 2021 awareness month was carefully chosen to create a platform for deliberations, dialogue and to create the necessary awareness on the existence of the new Act as the country embarks on a regulatory journey to improve its cybersecurity readiness.

According to Dr. Antwi-Boasiako, the milestones achieved on Ghana's cybersecurity journey are among the world's best. He indicated that Ghana adopted a multi-sectoral governance structure for its national cybersecurity in October 2017, leading to the establishment of the National Cyber Security Inter-Ministerial Advisory Council (NSIAC) and the National Cyber Security Technical Working Group (NCSTWG). This architecture, he said, has been replicated in other sectors of the country and has continued to serve as a national cybersecurity governance benchmark for several African countries and more than 5 countries have requested direct assistance to implement similar structures. He further referenced the National Cybersecurity Awareness Programme, dubbed 'A Safer Digital Ghana' launched by the Vice President, H.E. Dr. Alhaji Mahamudu Bawumia on October 1, 2018, focusing on Children, Businesses, the Public and Government; a model which officials from Ukraine, have requested support to replicate in their country. Among other things Dr. Antwi-Boasiako indicated that:

- Ghana has embarked on a journey for the protection of Children on the Internet through collaboration with UNICEF, an initiative which in 2019 alone, sensitised more than 40,000 students across the 16 regions of the country.
- The ECOWAS Commission requested Ghana to lead cybersecurity development in the sub-region and in 2018, at the sponsorship of the World Bank; more than 50 representatives from all the ECOWAS countries visited Ghana to learn from Ghana's experiences.

The Council of Europe has also chosen Ghana as the hub for cybercrime capacity building in the African region, which has given Ghana the opportunity to provide expertise to facilitate capacity-building programmes in cybercrime and electronic evidence handling abroad. This opportunity came about due to the development of home-grown expertise across the criminal justice sector. The World Economic Forum has approached Ghana to implement a private-public partnership for cybersecurity development in view of the Government's recognition to work closely with the private sector to improve the country's cybersecurity situation.

He stressed that with the passage of the Cybersecurity Act, Ghana has further demonstrated a forward-thinking leadership on cybersecurity matters, as Ghana is now Africa's first to respond to cybersecurity challenges through a formal legal framework. Thus, Ghana's latest ranking on the ITU's Global Cybersecurity Index, 86.69% and placing 3rd on the continent, is not only about structured processes in place as a country, but the appropriateness and the efficacy of what has been instituted. It is a story that looks into the future and evidently, Ghana's modest achievements are currently inspiring the rest of the continent.

He commended the visionary leadership of H.E. Nana Addo Dankwa Akufo-Addo and his personal commitment to Ghana's cybersecurity development. He also expressed appreciation to the Vice President of the Republic, H.E Alhaji Dr. Mahamudu Bawumia, who participated in the 2018 edition of NCSAM and launched the A Safer Digital Ghana campaign, Ghana's national cybersecurity awareness programme.

Dr. Antwi-Boasiako further hailed Hon. Mrs. Ursula Owusu-Ekuful, the Minister for Communications and Digitalisation for her unwavering determination and commitment to place cybersecurity where it belongs. Adding that, "It is impressive how she has framed cybersecurity issues not only as a national security issue but also as a developmental issue. She has done this through a bipartisan approach, and commended her for bringing all parties on board, on this developmental journey. Adding that history will certainly be kind to the Hon. Minister for carrying the vision of the President through to its fruition even as stakeholders were gathered to outdoor the Cyber Security Authority (CSA)".

The Ag. Director-General couldn't end his presentation without acknowledging the 7th Parliament of the Republic of Ghana for the bipartisan consensus which led to the passage of the Cybersecurity Act, 2020 (Act 1038)."We will look for further guidance and support from the 8th Parliament as we focus on the implementation of the Act", he added.

He further acknowledged the role of international partners; the World Bank, World Economic Forum (WEF), Security Governance Initiative (SGI) of the US Embassy, Council of Europe (CoE) and UNICEF, among others.

Furthermore, Dr. Albert Antwi-Boasiako recognized the National Communications Authority (NCA) for rendering a helping hand to the Centre on a journey that had transitioned into the Cyber Security Authority (CSA) by offering the CSA a temporary office space on the third floor of its building. He said the CSA will continue to count on NCA for support in diverse ways including offering guidance, to fulfil the mandate of the Cyber Security Authority.

He acknowledged the NCSTWG, private sector players as well as civil society groups, and all other stakeholders, counting on their cooperation towards the implementation of Act 1038.

To the staff of the Cyber Security Authority, Dr. Antwi-Boasiako said, "certainly, the journey has been challenging but fulfilling at the same time. My appreciation to all of you for your extraordinary commitment not just to deliver, but to deliver to a standard, which has contributed to our modest contribution to the development of this country. As the Hon. Minister always says the journey has only begun!"

Dr. Maxwell Opoku-Afari

First Deputy Governor,
Bank of Ghana (BoG)

REMARKS

The First Deputy Governor of the Bank of Ghana, Dr. Maxwell Opoku-Afari, in his remarks commended the organisers of the programme for bringing together players in the cybersecurity space to share experiences on the issues.

He shared with participants the steps being taken at the Central Bank to protect the financial sector from cybersecurity threats and related activities.

According to Dr. Maxwell Opoku-Afari, the gradual evolution and change in the business models of firms and institutions and the speed with which the entire digitalisation agenda is progressing has forced industry players to re-think ways and means of protecting the infrastructure that supports this new way of life. He added that “analysts have predicted that the next financial shock or shock to the global economy could manifest itself in the form of a cyber-attack and this makes it imperative for us to begin to think of how to secure and protect our infrastructure”.

The Deputy Governor indicated that cyber attacks have emerged as a global threat to financial stability and way of life and that successful cyber attacks on computer systems and networks supporting critical national assets and infrastructure could cause significant havoc; financial loss, undermine public confidence, and major disruption to the economy. He therefore encouraged all major stakeholders to launch a national effort aimed at creating cyber security awareness to combat the rising threat posed by cyber-attacks and cyber-crimes.

He added that the COVID-19 pandemic, and issues emanating from it, have accelerated the adoption of digitalisation in Ghana and is gradually changing the face of the economy as people work remotely, bank online, purchase goods and services online, etc. He therefore urged that, as a country, we need to position ourselves in readiness for the threats that come along with the changing lifestyles and ways of doing business.

Current trends in cybersecurity, he said, point to significant increases in attacks against Critical Information Infrastructure and related organisations that are drivers of national economies; making it more important than ever for policymakers to internalise in their discourse, the fact that attacks will certainly happen and prepare accordingly.

Dr. Opoku-Afari further discussed regulatory regimes that are being followed to enhance cybersecurity awareness in the banking sector indicating that regulating and close monitoring of cyber activities in the banking sector has become an important critical role for the central bank. He noted that regulatory frameworks alone may not be enough to protect the nation’s critical information infrastructure and hence must be followed by actionable steps to lock in potential intentions.

National Response and Preparedness at the National level, the Government of Ghana recognises the threat cyber attacks and cybercrimes pose to critical information infrastructure as well as the damage it can cause to the trust and confidence in our financial system. As a result, the Government responded swiftly through regulatory measures such as the Data Protection Act, 2012 (Act 843) and the Cybersecurity Act, 2020 (Act 1038), as well as supporting directives and other related legislation to enforce provisions of the law across all sectors of the economy.

The Bank of Ghana, as far back as October 2018 took actionable steps to issue the Cyber and Information Security Directive in a bid to enhance and protect the security of this critical sector of our economy. Following the issuance of the Directive, the Bank of Ghana has introduced many initiatives to strengthen and secure the information security architecture of the banks, to ensure the systems at the banks are robust and resilient.

On the way forward, the first Deputy Governor of the Bank of Ghana said it is important for institutions to undertake cybersecurity-related due diligence and assessments, identify proper detective controls, and enforce third-party and insider risk programmes to protect and safeguard their working environments from cyber-related activities that are not conducive for growth. He added that the Central Bank will continue to draw strength from Act 1038, which is intended to further promote and improve collaborative efforts between the Cyber Security Authority and the Bank of Ghana. He further pledged that the Central Bank would work closely with the Cyber Security Authority to monitor trends of cybersecurity issues in the financial sector and ensure a collaborative response to cybersecurity incidents. The Bank of Ghana will also play an active role in the implementation of the Cybersecurity Act, 2020 through our representation on the Joint Cybersecurity Committee (JCC) pursuant to Section 13 of Act 1038 and will endeavour to provide all support available to ensure the smooth formulation of policies in this area.

REMARKS

Delivering remarks on behalf of the US Ambassador to Ghana, the Chargé D'Affaires, of the US Embassy, Madam Nicole Chulick, stated that the increased rate of global connectivity and its associated challenges necessitates cooperation and collaboration to work together to ensure a safe internet. She lauded Ghana's effort in cybersecurity development over the years and reflected that the country is on the right cybersecurity developmental path and not lagging from best practice as the United States only established its Cybersecurity Agency in 2018. She added that in recognition of the severity of cybercrimes and it being a challenge to law enforcers, the President of the United States, Mr. Joe Biden prioritises all strategies to ensure that the United States is cyber resilient. Given this, she indicated that the US is ready to strengthen its engagement and collaboration with Ghana on its new journey of establishing a Cyber Security Authority (CSA) to augment efforts in the fight against cybercrime and improving cybersecurity.

Nicole Chulick

**Charge D'affaires,
US Embassy in Ghana**

Hon. Matthew Opoku Prempeh

Minister for Energy

REMARKS

The Minister for Energy, Hon. Matthew Opoku Prempeh acknowledged the Ministry of Communications and Digitalisation's effort in protecting the country's critical infrastructure and deemed the event timely. He, however, indicated that Government has not paid enough attention to the new threats posing risks to every sector of the economy and not just the energy sector hence cybersecurity is imperative. Outlining the efforts made by the Ministry of Energy to build the technical capacity of its staff, the Hon. Opoku Prempeh indicated that the Ministry has provided ICT training to its staff for them to understand the enormity of the task. Energy is a basic issue for human consumption, and it is important for technology to revolutionise it to be more affordable, he enumerated.

He acknowledged that the dangers of attacks in the energy sector are real and increasing and cited a number of attacks that have impacted the energy sector globally. "In 2017, Ukraine suffered an attack on the energy sector, Colonial Pipeline, responsible for supplying gas along the East Coast in the United States on May 17, 2021 suffered a ransomware attack, while in July 2019, a power supplier in Johannesburg, South Africa suffered a ransomware attack leaving residents without power for several hours", he said. These ransomware attacks affected the sector due to computers underpinning activities. Given the impact cyber-attacks have on the critical information infrastructure (CII) of nations, the Ministry of Energy is committed to work closely with the Ministry of Communications and Digitalisation to ensure that the right policy measures are adopted for compliance for the effective implementation of Act 1038 which prioritises the protection of CIIs, he ended.

Hon. Ursula Owusu-Ekuful

Minister for Communications and Digitalisation (MOCD)

KEYNOTE ADDRESS

The Minister for Communications and Digitalisation, Hon. Ursula Owusu-Ekuful gracing the occasion delivered the keynote address and officially launched the National Cyber Security Awareness Month (NCSAM) 2021, the Directive for the Protection of Critical Information Infrastructure (CII), and the Cyber Security Authority (CSA).

Welcoming participants to the 2021 edition of the National Cyber Security Awareness Month, the Minister said the event is an important edition of the National Cyber Security Awareness Month regarding Ghana's cybersecurity journey and she was hopeful it will present many opportunities, despite the persisting COVID-19 pandemic.

According to the Minister, the theme: "Ghana's Cybersecurity Act 2020: Its Implications and the Role of Stakeholders" seeks to emphasise on Ghana's efforts in accomplishing an important milestone – the enactment and implementation of cybersecurity legislation among four other critical pillars of the nation's cybersecurity development, as recommended by the International Telecommunication Union (ITU).

The passage of the Cybersecurity Act, 2020, she said, is indeed a milestone achievement that puts Ghana on the right path to a safer and more resilient digital ecosystem.

She thus appreciated the 7th Parliament

of the Republic of Ghana and the Parliament Select Committee on Communications, for the stellar work done in passing the Act into law on November 06, 2020. The commitment and direction provided by the National Cyber Security Inter-Ministerial Advisory Council, the National Cyber Security Technical Working Group and the National Cyber Security Centre (NCSC) in the passage of the law is unparalleled.

She also specially recognised the Legislative Drafting Division of the Attorney-General's Department, for the hard work and commitment in drafting the provisions of the Act "indeed, their efforts have not gone unnoticed as the Cybersecurity Act, 2020 (Act 1038) has been considered as a world-class legislation at par with legislations of the United States, the United Kingdom, Singapore, Rwanda and other countries with robust cybersecurity legislations"- she indicated. Adding that,"Indeed, it is not surprising that, in the latest release of the Global Cybersecurity Index (GCI) of the ITU, Ghana was ranked the 3rd country in Africa and 43rd globally with a score of 86.69% on the assessment scale. This is a major improvement from the 32.6% score recorded in 2017 when the then Ministry of Communications was directed by Cabinet to oversee Ghana's cybersecurity development".

She further recognised the unflinching support provided by international partners including the Government of the United Kingdom, the United States Government, the World Bank, the Council of Europe and UNICEF Ghana among others including domestic stakeholders. Above all, she acknowledged the President, H.E. Nana Addo Dankwa Akufo-Addo's commitment to cybersecurity as an imperative to secure Ghana's digital economy. She emphasised that, all the achievements chalked in Ghana's cybersecurity development are indeed a testament to a strong political commitment by the Government of H.E. Nana Addo Dankwa Akufo-Addo to institutionalise and develop Ghana's cybersecurity.

According to Mrs Ursula Owusu-Ekuful, "a substantive Cybersecurity Act for Ghana is indeed a significant achievement at this stage of our cybersecurity development, and this, together with the revision of Ghana's National Cybersecurity Policy and Strategy, ratification to the Convention on Cybercrime (Budapest Convention) and the African Union Convention on Cyber Security and Personal Data (Malabo Convention), the launch of the A Safer Digital Ghana campaign by the Vice President, H.E. Dr. Alhaji Mahamudu Bawumia, the launch of the Cybercrime / Cybersecurity Incidents Reporting Points of Contact as well as capacity building for the public sector including training for the criminal justice sector are major interventions introduced by my Ministry through the National Cyber Security Centre during the first term this government". She saluted all the staff of the NCSC for the hard work which has brought the country this far on this important journey – a journey to secure Ghana's digital economy.

According to the Minister, per World Economic Forum's, Global Risks Report 2020, Cybercrime damages might reach US$6 trillion equivalent to the GDP of the world's third-largest economy. It is therefore noteworthy that Ghana has taken adequate steps towards safeguarding its cyber ecosystem.

She added that "today marks an important turning point in Ghana's cybersecurity development as I formally launch the Cyber Security Authority (CSA), an agency with a critical mandate to protect Ghana's Critical Information Infrastructure (CII) and to lead Ghana's cybersecurity development through regulations". She indicated that, the transitioning of the National Cyber Security Centre into the Cyber Security Authority is not only a transition by way of a change in name, but a formal outdooring of an institution with regulatory powers and with a clear mandate to protect– government, private sector and the public from cyber-attacks.

With cyber attacks against critical information infrastructure rated the fifth top risk in 2020 according to the World Economic Forum, she acknowledged the rising need to have structures and systems in place to safeguard Ghana's Critical Information Infrastructure as per Sections 35-40 of Act 1038. She informed the gathering that as Minister responsible for cybersecurity matters, she had designated 13 sectors, namely, National Security and Intelligence, Information and Communications Technology (ICT), Banking and Finance, Energy, Water, Transportation, Health, Emergency Services, Government, Food and Agriculture, Manufacturing, Mining and Education, as sectors of our economy. Following the official designation of these sectors, she has also issued legal notices to a total of 189 institutions across the 13 sectors informing them of their designation as Critical Information Infrastructure Owners.

The designation of CIIs is accompanied by the introduction of a Directive to protect the 189 designated CIIs pursuant to section 92 of Act 1038. The Directive is expected to guide the implementation of Sections 35-40 of the Cybersecurity Act, 2020. The Directive establishes baseline cybersecurity requirements for all designated CII Owners, procedures for incident response as well as requirements and procedures for audit and compliance enforcements by the Authority. Additionally, the Directive outlines technical and organisational measures to be adopted by designated CII owners in protecting the CII systems and networks.

As provided in Section 36 of the Act, all designated CII Owners are mandated to register with the Authority. She therefore urged all institutions – both public and private which have been designated to comply with the designation and registration requirements fully. Failure by a CII Owner to comply with the Directives of the Authority shall necessitate administrative penalties per section 92 (2) of the Act.

She beckoned that “as we embark on this new journey, we do not imply that Ghana is now immune to cyber-attacks. Indeed, we are more prone to cyber-attacks now as we expand the various digital channels and platforms – both in the public and the private sectors. In view of this, I am tasking the newly established Cyber Security Authority to work with relevant stakeholders including members of the Joint Cybersecurity Committee (JCC), private sector stakeholders, civil society groups as well as Ghana’s international partners to protect and secure our nation’s digital assets.

I am working through the Joint National Security Coordinating Committee of the National Security Council Secretariat and also through Cabinet to ensure the Authority has the needed technology, funding and a dedicated office to operate from”. She then commended the National Communications Authority (NCA) for its generosity in making available, the 3rd floor of the NCA Tower to host the Cyber Security Authority, pending the completion of a dedicated permanent office complex for the Authority which is currently under construction.

To conclude, the Minister for Communications and Digitalisation said, the Government as a cybersecurity enabler, will continue to make the necessary efforts including relevant budgetary allocations to support national cybersecurity development activities. She then declared the 2021 edition of the National Cyber Security Awareness Month (NCSAM), the Directive for the Protection of designated CIIs and the Cyber Security Authority (CSA) launched.

CLOSING REMARKS & VOTE OF THANKS

At the end of the event, the Chief Director of the Ministry of Communications and Digitalisation, Mrs. Magdalene Apenteng expressed the Ministry’s appreciation to the stakeholders for gracing the occasion while appreciating the numerous contribution, commitment and efforts of the country’s domestic and international partners towards Ghana’s cybersecurity development and requested their unflinching support and dedication to see the newly established Cyber Security Authority (CSA) achieve its mandate.

Mrs. Magdalene Apenteng

Chief Director, Ministry of Communication & Digitalisation

UNVEILING OF THE OFFICIAL LOGO OF THE CYBER SECURITY AUTHORITY (CSA) BY HON. URSULA OWUSU-EKUFUL MINISTER FOR COMMUNICATIONS & DIGITALISATION

The Minister for Communications and Digitalisation, Hon. Ursula Owusu-Ekuful assisted by the Minister for Energy, Hon. Matthew Opoku Prempeh, in the presence of other dignitaries, private sector stakeholders, industry players, Ghana diplomatic Corps, the media and all invited guests unveiled the official logo of the Cyber Security Authority on the 3rd floor of the NCA tower.

WORKSHOP ON THE CYBERSECURITY ACT, 2020 (ACT 1038)

and the Directive for the Protection of Critical Information Infrastructure (CII)

NATIONAL
CYBER SECURITY
AWARENESS MONTH

The Cyber Security Authority (CSA) organised a Workshop on the Cybersecurity Act, 2020 (Act 1038), and the Directive for the Protection of Critical Information Infrastructure for representatives of designated Critical Information Infrastructure (CII) Owners, as part of the 2021 edition of the annual National Cyber Security Awareness Month (NCSAM).

The purpose of the workshop was to create awareness and to build the capacity of the designated CII owners in the protection of Ghana's Critical Information Infrastructure on the baseline cybersecurity requirements to ensure the protection of critical assets and systems.

The workshop which lasted for about an hour was attended by representatives of the following: Defence Intelligence, Eaton Towers Ghana, Ecoband Networks, Kwame Nkrumah University of Science and Technology, University of Cape Coast, Economic and Organised Crime Office, Electoral Commission of Ghana, Ericsson Ghana, External Intelligence, Financial Intelligence Centre, Gaming Commission of Ghana, Ghana Armed Forces, Ghana Broadcasting Corporation, Ghana Dot Com Limited, Ghana Immigration Service, Ghana Passport Office, Ghana Prison Service, Ghana Revenue Authority, Ghanaian Academic and Research Network (GARNET), Huawei Technologies (Ghana) S.A Limited, Judicial Service of Ghana, Lands Commission, National Communications Authority, National Identification Authority, National Information Technology Agency, and officials of the Cyber Security Authority.

The Lead for Critical Information Infrastructure Protection (CIIP) at the CSA, Mr. Benjamin Ofori, welcomed the participants and took them through the various sections of the Cybersecurity Act, 2020 (Act 1038) indicating the roles and responsibility of the Cyber Security Authority and CII Owners. He explained the elements of section 35-40, the CII provisions in the Cybersecurity Act, 2020 (Act 1038), to the participants.

Mr. Benjamin Ofori assured the participants that the Cyber Security Authority (CSA) shall provide guidance and support to designated CII owners pursuant to the implementation of the Directive and the Cybersecurity Act, 2020.

He further informed them that soon, sector-specific Directives will be developed to accommodate the varying maturity levels and operations of the CII sectors. He added that the Directive for the Protection of CII launched on October 1, 2021, applies to all CII owners to ensure they meet the baseline cybersecurity requirements.

Session 1

BACKGROUND

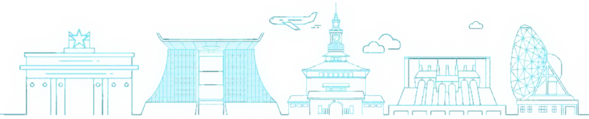
The purpose of the workshop was to promote capacity building and awareness creation on the roles of designated CII owners in the protection of Ghana's Critical Information Infrastructure, provide designated CII Owners with adequate understanding on the baseline cybersecurity requirements to ensure the protection of critical assets and systems.

The meeting was attended by representatives from the following institutions: Ghana Water Company Limited (GWCL), Ghana National Fire Service, National Ambulance Service (NAS), National Disaster Management Organisation (NADMO), Zenith Bank (Ghana) Limited, ARB Apex Bank, National Pensions Regulatory Authority (NPRA), GCB Bank Limited and officials of the Cyber Security Authority (CSA).

DISCUSSION POINTS

The meeting commenced with a welcome address read on behalf of Dr. Albert Antwi-Boasiako, the Ag. Director-General of the Cyber Security Authority by Mr. Benjamin Ofori, the CIIP Lead. Mr. Benjamin Ofori delivered a presentation on the Cybersecurity Act, 2020 (Act 1038). He highlighted the general outlook of Act 1038. He gave a detailed presentation on the CII provisions in sections 35 – 40 of the Cybersecurity Act, 2020 (Act 1038), indicating that section 35 of the Cybersecurity Act, 2020 (Act 1038) explains the designation of Critical Information Infrastructure (CII), focusing on the designation criteria used in the selection of Critical Information Infrastructure (CII).

Mr. Ofori stated that the gazette notice for the designation of CII sectors has been published with the Assembly Press after extensive consultative engagement with the Attorney General's Department. Adding that, the gazette notice for registration will be published on October, 7 2021 with the Assembly Press. Mr. Michael Appiah of ARB Apex Bank enquired about how registration of the CII will be conducted. Mr. Gerald Awadzi addressed Mr. Michael Appiah's concerns by stating that there will be further engagement with CII Owners to agree on the best procedures and strategies in registering CII owners.



Mr. Gregory Ojukwu of Zenith Bank enquired where the line is drawn in determining critical systems in an organisation. Mr. Awadzi stated that, only infrastructure that provide core services to citizens will be considered critical. Mr. Ofori took participants through the Directive for the Protection of Critical Information Infrastructure. He explained that the CII Directive operationalises the provisions of Sections 35-40 and section 92, adding that the CII Directive applies to all designated CII Owners, cybersecurity service providers for the purpose of ensuring cybersecurity in the country.

Mr. Michael Appiah stated that the Security Operations Centres (SOC) of most banks are connected to the Bank of Ghana's SOC and he wanted to make enquiries if all financial institutions will rely on the BoG SOC for incident reporting. Mr. Awadzi in response stated that the CSA will collaborate with the BoG and other regulators on the most effective way to regulate financial institutions and other institutions in Ghana when it comes to cybersecurity matters.

Mr. Gregory Ojukwu further sort clarification on how Audit and Compliance will be done by mentioning other standards and certifications banks are compliant with.

Additionally, he inquired what other audits will be required of financial institutions by the CSA and if existing internal audits will be applicable in this case. Mr. Benjamin Ofori answered that, the CSA will recognise and will rely on existing international standards and best practices that institutions are already compliant with for the start.

Madam Rashidatu Ibrahim of the Nation Pensions Regulatory Authority asked if there will be any financial support from the CSA for institutions that are below the baseline requirement since cyber security implementation is quite expensive.

Mr. Awadzi indicated that each organisation's cybersecurity posture will be examined and that will drive what support the CSA will offer but not in monetary terms.

Mr. Gregory Ojukwu asked for clarification on the Auditing and Compliance section which required CII Owners to seek clearance from the CSA within one month prior to any major organisational change in operation, personnel, and infrastructure. Mr. Awadzi highlighted that in that section, the CSA is focused on changes that directly affect core operations on the CII infrastructure and systems and the services provided by the critical infrastructure and system. Mr. John Mensah raised the issue of the source codes of critical systems in escrow as part of Technical and Organisational Measures in the Directive. He enquired how protected institutions will be upon compliance with the CII Directive. Mr. Benjamin Ofori replied stating that leveraging on escrow services ensures an organisation's continuity when developers providing these source code to client go bankrupt or are no more in operation and it is consistent with international best practices.

RECOMMENDATIONS / ACTION POINTS

It was agreed that the link to the workshop will be shared with participants to aid with their reporting processes.

Mr. Benjamin Ofori concluded the meeting (which lasted about an hour) by expressing his gratitude to all the participants for honouring the invitation and acknowledged all contributions from the participants.

Session 2

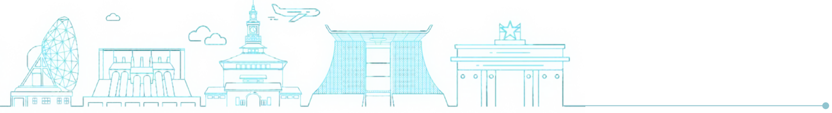
BACKGROUND

The meeting was attended by representatives of the following: Electricity Company of Ghana (ECG), Bui Power Authority (BPA), Karpowership Ghana Company Limited, SIC Life Company Limited (SIC Life), Bulk Oil Storage and Transportation Company Limited (BOST), National Petroleum Authority (NPA), Ghana Civil Aviation Authority (GCAA), Ghana Maritime Authority (GMA) and officials of the Cyber Security Authority (CSA).

DISCUSSION POINTS

The workshop commenced with a welcome address by Mr. Benjamin Ofori, the CIIP Lead. He gave an overview of the workshop, which was in two parts namely Cybersecurity Act, 2020 (Act 1038) and the Directive for the Protection of CII.

Mr. Benjamin Ofori highlighted the various sections in the Cybersecurity Act, 2020 (Act 1038) indicating the roles and responsibility of the Authority and CII owners. He further explained section 35-40 as the CII provisions in the Cybersecurity Act, 2020(Act 1038). Mr. Benjamin Ofori indicated that section 35 of the Cybersecurity Act, 2020 (Act 1038) explains the designation of Critical Information Infrastructure (CII), highlighting the designation criteria used in the selection of Critical Information Infrastructure (CII).



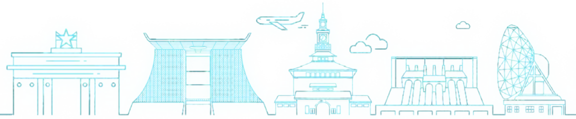
Mr. Gilbert Dordor of the Electricity Company of Ghana asked if the Cyber Security Authority will be conducting background checks on employees of CII owners to aid their Human Resource avoid employing people that could pose as threats to institutions. Madam Audrey Mireku of the Computer Emergency Response Team of the CSA answered the above, stating that what he is asking about is addressed in the CII Directive and has to be implemented at the institutional level. Mr. Benjamin Ofori further presented on the Directive for the Protection of CII which operationalises the provisions in section 35 – 40 and section 92 of the Cybersecurity Act 2020 (Act 1038), adding that the Directive applies to all designated CII Owners, cybersecurity providers or service providers for the purpose of ensuring cybersecurity in the country. Mr. Benjamin Ofori assured the participants that the Cyber Security Authority (CSA) shall provide guidance and support to designated CII owners pursuant to the implementation of this Directive and the Cybersecurity Act, 2020. The CSA has the overall oversight responsibility to ensure the implementation of the Directive. Mr. Benjamin Ofori highlighted the next steps after the implementation of the Directive which includes designation of CIIs, registration of CIIs, and engagement with CIIs.

Mr. Kwame Agyemang of SIC Life Company Limited asked for clarification on the registration process. Mr. Benjamin Ofori answered that once an institution has been designated as a Critical Information Infrastructure Owner, they'll be required to register their critical systems and services through a collaborative engagement with the Cyber Security Authority. Mr. Michael Osei of Karpowership Ghana Company Limited asked that once an institution has been designated as a Critical Information Infrastructure, does the institution have to ensure they are registered under the Data Protection Commission even though they've been designated. Mr. Gerald Awadzi answered by highlighting that, the Directive for the Protection of CII, requires that every CII Owner develops a cybersecurity policy which should address Data Protection concerns of the designated CII Owner consistent with the Data Protection Act, 2012. Hence it is essential that the institution is registered under the Data Protection Commission.

RECOMMENDATIONS/ ACTION POINTS

It was agreed that the link to the workshop will be shared with participants to aid with their reporting processes.

Mr. Awadzi concluded the meeting (which lasted for about an hour) by expressing his gratitude to all the participants for honouring the invitation and acknowledged all contributions from participants of the workshop.



WORKSHOP ON LAW ENFORCEMENT AGENCY TRAINING STRATEGIES

The growth in the use and development of information and communications technologies go hand in hand with the rise of crimes committed against or through the use of computer systems. The Council of Europe's approach to protect societies worldwide in the cyberspace is based on the development and implementation of the Budapest Convention on Cybercrime, through a dedicated programme of capacity building for criminal justice authorities.

In this line, Law Enforcement Agencies need to develop strategies on cybercrime and electronic evidence to ensure that investigators acquire and maintain sufficient knowledge to fulfil their roles effectively. The Council of Europe (CoE) has therefore developed an approach for Law Enforcement Agencies aimed to empower countries to develop practical strategies in responding to cybercrime.

As part of the programme of activities for the National Cyber Security Awareness Month 2021, the CoE in collaboration with the Cyber Security Authority (CSA), organised a virtual workshop to discuss and deliberate on issues regarding Law Enforcement Agency Training Strategies.

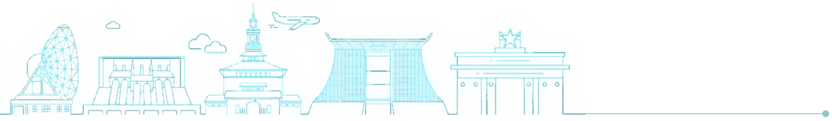
The workshop was attended by the judicial authorities including justices of the High Court, District Court and Circuit Court, prosecutors from the Ghana Police Service, officers from the Criminal Investigations Department (CID) and officers from Law Enforcement Agencies including the Bureau for National Investigations (BNI) and the Economic and Organised Crime Office (EOCO) as well as officers from the Cyber Security Authority.

The facilitator greeted all and explained that prosecutors and Law Enforcement Agencies must have effective tools to prosecute. He explained the training was aimed at enhancing the capacities of the judiciary and Law Enforcement Agencies to actively tackle issues of cybercrime. He spoke on the ongoing collaboration with the CSA on strengthening capacities of the Ghanaian judiciary and Law Enforcement Agencies based on the Budapest Convention. He noted that Ghana collaborates with numerous states to uphold human rights and provisions in the Budapest Convention. He noted that Ghana's efforts in cybersecurity have made it a hub for cybersecurity capacity building among Anglophone countries in West Africa. He wished participants fruitful deliberations and encouraged them to share the knowledge learnt with fellow colleagues.

The representative from the CID gave participants an overview of the training and spoke on the role of the cybercrime unit of the Ghana Police CID. He also spoke extensively on the need for capacity building especially for Law Enforcement Agencies and the Judiciary.

Mr. Zahid Jamil from the Council of Europe gave an overview of global statistics relating to social media usage. He also spoke about the importance of international cooperation in the resolution of cybercrime. He stated that business e-mail compromise and ransomware form part of the top threats that multi-national corporations are exposed to. Mr. Jamil explained cybercrime as the nexus between technology, crime, a victim, a witness, an aid, a communication tool, and a storage medium.

He spoke on the three dimensions of the Budapest Convention, stating that the Convention serves as a standard, provides procedures for follow up and assessment and also serves capacity building purposes. Mr. Jamil also gave a brief history on the Budapest Convention. He also spoke on the various cybersecurity programmes being implemented by the Council of Europe.



Participants were taken through fundamentals of a cybercrime treaty, functions and benefits of a cybercrime treaty. In his conclusion, Mr. Jamil debunked some widespread rumours about the Budapest Convention.

After a short break, the Ag. Director-General, Dr. Albert Antwi-Boasiako gave some brief remarks encouraging participants to actively engage in the workshop. He also educated participants on the various achievements of the Centre now Authority including the launch of the A Safer Digital Ghana Campaign by H.E. Dr. Alhaji Mahamudu Bawumia.

Before the day's session ended, Madam Catalina Stroe from the Council of Europe introduced participants to some of the substantive laws in the Budapest Convention.

She expanded on provisions covering international cooperation under the Budapest Convention and also explained provision on mutual legal assistance.

Participants were taken through a session on electronic evidence handling and introduced to computer forensics.

The day's session ended with Mr. Zahid Jamil presenting elaborately on sextortion and various elements that constitute the offense.

CLOSING REMARKS

Madam Catalina Stroe

Madam Catalina Stroe congratulated participants for actively engaging in the workshop. She further encouraged participants to conduct research to learn more about cybercrime and cybersecurity in order to aid them in the execution of their duties as Law Enforcement officers.

WORKSHOP ON THE INTEGRATION OF EUROPEAN CYBERCRIME TRAINING & EDUCATION GROUP TRAINING MATERIALS

The Council of Europe, through the GLACY+ Project organised a workshop on the integration of European cybercrime training and education group training materials on October 6, 2021 as part of training strategies for priority countries in investigating cybercrime and managing digital evidence.

The participants included officials of the Criminal Investigations Department (CID) of the Ghana Police Service, Ghana Police Academy, National Intelligence Bureau (NIB), Kofi Annan International Peacekeeping and Training Centre (KAIPTC), Economic and Organised Crime Office (EOCO) and National Signals Bureau (NSB). There were also representatives and two experts from International Criminal Police Organisation (INTERPOL) who facilitated the workshop.

The Director of Operations, of the Cyber Security Authority (CSA), Mr. Owusu Bediako-Poku welcomed the facilitators and participants on behalf of Ag. Director-General of the CSA, Dr. Albert Antwi-Boasiako.

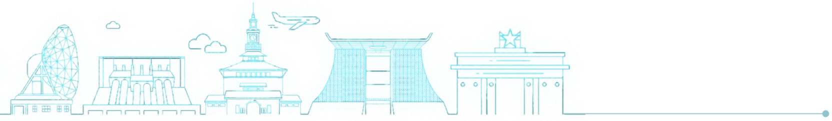
He indicated that the Cyber Security Authority is keen on ensuring law enforcement agencies continuously engage and develop their skills and knowledge base in the area of cybersecurity. He noted that criminals are increasingly replacing guns with sophisticated computer-assisted weapons. Recent acts of electronic crime in the US, such as the $15 million white-collar case called "Operation Derailed" in Atlanta, Georgia, highlight the need for increased law enforcement vigilance. The exponential growth of various kinds of digital evidence that law enforcement agencies must gather and maintain, such as reports, images, videos, and other electronic records, is one of the most pressing concerns facing all law enforcement agencies. Mr. Bediako-Poku expressed the commitment of the CSA to the coordination of cyber related training programs for the law enforcement agencies in the country to help to eradicate cybercrime to its barest minimum.

Mr. Baba Faisal of the Police Academy, gave a brief overview of the national training programme, where he spoke about the current status and approach at the academy for training senior police officers.

Mr. Christian Koranteng of National Intelligence Bureau (NIB), speaking on how they deal with cyber incidents, indicated that the NIB manages and receives calls from people who have been victims of cybercrime, and with the help of their available resources and tools, they have been able to track some cyber criminals who have been successfully prosecuted.

Mr. Stephen Ekow Yeboah of the Kofi Annan International Peacekeeping and Training Centre (KAIPTC) indicated that KAIPTC trains security professionals and personnel, mainly the police, the army and civilians on peace operation courses.

Dr. Gustav Yankson of the Ghana Police, Criminal Investigations Department (CID) was asked whether the National Cybersecurity Policy and Strategy was in use, referring to the 2016/2017 Policy and Strategy, and if there was a lower-level plan to deal with capacity building of cyber investigations and enforcements to improve prosecution of cybercrimes. Dr. Yankson noted that there is no policy or specified curriculum for law enforcement. He however noted that some work has been done in the areas of awareness and issues on child online protection. He indicated that some programmes and trainings have been adopted, including training of judges and investigators and other intelligence agencies. He further noted that the priority focus is on getting the structures in place and having more trainings. More specifically, he noted that within the Ghana Police Service,



some development has taken place in the area of capacity building and there are still ongoing developments to be able to capture all police officers-

(i) category for all police officers to help with issues since they are the first respondents

(ii) category for investigators; senior officers

(iii) category for cybercrime unit

(iv) category for management so they can properly understand and develop policies which will help improve policy development on this particular curriculum.

The workshop sought to create Ghana's desired cybercrime strategy through collaborative engagements among participants and trainers. The overall session sought to identify the facilities/infrastructures, curriculum, trainings, and cross-boundary engagements. Ghana currently has and if any, the strategies that have been adopted by the various bodies in dealing with cybersecurity. This included the areas of police, judiciary, and prosecutors. The pointers noted were reviewed and desired goals also noted before the session was rounded up. Also it was noted during the session that Ghana was involved in the development of the 2021 ECOWAS Regional Cybersecurity and Cybercrime Strategy and the Regional Critical Information Infrastructure Policy which was adopted in 2021.

FORUM ON THE CYBERSECURITY ACT, 2020 (ACT 1038)

for Cybersecurity Service Providers and Professionals

NATIONAL
CYBER SECURITY
AWARENESS MONTH

OPENING REMARKS

Dr. Albert Antwi-Boasiako
Ag. Director-General,
Cyber Security Authority (CSA)

He begun by indicating that whilst Ghana's Cybersecurity Act, 2020 (Act 1038) is not perfect, it remains one of Africa's best legislations. He quoted section 81 of Act 1038, which establishes an Industry Forum that allows for cybersecurity service providers to be active within the ecosystem.

He elaborated that the forum was meant to solicit ideas and discussions which were meant to help implement the Act in areas such as incident reporting and collaboration with relevant stakeholders. He concluded that with the right support, the CSA and industry would collectively implement the Act successfully.

KEYNOTE ADDRESS

Hon. Ursula Owusu-Ekuful
Mnister for Communications and Digitalisation

The Honourable Minister in her keynote address thanked the cybersecurity service providers for taking active steps over the years, in collaborating with Government to secure the cyberspace, noting that Ghana was fortunate to have escaped major cyber attacks so far due to this combined effort.

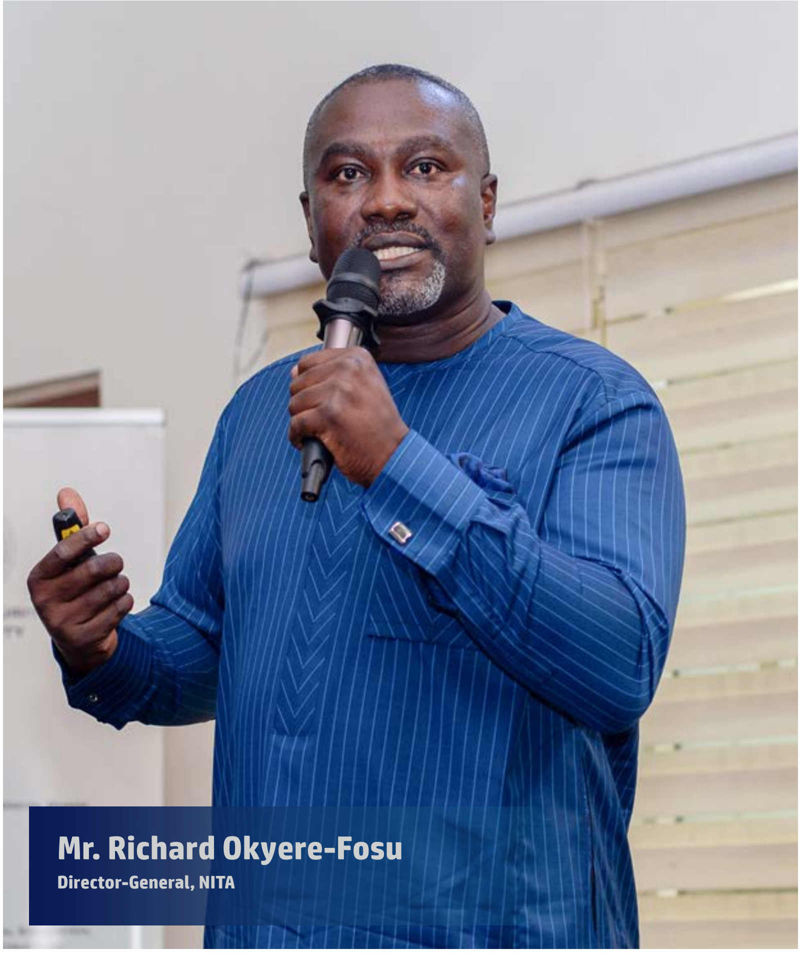
She stated that with the passage of the Cybersecurity Act, it was prudent for service providers to understand their roles and how the Act impacts on their respective organisations and their activities. She referenced section 49 of the Act which introduces the mandatory licensing of the service providers, therefore, allowing for the proper recognition of service providers within the industry.

“Cybersecurity is a sector where no one sector can act in a silo and hence there is a need for corporation between public and private sectors. The Law mandates the Authority to certify professionals, products, and services.” She stated that there was a huge skill gap which provides an enormous opportunity for young people in the country.

Mrs. Owusu-Ekuful further stated that, per section 81 of the Act, an Industry Forum which is a platform that will periodically bring the industry together to discuss matters of common interest to the industry will be established.

PRESENTATION

SAFEGUARDING THE GAINS OF DIGITALISATION IN GHANA – THE NATIONAL INFORMATION TECHNOLOGY AGENCY'S (NITA) ROLE AS THE ICT REGULATOR



Mr. Richard Okyere-Fosu

Director-General, NITA

The Director-General of the National Information Technology Agency (NITA), Mr. Richard Okyere-Fosu in his presentation on the above topic, acknowledged the progress made so far by other regulators in the Information and Technology space. He displayed a maturity assessment of NITA's current progress, touching on the institution's shortfalls and the gaps that needed overcoming to achieve the desired levels of service delivery. He also noted several key partnerships with other institutions and regulators which will lead to achieving NITA's targets.

PRESENTATION

OVERVIEW OF THE NEW CYBERSECURITY ACT, 2020 (ACT 1038)

Mr. Owusu Bediako-Poku

Cyber Security Authority

Mr. Owusu Bediako-Poku gave a background perspective to how the Act came about and outlined the need for a central Cybersecurity Act that encompasses all other cybersecurity-related legislations. He noted that, Statistics from Hootsuite - We are Social, an online social media dashboard, states that in 2020 Ghana was ranked 9th in social media usage worldwide.

He noted that this was a strong indication of the importance of cyberspace to Ghanaian so it needed regulations to secure it. He outlined the various sections of the Cybersecurity Act, 2020 highlighting the areas of interest for the day; sections 49-61.

PANEL DISCUSSION

Mr. Owusu Bediako-Poku introduced the Moderator for the panel discussion, Mr. Albert Yirenchi from Stanbic Bank. Mr. Yirenchi introduced his fellow panelists. Panel members included:

- → Mr. Nana Arezie Oduro-Asare, **EY Ghana**,
- → Mr. Daniel Gyampo, President of **ISACA Accra**,
- → Mr. C. K. Bruce, CEO of **Innovare** and
- → Mr. Eric Mensah, Head Technical Operations, **e-Crime Bureau**.

In response to a question by the moderator, the panelists outlined the various services they rendered. The moderator in a follow-up question, asked Mr. C.K Bruce, to outline how the Act would affect his institution's survival and clientele. Mr. C.K Bruce answered that it was in everyone's interest to promote regulation of the cybersecurity industry as that would accelerate growth and maturity of the entire sector. The moderator asked Mr. Eric Mensah if there was the possibility of backdoors in systems in Ghana. Mr. Mensah replied that there were skills in Ghana that can be exploited to avoid the issue of using systems that may have backdoors in them, emphasising that local solutions were the way to go. In support of Mr. Mensah's submission, Mr. Oduro also said that the industry could help the Authority to develop standards that makes sure the right developments were done.

Mr. Bruce in his response explained that certifications must have a code of ethics which binds professional careers, services, products, and institutions to spur growth and development within the industry. The moderator made an appeal to the Minister for Communications and Digitalisation to ensure that government sectors were also mandated to follow the law. The minister in response assured the panel that the Cybersecurity Act, 2020 would not be toothless and have the effect it was intended to have to sanitise Ghana's digital space.

Q&A

There were questions from the audience. One asked for

Q "the role of the Ghana Standards Authority in terms of cybersecurity regulation."

A The Ag. Director-General of the CSA, Dr. Antwi-Boasiako said "section 61(d) of the Cybersecurity Act 2020, mandates the CSA to collaborate with all other relevant institutions in ensuring that the right standards were enforced in relation to cybersecurity. This collaboration will provide skilled support to the Ghana Standards Authority in its regulatory role whenever cybersecurity was concerned.

An audience member urged the industry to think through how the standards would be effective in terms of the implementation across all niches of the cybersecurity sector".

MESSAGE FROM SPONSORS

Huawei Technologies (Ghana) S.A. Limited

Huawei Technologies (Ghana) S.A. Limited in their sponsorship message said that we should not trust anyone on the internet and that Huawei Technologies (Ghana) S.A. Limited was putting in necessary standards and best practices to implement their zero-trust approach to secure and manage cybersecurity and privacy.

Ernst and Young (EY)

Mr. Nana Arezie Oduro-Asare in his message stated that compliance was not security, so it should be embedded in the strategy (cybersecurity, technology, and business) and design process. He urged the audience to the know the regulations and standards that apply to their organisation. He urged all service providers to use the EY security transformation program, and compliance as a service program.

MINISTRY OF COMMUNICATIONS & DIGITALISATION
NATIONAL CYBER SECURITY AWARENESS MONTH 2021
FORUM ON THE CYBERSECURITY ACT, 2020
FOR CYBERSECURITY SERVICE PROVIDERS
& PROFESSIONALS

e-Crime Bureau

In a video footage, e-Crime Bureau outlined its mission to become a market leader in digital forensics and investigations in Africa. An e-Crime Bureau officer stated in the footage that e-Crime Bureau had collaborated with the Ghana Police Service and some other relevant institutions to develop online child protection solutions.

Innovare

In a video footage, Mr. Albert Turkson stated that Innovare is a trusted brand for training in cybersecurity, IT audit, IT Risk, and project management in Ghana.

Edward Mensah Wood and Associates

A representative from Edward Mensah Wood and Associates stated that institutions could be attacked in many ways. He asked if the industry players were adequately covered in terms of insurance. There was a huge gap in cyber risk insurance due to the many ways we could be attacked. He introduced Edward Mensah Wood and Associates insurance stating that their covers were free.

SUBMISSION FROM CYBERSECURITY PROFESSIONAL BODIES

Benjamin Cobblah, ISACA Accra.

ISACA representative, Mr. Benjamin Cobblah, mentioned ISACA's reach in other countries and advertised ISACA's range of IT governance and risk products and services.

Mr. Stephen Cudjoe-Seshie, ISC^2.

The ISC^2 representative, Mr. Stephen Cudjoe-Seshie mentioned the identification of credible partners as part of the process of certification and accreditation. He outlined there were tools and products that have been designed for various demographics in Ghana to cater for their cybersecurity training and development needs.

Mr. Sherrif Issah, IIPGH.

Mr. Sherrif Issah, mentioned that he has a very close collaboration with academia to train students in the universities and other projects. He stated that their efforts encompass all members of the society and they even recently trained kids through the "coding for kids" program. He afterward outlined various positives that came from the mentioned awareness training program.

SUBMISSION FROM PARTICIPANTS

→ A gentleman asked for the order in which licensing within the industry would be done

→ Another participant asked what would be done to make sure that accredited institutions remain accredited despite loss of employees

→ A representative of Institute of ICT Professionals in Ghana (IIPGH) asked if there would be a special accreditation from the Authority. Dr. Antwi-Boasiako stated that the establishment of Ghanaian-based processes to handle licensing and accreditation would be done.

→ An audience member asked if the authority would use political affiliation with regards to recruitment. Dr. Antwi-Boasiako stated that the Authority recruits from two broad categories. The Authority recruits a combination of officers that have a wealth of experience and officers that are young and willing to learn as a way of filling the skills gap.

→ Mr. Bright Ohene from GCB Bank Limited asked how soon the Authority would come up with a licensing list. Dr. Antwi-Boasiako stated standards would be rolled out very soon to drive growth, indicating that engagements with the industry would be key to some of the essential processes that would drive growth within the industry.

GLOBAL INTERNET FORUM TO COUNTER TERRORISM (GIFCT), TECH AGAINST TERRORISM (TAT) AND CYBER SECURITY AUTHORITY (CSA) MULTI- STAKEHOLDER WORKSHOP

This workshop was part of a global series of knowledge-sharing with technology companies relevant security related policy makers, law enforcement, experts on counter-terrorism and counter-extremism and NGO/CSO practitioners on preventing violent extremism (PVE) and countering violent extremism (CVE) globally. The meeting was held under the Chatham House Rule.

OPENING & WELCOME REMARKS

Dr. Albert Antwi- Boasiako

Acting Director-General, CSA

The Acting Director-General of the Cyber Security Authority (CSA), Dr. Albert Antwi-Boasiako in his welcome address to open the session, indicated that it is important to engage in an inclusive dialogue among relevant stakeholders on matters that boarder on national security and safety. He also noted that it is of high importance particularly in cyber related discussions to create opportunities for better and informed evidence-based policies and regulations. He emphasised that the workshop was a step to further enhance collaborative effort with international partners as the CSA seeks to meet its goals. Dr. Albert Antwi-Boasiako noted that the increased use of ICT, the internet and social media has added other dimensions to extremist and terrorist related activities and as such extensive discussions must be held to provide solutions to counter terrorism and violent extremism related activities and this cannot be done without the help of the tech community. Hence, the work of the Global Internet Forum to Counter Terrorism (GIFCT) is very relevant.

Dr. Albert Antwi-Boasiako stated that Ghana's Cyber Security Policy and Strategy reaffirms this perspective and highlights the concerns of both domestic and global peace and security. He stated that a report by the United Nations Office on Drugs titled "The use of the Internet for terrorism purposes" highlighted a few ways in which violent extremists and terrorists use digital infrastructure to facilitate their agenda. He stated that whiles terrorists have devised several ways to utilise the internet for illegal purposes, the use of the internet also allows for the collection of intelligence and other actions to prevent and counter terrorism and to gather evidence for prosecutions of such acts. Dr. Albert Antwi-Boasiako showed his excitement that Ghana has been chosen as the country to implement the vision of GIFCT. He again noted that he serves on the Independent Advisory Committee of the GIFCT on behalf of the Government of Ghana and raised concern for GIFCT to include more African countries. He assured participants of the Government of Ghana's commitment to work with GIFCT, individual technology service providers, other governments on the continent and worldwide to ensure that the issue of violent extremism and terrorism is dealt with while respecting the rights of citizens to use digital infrastructure as access to digital platforms and the internet has become a human right.

INTRODUCTION OF GLOBAL INTERNET FORUM TO COUNTER TERRORISM (GIFCT)

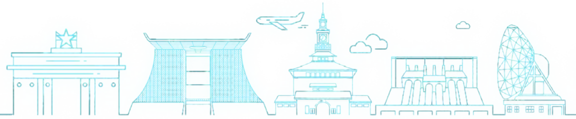
The representative from the Global

Internet Forum to Counter Terrorism gave an overview of the work that the GIFCT does.She stated that GIFCT is a unique entity because they were founded originally by technology companies for technology companies in 2017 and its goal as a Non-Governmental Organisation is to prevent terrorists and violent extremists from exploiting digital platforms. She said GIFCT identifies four core areas of work regarding how technological solutions can be shared, action-oriented research, multi-sector knowledge sharing and how to respond in a real-world crisis with online requests. In 2017, GIFCT set up a hash-sharing database of “hashes” or digital “fingerprints” to stop bad pieces of content from spreading. The NGO also works with tech companies and organises mentorship sessions in partnership with Tech Against Terrorism (TaT). The GIFCT representative further stated that in April 2019 an Incident Response Framework was created in response to the Christchurch Call to Action and noted that when a terrorist incident happens offline and has an online element, GIFCT provides and coordinates for members situational awareness, information sharing, hash sharing, and communications and stakeholder engagement. She stated that the Global Network on Extremism and Technology is an academic global network the GIFCT funds, and it brings the voices of academics around the world to contribute and fund them to write small insights about technological shifts that are being seen. Monthly e-learning sessions and webinars are organised and it was noted that an upcoming webinar on October 28, 2021 will focus on financial systems, fintech and terrorist finance and what these trends are starting to look like.

PRESENTATION
STATE OF PLAY-EXPERT RESEARCHERS AND GOVERNMENT THREAT ASSESSMENT

→ The first panelist as the representative of the Institute of Security Studies gave an overview of the threat landscape of violent extremism and terrorism in West Africa. He noted that in the context of West Africa, violent extremism is no longer confined to the northern part of the region, which is the Sahel, and to some extent the Chad Basin. He noted that there is currently not only a rapid spread of violent extremism in these regions, but also there is a downward move towards the West African coast specifically towards Ghana, Benin, Togo and more especially Cote D’Ivoire. This spread of violent extremism has generated many concerns among governments of these coastal states and their partners about what is an apparent spill over from the Sahel and the Lake Chad Basin into the coast and the recent attacks in the northern part of Cote D’Ivoire has reinforced these concerns. The representative of the Institute of Security Studies stated that the Coastal states have responded to these apparent spills by carrying out military operations along their boarders. Ghana is currently conducting “Operation Conquered Fist” in its five northern regions with the aim of preventing violent extremism groups from staging attacks on Ghanaian territory. In recent times, there was a joint operation between Cote D’Ivoire and Burkina Faso in the northern part of Cote D’Ivoire. Based on the research done by the Institute of Security Studies, the spill over of violent extremism is not just about attacks but also the underground dealings of violent extremist groups in terms of their ability to generate human resources, financial resources, or operational resources needed to be able to carry out attacks. The research that has been done points to the existence of some sort of a supply chain of resources involving Ghana and neighbouring coastal states. In Ghana there are cases of some Ghanaian nationals who have left Ghana to join the fight in the Sahel and in North Africa. This suggests that there is some recruitment going on in Ghana and some coastal states, however there is not much information as to who is behind these recruitments and how they are being organised and as such more research needs to be conducted in this regard. Again, some parts of Ghana and some parts of other coastal states are serving as hide outs and places for rest for violent extremist groups and this is confirmed by occasional complaints by Burkina Faso officials. He also noted that there are cases of stolen livestock from the Sahel being sold in Ghana, Togo, Cote D’Ivoire and the profits being ploughed back into buying weapons, fuel and food. In conclusion, the Institute of Security Studies’ representative made some propositions, which he stated that there is the need for coastal states and their partners to have a broader understanding of what a spillover of violent extremism or terrorism entails and as such work to tackle the various dimensions they entail.

→ The second panelist from the Cyber Security Authority (CSA), Mr. Isaac Socrates Mensah in his presentation noted that Ghana’s framework for preventing and countering violent extremism and terrorism is based on four main pillars, which is to prevent, protect, pre-empt, and respond. He stated that the Prevention



pillar is concerned with ways to prevent the recruitment and mobilisation of terrorist activities and further explained that the Pre-emption pillar deals with enhancing sustainable capability of security services to identify risks and uncover threats for rapid response to these emerging threats, whereas the Protection Pillar is concerned with the protection of vulnerable areas specifically the border areas of the country to prevent spill overs in terms of violent extremism. Finally, he explained that the Response Pillar refers to the building of various mechanisms to respond to the challenges the country may face. The Authority's representative gave an overview of the legislations and treaties that the country has in place to address violent extremism and terrorism in Ghana. He made mention of the Cybersecurity Act, 2020 (Act 1038), the Electronic Transactions Act, 2008, (Act 772), the Electronic Communications Act, 2008 (Act 775), Data Protection Act, 2012 (Act 843), Budapest Convention, Malabo Convention, Anti-Terrorism Act, 2008 (Act 762) and others. In terms of response, he noted that CSA is committed to the building of a Computer Emergency Response Team Ecosystem. He noted that a National CERT has been established as well as the National Communications Authority (NCA) CERT, the Bank of Ghana Security Operations Centre (financial sector CERT) and the National Information Technology Agency Security Operations Centre (NITA-SOC) government sector CERT. Also in the works is health sector CERT.

→ The third panelist from Tech Against Terrorism (TaT), stated that TaT is a public-private partnership based in London focused on knowledge-sharing and providing support to tech platforms. He noted that the threat landscape involves the use of variety of interlocking technologies by terrorists to share content and plan operations. He further noted that this threat landscape can be categorised into three areas; Strategic purposes which entails content- sharing, social media, video streaming and gaming, Operational purposes involves VPN, encrypted messaging, hostile OSINT and financial tech and payments crowdfunding. He noted that terrorists are exploiting emerging technologies such as decentralised file servers, decentralised messaging platforms. A key trend he noted was the migration of terrorists to a growing number of niche online platforms that lack the capability or willingness to remove content. He stated that there is migration from lower concentration of terrorist actors, higher sophistication of COMO avoidance to a higher concentration of terrorist actors and lower sophistication of COMO avoidance. He introduced a case study on the Islamic State West Africa (ISWA), which refers to separate groups in the Lake Chad region and the Sahel respectively. He noted that almost all official ISWA content is produced by official IS media outlets and the primary platforms exploited include Telegram, Rocketchat, Hoop Messenger, terrorist-operated websites, and archiving services. He also expanded on the Terrorist Content Analytics Platform (TCAP) which seeks to track, verify, classify, alert and archive terrorist content across the internet. He noted that the 1st phase of TCAP is now complete with live content alerts to smaller platforms. The next focus of TaT is on three workstreams which are Expanding TCAP alerts: supporting smaller platforms in identifying content and helping them with content moderation; classifying, archiving and transparent hashtag of terrorist content: supporting smaller platforms by providing content taxonomy and metadata to allow more granular content moderation decisions and Content Moderation Workflow Tool: supporting smaller tech companies by developing a tool that provides context to allow swift and informed decisions at scale.

→ The final panelist from Facebook in her presentation noted that due to the nature of the products and services that Facebook offers, the basis of the work they do is dependent on how the users feel on the Facebook platform and the trust and security that they can provide to their users. She gave an overview of the community standards Facebook has and noted that Facebook's community standards have 4 pillars which are Violence and Criminal Behaviour, Safety, Integrity and Authenticity, and Objectionable Content. She also stated that the values, which form the basis for the community standards, are voice, privacy, safety, authenticity, and dignity. She emphasised that Facebook seeks to create a place for freedom of expression and give people a voice whiles protecting personal privacy and information and to ensure that expression that has the potential to intimidate, exclude or silence others is not permitted on the platform. Again, Facebook seeks to ensure that people are more accountable for their statements and actions.

In conclusion, the moderator noted that the Global Internet Forum to Counter Terrorism is looking forward to holding an in-person workshop in Ghana in 2022 and as such, the partnership with Ghana will not end any time soon.

IMPACT OF THE NEW CYBERSECURITY ACT, 2020 (ACT 1038) ON COMPUTER EMERGENCY RESPONSE TEAM (CERT) OPERATIONS

BACKGROUND

As part of measures to effectively implement Ghana's Cybersecurity Act, 2020 (Act 1038), the Cyber Security Authority (CSA) organised a Workshop on the Impact of the New Cybersecurity Act, 2020 (Act 1038) on the operations of Computer Emergency Response Teams (CERT). The event was an opportunity to engage cybersecurity service providers and professionals in the industry to deliberate and explore ideas for the effective implementation of the Act.

The meeting was attended by representatives from industry players and institutions like Defence Intelligence, Data Protection Commission, National Intelligence Bureau, Ghanaian Academic and Research Network (GARNET), National Communications Authority, Bank Of Ghana, National Signals Bureau, National Information Technology Agency, Ghana Health Service, and so on.

OPENING REMARKS

Mr. Owusu Bediako-Poku
Director of Operations, CSA

Mr. Owusu Bediako-Poku acknowledged the National Computer Emergency Response Team on the extraordinary effort and collaborations with other Sectoral CERTs to respond to cybersecurity incidents.

Mr. Owusu Bediako-Poku further presented a breakdown of the statistics of incidents received by the National CERT and the collaboration and support received from both local and international partners in resolving incidents.

PRESENTATION CYBERSECURITY ACT, 2020 (ACT 1038)

Mr. Alexander Oppong
Capacity Building and Awareness Creation Lead, CSA

Mr. Alexander Oppong introduced the various digitalisation initiatives by the government and the private sector. He indicated the overall contribution of the telecommunication sector to the GDP of the country and explained the statistics and trends of Ghana's digitalisation journey. The statistics depicted that, in 2020 Ghana was the 10th country with the highest use of social media globally. He further indicated the impact of cybercrimes globally and hence the need for effective collaboration in Ghana's cybersecurity journey. Mr. Oppong's presentation touched on Ghana's cybersecurity landscape, Ghana's Cybersecurity Policy and Strategy and reference point of the Cybersecurity Act, 2020 (Act 1038). He acknowledged the involvement of international and local partnerships in the passage of the Cybersecurity Act, 2020 (Act 1038).

PRESENTATION CYBERSECURITY ACT, 2020 (ACT 1038)

Mrs. Audrey Mnisi Mireku,
CERT Lead, CSA

Mrs. Audrey Mnisi Mireku outlined the mandate and role of the National CERT and the role and responsibility of Sectoral CERTs. She explained the criteria for the selection of Sectoral CERTs and the formation of Ghana's CERT Ecosystem. She explained how the various sections of the Cybersecurity Act, 2020 (Act 1038), related to computer incident responses and their impact on CERT operations.

REMARKS

A participant mentioned an ongoing trend within the health sector, where the unregulated sharing of personal details of patients and employees should be of concern to the country. Personal data is shared with organisations which are unknown. He advised that Data Protection standards need to be enforced to curb this problem. Mrs. Audrey Mnisi Mireku stated that there are baseline technical controls specified by the CII directive that would be implemented by Sectoral CERTs to cover this issue. She also stated that the CII directive outlines steps to implement baselines and risk assessment for institutions.

It was also indicated that the implementation and establishment of CERTs in the various sectors would pose difficulties for some, citing challenges such as lack of budgets; the CSA was urged to assist in establishing unformed CERTs such as the Military CERT.

ADVISORY WORKSHOP ON THE STREAMLINING OF PROCEDURES FOR MLA ENHANCED BY THE SECOND ADDITIONAL PROTOCOL RELATED TO CYBERCRIME AND ELECTRONIC EVIDENCE

BACKGROUND

As the use of and reliance on information technology becomes more prevalent in society, the unauthorised accessibility to computer systems and networks have also rapidly risen. This amongst many other cybercrimes currently present transnational challenges and require effective international cooperation at all levels, specifically at the judicial and police levels to improve international cyber resilience.

Law enforcement agencies and prosecution services are therefore increasingly required to deal with identification of cybercriminals in foreign jurisdictions through data acquisition internationally and the use of tools such as the 24/7 points of contact network and the Mutual Legal Assistance Treaty (MLAT) to ensure successful investigations and prosecutions.

In line with this, the Council of Europe (CoE) in partnership with the Cyber Security Authority (CSA) as part of the programme of activities for the National Cyber Security Awareness Month (NCSAM) 2021, organised a two-day Advisory Workshop on the Streamlining of Procedures for MLA enhanced by the Second Additional Protocol related to Cybercrime and Electronic Evidence in Accra. The workshop was held from October 18 - 19, 2021 in Accra.

This training was delivered by CoE experts and Ghanaian officials from judicial authorities and law enforcement agencies, who shared knowledge and expertise with participants.

The meeting was attended by officials from the Criminal Investigations Department (CID) of the Ghana Police Service, the Attorney General's Department, Judicial Service of Ghana, National Intelligence Bureau (NIB), Economic and Organised Crime Office (EOCO), National Signals Bureau (NSB) and Cyber Security Authority (CSA).

WELCOME REMARKS

Dr. Albert Antwi-Boasiako
Ag. Director-General,
Cyber Security Authority

Dr. Antwi-Boasiako thanked officials and experts from the CoE for their efforts in assisting Ghana to effectively utilise various instruments and tools in the Budapest Convention and the use of digital evidence to combat cybercrime issues.

He noted that there has been some interventions such as trainings, capacity building workshops and advisory missions since Ghana acceded to the Budapest Convention in 2018. He further noted that the advisory mission focused on MLAT; how to effectively use provisions in the convention and the 24/7 point of contact which remains an important single channel for cross-border cooperation on cybercrime investigations and prosecutions. He mentioned that online services used by most Ghanaians are hosted in other countries and it is imperative that formal cooperation exists to provide the required assistance and electronic evidence needed to fight cybercrimes hence the advisory workshop aimed at strengthening formal cooperation and establishing the required conditions to utilise the provisions in the conventions.

In his conclusion, Dr. Antwi-Boasiako stated that the Cyber Security Authority has the responsibility to ensure that specialised agencies with powers to regulate cybersecurity are well equipped and this intervention is one of the mechanisms to ensure capacity building. He thanked participants for joining the workshop and urged them to engage actively in the sessions.

REMARKS

Ms. Martha Stickings
Programme Manager,
Cybercrime Programme Office of the
Council of Europe

Ms. Martha Stickings welcomed all participants and stated that it was a pleasure to organise such a workshop in collaboration with Ghana which is one of the priority countries of the GLACY+ Project. She then thanked Dr. Antwi-Boasiako for his continual support for the project. Ms. Stickings gave a brief history of the Council of Europe and an overview of the GLACY+ Project. She mentioned that the main aim of the project is to strengthen the capacity of states worldwide to acquire legislation on cybercrime and electronic evidence and to effect international cooperation. She emphasised that the aim of the two-day advisory mission was to facilitate discussions between participants and CoE experts on how to simplify MLA procedures and to utilise other international cooperation tools.

DAY ONE

PRESENTATION
INTERNATIONAL CO-OPERATION TOOLS WITH REFERENCE TO ARTICLES 24 TO 35 OF THE BUDAPEST CONVENTION

Madam Betty Shave
Expert, Council of Europe

Madam Shave gave an overview of the general principles relating to mutual assistance, procedures pertaining to mutual assistance requests in the absence of applicable international agreements, mutual assistance regarding provisional measures, mutual assistance regarding investigative powers and the 24/7 network.

Justice Afia Serwah Asare-Botwe
Judicial Service of Ghana
She educated participants on the legal basis of international cooperation on cybercrime and electronic evidence vis a vis current legislation in Ghana. She mentioned that after the accession to the Budapest Convention, there was an amendment to the Electronic Transactions Act, 2008 (Act 772) and the passage of the Cybersecurity Act, 2020 (Act 1038) to be in consonance with the convention.

She iterated that, investigators must capitalise on the INTERPOL I-24/7 to request assistance since it is a web-based communication system that can be accessed by authorised law enforcement officials to obtain immediate assistance in computer-related investigations and evidence collection. She also mentioned that in Ghana there is the Mutual Legal Assistance (MLA) Act, 2010 (Act 807) which governs the MLA methods by competent people thus this can also be leveraged on as part of international cooperation but stressed the request for cooperation and assistance in the acquisition and preservation of data and other evidence are dependent on domestic and international law. She told investigators to desist from making common errors such as not having a search and seizure warrant in the acquisition of digital evidence to prevent it from not being admissible at the court of law.

She further stated that when enquiring information, investigators must state clearly and be succinct when writing their affidavits. She concluded by advising investigators that they should endeavour to let their actions and procedures be consistent with both local and international laws during investigations.

Mr. Pedro Verdelho
Council of Europe Expert

He led a discussion on the existing model of formal assistance in Ghana. Mr. Verdelho explained that the Budapest Convention differentiates between different types of data an investigator may ask from a service provider and that article 81 of the Budapest Convention may directly ask a service provider abroad for subscriber information.

Mr. Branko Stamenkovic
Council of Europe Trainer

He gave a brief presentation on the existing practice regarding requesting and receiving assistance requests: current practices and issues. He gave an overview on the already existing Mutual Legal Assistance and mentioned that with respect to cybercrime, speed in investigating is very essential due to the tricky nature of digital evidence. He touched on the basic level of the MLA citing bilateral, multilateral (regional) and international as some of the basic levels. He mentioned direct transmission between judicial authorities and transmission between central authorities as some of the MLA channels.

In his presentation, he further stated other channels which support MLA spontaneous information exchange such as Article 26 and 35 of CoE Cybercrime Convention, European Judicial Cybercrime Network (EJCN) and joint investigation teams. There was a coffee break after the session.

Mr. Branko Stamenkovic, spoke extensively on using informal assistance to obtain electronic evidence: current practices and issues encountered. He explained that the MLA is usually demanding and delays when a request is made. He went further to demonstrate the processes involved in exercising the MLA. He explained that administrative assistance can be classified as informal assistance since no formal letter of request has to be issued. He added that this form of assistance is used when making evidence requests to a state where no coercive power is required. He also mentioned that although the means of making an informal request is administrative, the material that can be sought is evidential and will be admissible at the court of law, that is if an informal request is made and executed lawfully. He proceeded to present on country-specific cybercrime laws that investigators can leverage on to informally request for digital evidence.

DAY TWO

PRESENTATION

CURRENT PRACTICES, ISSUES ENCOUNTERED AND OPPORTUNITIES.

Madam Betty Shave in collaboration with national and multi-national service providers

She explained that a good relationship with national and multi-national service providers help countries when requests are made to service providers in gathering digital evidence. She noted that educating service providers and government officials about requirements and technology helps the relationship between them. She also explained that with regards to multi-national service providers, organising collaborative events and projects aids in mutual learning and quickening the response to requests made to multi-national providers through their national offices present in one's country.

With regards to communication with service providers, she highlighted that learning the capabilities, retention polices of service providers and request handling greatly improves communication with them. She further urged government officials to leverage on the 24/7 network to determine whether an unfamiliar provider is a criminal or to seek help in facilitating a request, especially if it is an emergency.

Mr. Branko Stamenkovic also demonstrated how law enforcement can request information from social media service providers since they have made channels available for subscriber requests. He added that previously, such requests were made to the service providers as the institution requesting should be well informed

about the process and policies of the service providers and that official address should be used in the request. He asked to know the supervisors of the 24/7 network in Ghana. Mr. Frank Antwi-Boasiako responded to the question by saying that the National Security Council Secretariat is in charge of the 24/7 network in Ghana.

Madam Yvonne Atakora-Obuobisa, the Director for Public Prosecutions at the Ministry of Justice and Attorney General's Department gave a brief presentation on the existing informal assistance in Ghana with regards to digital evidence.

She mentioned that there was the need for state institutions to cooperate with each other quickly via phone calls and emails rather than relying on the old methods of cooperating like writing letters and waiting for responses. She said due to the fast pace at which cybercrimes are committed, fast cooperation will help in cybercrime investigations. She also gave the opinion that requisite skills must be developed in order to cooperate on a faster and even level. Madam Obuobisa highlighted sections of the Cybersecurity Act, 2020 (Act 1038) with respect to international cooperation and urged investigators to leverage on the 24/7 network.

Mr. Pedro Verdelho presented on the future second additional protocol to the Budapest Convention on Cybercrime. This discussed the strengthening of co-operation and disclosure of electronic evidence to enhance Mutual Legal Assistance. He mentioned that the draft protocol was concluded in May 2021 and is currently in the internal political process within the Council of Europe and that it is expected to be approved by the parties to the Budapest Convention and by the Committee of Ministers. He also stated that the protocol is expected to be opened for signature in the first months of 2022. He explained that the second protocol included formal standard provisions (such as purpose, scope of application, effects and territorial application), conditions and safeguards; a very detailed regime on the protection of personal data.

CLOSING REMARKS

Dr. Herbert Gustav Yankson

He thanked officials of the CoE and encouraged participants to share the knowledge learnt with fellow colleagues to build capacity with regards to international cooperation. Ms. Martha Stickings from the CoE also thanked participants for their contributions.

SPECIALISED COURSE ON THE INTERNATIONAL COOPERATION FOR PROSECUTORS AND JUDGES

BACKGROUND

As the use of information and technology becomes more pervasive in our society, the targeting and exploitation of computer systems have become increasingly common. The sophistication in crimes committed using computer systems have become a problem for many countries. There is, however, the existing concern with the slow adjustments in the judicial actors applying laws. A major contributing factor to this is inadequate training, where judges, prosecutors and other judicial officials can build their skills, capacity and knowledge to better understand cybercrime and its nature and how to utilise available instruments and approaches to international cooperation. It is thus important that in investigating and prosecuting cybercrime, countries are ready and capable of employing a range of international cooperation modalities available under the Budapest Convention on Cybercrime in a proficient and timely manner.

As part of the GLACY+ Project, a three-day workshop was organised to take representatives from the justice sector through a Specialised Online Module on International Cooperation.

Joining virtually, there were:
(i) Council of Europe experts and
(ii) GLACY+ team members

Joining in person were:
(iii) Ag. Director-General of Cyber Security Authority (CSA), Dr. Albert Antwi-Boasiako
(iv) Director, Cybercrime Unit of Criminal Investigations Department (CID), Dr. Herbet Gustav Yankson
(v) Participants from the Office of the Attorney-General, Department of Public Prosecution
(vi) Participants from Ghana Judicial Service
(vii) Participants from Criminal Investigations Department (CID), Ghana Police Service

DAY ONE

OPENING REMARKS

Dr. Albert Antwi-Boasiako
Ag. Director-General, Cyber Security Authority (CSA)

Dr. Albert Antwi-Boasiako began by welcoming all participants and thanked them for their willingness to learn and engage on a very important topic relevant to their work, as it showed a unified commitment towards building expertise and skills to better deal with cyber incidents and cases. He added that the Government of Ghana would continue to take active steps to be well equipped to better handle cybercrime and threats. Dr. Antwi-Boasiako noted that the specialised course supported the nation's efforts to build public players who will be able to handle cyber related matters. In his closing statements, Dr. Antwi-Boasiako noted that the justice sector is a primary and key player in enforcing national and international laws pertinent to our jurisdiction. Hence, it is a great relief that the workshop was taking place.

REMARKS

Ms. Martha Stickings
Council of Europe (CoE)

In her remarks, Ms. Stickings started by thanking Dr. Antwi-Boasiako, who has been a great support to the GLACY+ Project and the Council of Europe in general. She also welcomed all the participants to the workshop.
Ms. Stickings noted that Ghana is one of the first countries to be covered

under the GLACY+ Project and has cooperated closely with the Council of Europe for some years. Ms. Stickings took the participants through the work of the Council of Europe on cybercrime, and the GLACY+ Project. She highlighted the aim of the GLACY+ Project, which is to strengthen capacities of States to apply legislations on cybercrime and electronic evidence, and to enhance their ability to effectively cooperate in this area. To achieve this aim, Ms. Stickings noted the three key components:

- to promote consistent cybercrime legislation, policies and strategies
- to strengthen the capacity of police authorities to investigate cybercrime and to engage in effective police-to-police cooperation and to create cybercrime units in Europe and other regions
- to enable criminal justice authorities to apply legislation, prosecute and adjudicate cases of cybercrime and electronic evidence and to engage in international cooperation.

OVERVIEW
LEGAL BASIS OF INTERNATIONAL COOPERATION IN RELATION TO CYBERCRIME & ELECTRONIC EVIDENCE

Ms. Hania Helweh
Council of Europe Consultant

Ms. Helweh started by giving a refresher on cybercrime and electronic evidence, where she touched on some offences such as computer-related offences, content-related offences, child pornography and copyright infringement. She gave an overview of the Budapest Convention, as a leading tool for cooperation in cybercrime and electronic evidence. Ms. Helweh gave a background of the Convention, noting that as at November 2020 there were 66 parties to the Convention and that as at October 2021 the total number of ratifications, signatures and invitations were 77. In analysing the Budapest Convention, Ms. Helweh looked into

(i) criminalising conduct
(ii) procedural tools
(iii) international cooperation.

She also touched on approaches to international cooperation for the participants to better understand the different channels and mechanisms for international cooperation. Speaking on this, Ms. Helweh gave an overview of Global and Regional Mechanisms, which include the United Nations Convention against Transnational Organized Crime (UNTOC), United Nations Convention against Corruption (UNCAC).

PRESENTATION
MUTUAL LEGAL ASSISTANCE (MLA) PRACTICE & PROCEDURES

Ms. Hania Helweh
Council of Europe Consultant

The first part of this session touched on international cooperation instruments, standards and channels of communication. Some of the instruments discussed included treaties and types of treaties, MLA legal requirement and considerations. Ms. Helweh referred to sections 27; 29-35 of the Budapest Convention when speaking on the standards on transmission through central authorities, existing grounds for refusal and more. She also noted future standards on international cooperation pertaining to cybercrime and e-evidence, referring to articles 2-4 and 6-9 of the 2nd Additional Protocol. Council of Europe assessment of MLA and other provisions, recommendations, and existing support. She proceeded to speak on the MLA channels of communication:

(i) direct transmission between judicial authorities
(ii) transmission between central authorities.

PRESENTATION
INFORMAL METHODS OF INTERNATIONAL COOPERATION

Mr. Branko Stamenkovic
Council of Europe Consultative Council of European Prosecutors (CCPE) Member

After giving an overview of the session, Mr. Stamenkovic kicked off the presentation by touching on formal versus informal MLA in criminal matters and citing examples of both formal and informal MLA. He stressed on the golden rule, which is to ensure that any administrative informal request is made and executed lawfully despite the 'informal' nature. He then proceeded to speak on international organisations and networks specialised in informal and formal cybercrime cooperation. Here, Mr. Stamenkovic gave an overview of some international bodies and their roles and objectives:

→ INTERPOL National Central Bureau (NCB) and Reference Points (NCRP), European Union 24/7

- Contact Point Entry, EUROPOL
- EUROJUST,
- Eurojust Judicial Cybercrime Network (EJCN).

Mr. Stamenkovic then spoke on the Budapest Convention international cooperation 24/7 network (Article 35). The last part of his presentation touched international response to cybercrime.

DAY TWO

MODERATOR:

Ms. Patricia Adafienu
Cyber Security Authority

For the second day, the first part of the event was led by Ms. Hania Helweh, a Council of Europe Consultant. She spoke on mechanisms under the Budapest Convention to facilitate International Cooperation. For this session, she gave insight and guidance on matters of international cooperation on cybercrime and electronic evidence as provided by the Budapest Convention and its forthcoming Second Additional Protocol.

Following this, a case study was presented to participants on the topic- Utilising Digital Evidence Acquisition through International Cooperation Mechanisms.

The second part of the session touched on challenges faced by the participants when handling cases. Participants shared their experiences with other parties and how sometimes, the parties they work with make the cases difficult, which in turn puts a strain on the entire process. Both prosecutors and investigators shared their experiences.

The final session of the day touched on Public Private Partnerships (PPP)/Cooperation. During this presentation, the legal basis of public private partnerships were discussed, including the nature of partnerships and the implications on the parties and States involved. This presentation also spoke further on MLA and its purpose to present a guide to help different countries cooperate and the terms on which they operate.

DAY THREE

MODERATOR:

Ms. Patricia Adafienu
Cyber Security Authority

Final Day Session

The final day focused on Skills Building in Cybercrime, where the main highlight of the day was on the groups and Council of Europe representative discussing the case study and the findings. Some of the areas/subjects identified in the case study included international cooperation and processing requests pertaining to legal issues that require foreign assistance.

The participants were arranged in smaller groups to work on the case study into Skills Building in Cybercrime. This was followed by a group report. There was a Post – Test and Open Forum where participants shared their experiences and some of the new insights they had received from the session.

FORUM ON WOMEN IN

Technology & Cybersecurity

NATIONAL
CYBER SECURITY
AWARENESS MONTH

Mrs. Magdalene Apenteng

Chief Director, Ministry of Communications and Digitalisation

OPENING REMARKS

In her remarks, Mrs. Magdalene Apenteng, expressed her gratitude to the Cyber Security Authority (CSA) for leading such an engagement. She formally welcomed all in attendance and entreated all to participate fully in the forum. She added that the Government of Ghana is aware of the effects lack of access to internet is having on its people and how through initiatives, such as this bring the needed attention to bridging the digital divide. Mrs. Apenteng also referred to some statistics, which indicated that a global average of 52% of women are offline, compared to that of men, which is 42%. Women's access to technology is much more limited, because of cultural and economic factors, including others. She also cited a GSMA report on Mobile Economy in Sub-Saharan Africa where it shows that women across the region are 13% less likely than men to own a mobile phone and reports the gender gap in mobile internet use at 37%, indicating that this is the highest of any region.

SHARING OF EXPERIENCE

Ms. Eno Bragro Attrams

Administration Officer, CSA

Ms. Attrams in her address, spoke on how she had always wanted to and imagined that she would find herself in the humanities field. Working towards this, she pursued General Arts in her higher education. She then began to develop an interest in Information Technology (IT) but did not further her knowledge base in IT because of the mindset she had built that technology is mostly pursued by men and is a male dominated field. Finding herself at the Cybersecurity Secretariat for her National Service, Ms. Attrams worked with Dr. Antwi-Boasiako very closely and received a lot of encouragement from the now Ag. Director-General of the CSA as well as from her parents. Under Dr. Antwi-Boasiako’s leadership, Ms. Attrams remarked that the opportunities she had to learn have better equipped her with the necessary technical and professional skills, indicating that she is currently working towards pursuing a Master’s degree in Cybersecurity. She highlighted on some of the experiences she has had from the numerous workshops she has engaged in, despite not having a science background.

SHARING OF EXPERIENCE

Madam Jennifer Mensah

Cybersecurity & Data Privacy Legal Practioner (NCA)

The Cybersecurity and Data Privacy Legal, Madam Jennifer Mensah acknowledged all dignitaries present and shared her experience on the journey so far, indicating that she had her BSc. in Biochemistry from University of Ghana before landing at NCA as a Data Collector in the engineering division in her search for a job. She further read law and specialised in Cybersecurity and Data Privacy to enhance her competence in her field of work. Madam Jennifer Mensah highlighted that she supports the Chief Information Security Officer of NCA to manage a team of 14 people who are mandated to ensure that licensees and authorisation holders comply with the Cyber Security Obligations and Data Privacy Obligations as prescribed in the law.

She added that she had some training with the Data Protection Commission (DPC) which led to her promotion to Data Protection Supervisor. She was also part of the trainers who trained lawyers, Judges, and law enforcement agents on Global Action on Cyber Crime (GLACY+) Project. Madam Jennifer Mensah indicated that "since we live in a digital world, it is upright for law enforcers to understand cybercrimes to convict cybercriminals".

PANEL DICUSSION

The Minister for Communications and Digitalisation and MP for Ablekuma West Constituency, Mrs. Ursula Owusu-Ekuful who had been adjudged the Digital Leader of the Year at the 11th Ghana Information Technology & Telecom Awards (GITTA 2021), was the moderator of the panel discussion. She is a lawyer with over 30 years' experience. She was appointed the Minister for Communications in 2016 by the President and has occupied that office position till date. In the biography, Hon. Ursula Owusu-Ekuful was recognised for her dedication and oversight of the development of cybersecurity in the country. At the end of the Minister's first tenure, Ghana's cybersecurity ranking had greatly increased from 32.6% to 86.69%. The Hon.Minister has successfully institutionalised Ghana's cybersecurity, crafting Ghana's Cybersecurity Agenda and supporting local tech start-ups as well as encouraging women and children to venture into ICT, as she champions the 'Girls in ICT' Initiative in Ghana which is aimed at bridging the digital divide in Ghana.

The all-female panel comprised :

Ms. Folake Olagunju, the Programmes Officer of ECOWAS (virtual presentation), Ms. Farida Bedwei, the Chief Executive Officer of Byte the Bits, Mrs. Patricia Obo-Nai, the Chief Executive Officer of Vodafone Ghana. Ms. Adoma Peprah, the Country Manager for VISA Ghana, Ms. Adjoa Asamoah, the Information System Audit Lead of ISACA, Ms. Lucy Quist, Managing Director of Morgan Stanley (virtual presentation)

MODERATOR:

Hon. Ursula Owusu-Ekuful

Minister for Communications & Digitalisation (MOCD)

The Minister for Communications and Digitalisation engaged the panelists on their journeys into the field and working space of technology and cybersecurity. She asked for their experiences and challenges in getting to such high ranks in their working environments.

REMARKS

Ms. Folake Olagunju

Programmes Officer, ECOWAS

Madam Folake Olagunju indicated that she started working with British telecom and then moved on to

Business Analysis and Programme Management due to her interest in that field. She stressed on the importance of Cybersecurity and the need to enroll in that field and added that the outbreak of COVID-19 gave rise to the use of technology. Madam Olagunju finally congratulated the Minister for Communications and Digitalisation for establishing the Girls in ICT Initiative and promised to get in touch with her.

REMARKS

Ms. Farida Bedwei
Chief Executive Officer,
Byte The Bits

The Chief Executive Officer of Byte the Bits, Madam Farida Bedwei, disclosed that her handwriting motivated her to pursue ICT, starting as a typist in 1980. She was home schooled by her mother up to the age of twelve (12) and continued with studies in GW Basic Programming Language. Madam Bedwei indicated that after she obtained a Diploma in IT, she walked into Hemant Software Services Limited to apply for work. She finally established Byte the Bits to impact field solutions, to promote data analysis and to make better decisions with credible data.

REMARKS

Mrs. Patricia Obo-Nai
Chief Executive Officer,
Vodafone Ghana

The Chief Executive Officer of Vodafone Ghana, Mrs. Patricia Obo-Nai specified that she offered electrical engineering and had her internship with a roadside radio shop where she learnt more about soldering. She had employment at Tigo where she spent 14 years and finally was employed at Vodafone Ghana in 2014 as the Chief Executive Officer. She understood the front desk role and could relate and understand complaints from customers in areas of system breakdown. She then grew interest in technology issues and became the CEO of a telecommunication company.

REMARKS

Ms. Adoma Peprah
Country Manager,
VISA Ghana

The Country Manager for VISA Ghana, Madam Adoma Peprah, indicated that she did her MBA on part-time basis and worked in the banking sector. In 2019, she moved to Ghana to do something for the continent which has always been her passion.

Throughout her career, her biggest highlight was when a Multinational Company had requested her to open up for them as a representative. She added that her career has always been linked through the jobs she has done. From her personal experience, she encouraged the invited guests to have a goal in mind to guide them, as this key factor helped her to reach where she is today.

REMARKS

Ms. Adjoa Asamoah
Information System Auditor,
Bank of Ghana

The Information System Audit Lead of ISACA, Madam Adjoa Asamoah, studied Computer Science in Ashesi University and completed in 2006. Madam Asamoah always had interest in spy movies and conspiracy theories, with this interest she tried being a hacker and that's what built her interest in the computer science class; her class had only 4 females when graduated. She added that Madam Farida Bedwei inspired her to take up a programming course, at a time when she was on internship. This field, she said has opened ways for her to speak at different conferences in Rwanda and other places.

REMARKS

Mrs. Lucy Quist
Managing Director,
Morgan Stanley

The Managing Director of Morgan Stanley, Mrs. Lucy Quist in a video display indicated that technology can be used to accelerate the transformation needed as a country, therefore, the transformation is needed as a country to derive economic benefit for all. Speaking on how technology can aid young women in digitalisation, she emphasised that technology is the new mining hub for data collection. Also, since most women are into small scale businesses, this can better their businesses beyond the traditional medium of marketing. Additionally, for economic change, policy makers should create policy to entirely preserve the use of the internet she concluded.

Hon. Ama Pomaa Boateng
Deputy Minister for Communications and Digitalisation

CLOSING REMARKS

The Deputy Minister for Communications and Digitalisation, Hon. Ama Pomaa Boateng, thanked all for gracing the event. Shet thanked the Minister for Communications and Digitalisation, Hon. Ursula Owusu-Ekuful for her enormous support in ensuring children particularly girls in Ghana are knowledgeable in Information Technology through the Girls in ICT Initiative. Hon. Pomaa Boateng indicated that three thousand (3,000) girls in the Ashanti Region had been trained in Cybersecurity and one thousand (1,000) primary and JHS girls had been trained in coding in the month of September in ten (10) regions of Ghana. Hon. Pomaa Boateng finally encouraged all especially ladies to take IT seriously since we are in a digital world.

HIGH-LEVEL AND REGIONAL ENGAGEMENTS

on the Cybersecurity Act, 2020 (Act 1038)

NATIONAL
CYBER SECURITY
AWARENESS MONTH

HIGH-LEVEL AND REGIONAL ENGAGEMENTS ON THE CYBERSECURITY ACT, 2020 (ACT 1038)

BACKGROUND

The 2021 edition of the NCSAM entailed a few scheduled regional activities consistent with previous editions. This year's exercise took a different approach comprising high-level engagements on the New Cybersecurity Act, 2020 (Act 1038) led by the Acting Director-General of the Cyber Security Authority (CSA), Dr. Albert Antwi-Boasiako.

The high-level and regional engagements sought to engage with relevant stakeholders to deliberate on the Act and its implications, as Ghana aims to build upon its foundational cybersecurity pillars, which has been ranked 3rd on the African continent with a rating of 86.69% according to the ITU's Global Cybersecurity Index report, 2020. The expectation was to improve awareness of the Cybersecurity Act and its implications on the specific sectors of Ghana's economy.

Stakeholder bodies who were engaged included; Heads of State-Owned Institutions, members of selected Regional Security Councils (REGSEC), Civil Society Organisations, Ghana Journalists' Association (GJA), Media representatives, and Private sector stakeholders.

NCCE UNDERGOES TRAINING ON CYBERSECURITY ACT, 2020 (ACT 1038) FAKE NEWS

The staff of the National Commission for Civic Education (NCCE) were trained on the new Cybersecurity Act, 2020 (Act 1038) and how to identify fake news in order to alert the public on the risks.

The high-level event was jointly organised by the Commission and the Cyber Security Authority (CSA) in Accra on October 21, 2021. The training was aimed at increasing the knowledge of staff to create public awareness on the dangers of fake news. The capacity building and sensitisation programme on the identification of fake news for staff of NCCE.

Commenting on the essence of the training, the Chairperson of the NCCE, Ms. Josephine Nkrumah, noted that with the unfolding events in the world and how quickly information goes viral in the Cyber space as well as how people react to them, it was important for Civic Educators to have knowledge on fake news.

The Acting Director-General, Cyber Security Authority (CSA), Dr. Albert Antwi-Boasiako, commended the leadership of NCCE for being proactive in taking initiative to train their staff on fake news.

He said the Cybersecurity Act, 2020, mandates the CSA to conduct awareness creation, sensitisation, and capacity building programmes on risk arising from the use of the cyber space among Ghanaians. He noted that by exploring CSA's common grounds with the NCCE, which promotes civic education, the citizenry would be adequately informed to identify the risk they are exposed to in using the cyber space.

Dr. Antwi-Boasiako further stated that cybercrime poses a threat to Government, State Institutions, individuals using mobile money digital platforms and children who are more vulnerable, and expressed grave concern about fake news gaining legitimacy in the media.

He therefore reaffirmed the commitment of the CSA to not just share knowledge with NCCE, but to collaborate with the Commission to implement the National Cybersecurity Policy and Strategy, as well as access the possibility of organising joint quarterly programmes in 2022.

Mr. Alexander Oppong, the Lead for Capacity Building and Awareness Creation at the CSA took participants through a presentation on fake news, how to identify them, as well as the Cybersecurity Act, 2020 (Act, 1038).
He said fake news also known as hoax news is a false information or propaganda either written or published to look like authentic news and according to section 76, of the Electronic Communications Act, 2008 (Act 775) sharing of fake news is illegal. Some effects of fake news are that they have financial and even health impacts on the victims, they produce fear and threaten national security. It also undermines the democratic process and democratic impacts. It is therefore important that civic educators get the required knowledge to combat against these crimes.

Mr. Oppong further touched on the types and effects of fake news and urged participants to verify fake news from the source. To spot fake news, one must: verify where the story is from, who is producing the story, if it looks professional, if it has bad spelling, or grammar. He said that if it does not have the above-mentioned then the news is authentic.

The NCCE Commission Secretary, Mr. Kojo Tito Voegborlo, entreated participants to make good use of what they have learned and help create the needed awareness among their peers and the public.

WORKSHOP ON THE CYBERSECURITY ACT FOR THE CRIMINAL JUSTICE SECTOR

The Cyber Security Authority (CSA) met with the Criminal Justice Sector on Friday, October 15, 2021, in Accra.

The workshop focused on empowering the Criminal Justice Sector on the provisions of the Cybersecurity Act, 2020 (Act 1038).

In Attendance were the Acting Director-General of the Cyber Security Authority, Director of Public Prosecutions, Madam Yvonne Atakora-Obuobisa, Justice of the High court, Justice Afia Serwah Asare-Botwe, amongst other key participants from the sector.

Dr. Albert Antwi-Boasiako urged the participants to address and focus on cases with key evidence of crimes so that prosecutions can be made to counter crimes and adhere to the Cybersecurity Act, 2020 (Act 1038). Using an example of a thousand cases, he noted that if only 20 of those cases provide credible evidence that can be addressed after triaging, that is where agencies such as the Criminal Investigations Department (CID) and the Bureau of National Investigations should focus their efforts (BNI).

Madam Yvonne Atakora-Obuobisa emphasised the importance of prosecutors, investigators, and other intelligence officials in the implementation of the Cybersecurity Act, 2020 (Act 1038) and its relationship to the Criminal Justice sector. She also discussed what crimes can be prosecuted, investigated and how to best obtain evidence.

Justice Afia Serwah Asare-Botwe stressed the importance of understanding that electronic evidence is an inherent part of the prosecution and the need for parents to be more vigilant and protective of their children's online interactions. She noted that as we progressed into the electronic age, we would require electronic evidence to prove murder and many other cases that may arise.

The Cyberstecurity Act 2020 was thoroughly discussed, starting with its establishment and foundational definitions in order to guide all participants in their knowledge and understanding of what the Act constitutes and to further help them in exercising their duties.

WORKSHOP ON THE NEW CYBERSECURITY ACT FOR GOVERNMENT CHIEF EXECUTIVE OFFICERS

The Cyber Security Authority (CSA) organised a Workshop on the Cybersecurity Act, 2020 (Act 1038) for Chief Executive Officers (CEOs) of State-Owned Enterprises in Accra on Thursday, October 14, 2021 in Accra in collaboration with the State Interests and Governance Authority (SIGA) to sensitise CEOs on the provisions of the Cybersecurity Act, 2020 (Act 1038), seek their inputs for implementation, and the need for them to incorporate cyber security measures in their operations.

The workshop was attended by the Director-General of the State Interests and Governance Authority (SIGA), Hon. Stephen Asamoah-Boateng, alongside major Chief Executive Officers of State-Owned Enterprises in Ghana.

Speaking at the event, Dr. Albert Antwi-Boasiako, the Acting Director-General of the Cyber Security Authority (CSA), explained that the Act established the Authority from the former National Cyber Security Centre (NCSC) and provides a comprehensive legal framework for the protection of the nation's critical information infrastructure, regulate cybersecurity activities including licensing of cybersecurity services, prevent, manage and respond to cybersecurity threats and cybersecurity incidents, and testablish a platform for cross-sector engagement on matters between key public institutions and the private sector amongst others

He informed the participants that cyber security exposures and vulnerabilities could be the unmaking of business organisations, adding that organisations such as FedEx and Maersk in 2017 lost about $10 billion due to cyber-attacks on their systems and operations.

He said it was, therefore, important for heads of SOEs to put systems in place to prevent their organisations from cyber-attacks; - “The responsibility of protecting our data and critical information rests with managing directors and CEOs of state institutions,”.

Hon. Stephen Asamoah-Boateng, Director-General of the State Interests and Governance Authority (SIGA) urged state-owned enterprises (SOEs) to embrace cyber security issues and put in the necessary structures to protect their organisations from cyber-attacks. He noted that the deployment and the promotion of cyber security measures in organisations would feature prominently in the performance contract assessment processes to increase the need for CEOs to adopt measures to combat cybersecurity threats.

REGIONAL ENGAGEMENTS

SUMMARY OF EVENTS

EASTERN REGION

The team led by the Acting Director-General of the CSA on October 19, 2021, engaged members of the Eastern Regional Security Council (REGSEC) comprising the Chairman and Eastern Regional Minister, Hon. Seth Kwame Acheampong, and heads of the security agencies in the region as well as selected media.

Also in the Eastern Region, there was an engagement with the members of Ghana Journalists' Association.

VOLTA REGION

A cybersecurity sensitisation event was held at the Awudome Senior High School on Thursday, October 14, 2021 in Awudome. This effort targeted students with sensitisation on cyber hygiene best practices with the fundamental objective of spearheading the Child Online Protection agenda. The event recorded about 1200 participants comprising students and teachers at the school.

GREATER ACCRA REGION

A total of four (4) high-level engagements led by the Acting Director-General of the Authority and the Lead for Capacity Building & Awareness Creation at the Authority, Mr. Alexander Oppong, from Thursday, October 14 to Friday, October 22, 2021 in Accra. These were workshops on the New Cybersecurity Act, 2020 for Chief Executive Officers (CEOs) of State-Owned Institutions, and High-Level Engagement on the New Cybersecurity Act, 2020 (Act 1038) with the Ghana Journalists' Association (GJA) both on Thursday, October 14, 2021. The workshop on the New Cybersecurity Act, 2020 (Act 1038) for the Criminal Justice Sector, and High-Level Engagement on the New Cybersecurity Act, 2020 (Act 1038) with the National Commission for Civic Education (NCCE) were both held on Friday, October 22, 2021. A total of 230 participants were recorded for all the events with the following distribution: 80 participants for the CEOs workshop, 50 participants for the GJA event, 50 participants for the Criminal Justice Sector workshop, and 50 participants for the NCCE workshop.

WESTERN REGION

The Ag. Director-General of CSAtt led the two (2) high-level engagements in this region on Thursday, October 21, 2021 in Takoradi. The targeted stakeholders were members of the Ghana Chamber of Commerce and the Institute of Chartered Accountants Ghana (ICAG). A total of 110 participants comprising 80 representatives from the Ghana Chamber of Commerce and 30 representatives from ICAG participated in a separate event conducted for each group. The participants from the Ghana Chamber of Commerce

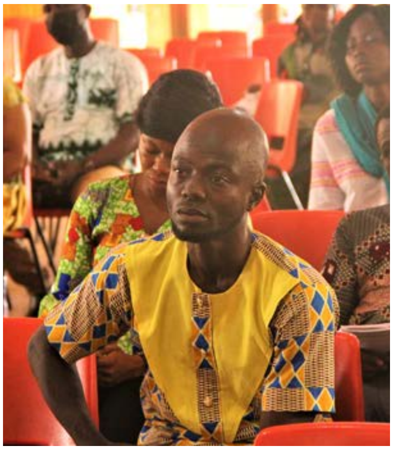
included representatives from the Association of Small-Scale Miners, Traders, Drivers, Western Diamond, Real Estate developers, Registrar General-Sekondi, Traditional Healers, Beauticians, Cosmetologists, Prudential Life Insurance, Contractors, Civil and Mechanical Engineering, GIPA, Stanbic Bank among others.

WESTERN NORTH REGION

There was a cybersecurity sensitisation event at the Sefwi Wiawso Senior High School on Friday October 22, 2021, in Sefwi Wiawso. This effort targeted students with sensitisation on cyber hygiene best practices with the fundamental objective of spearheading the Child Online Protection agenda. The event recorded about 1,100 participants comprising students and teachers at the school.

NORTHERN REGION

The team led by the Lead for Capacity Building & Awareness Creation at the Authority, Mr. Alexander Oppong engaged members of the Ghana National Association of Teachers (GNAT) in Tamale and its environs in a high-level engagement on the Cybersecurity Act, 2020 on Tuesday, October 26, 2021. A total of 70 members of the Association participated in the event.



ASHANTI REGION

Two (2) high-level engagements led by the Acting Director-General of the Authority were organised in this region. These were High-Level Engagement on the New Cybersecurity Act, 2020 (Act 1038) with the Ghana Bar Association (GBA), and Workshop on the New Cybersecurity Act, 2020 (Act 1038) for the Criminal Justice Sector, on Wednesday, October 27, 2021 and Thursday, October 28, 2021 respectively in Kumasi. A total of 110 participants were recorded for all the events comprising 60 participants for the GBA event, and 50 participants for the Criminal Justice Sector workshop.

HIGH LEVEL ENGAGEMENT ON THE NEW CYBERSECURITY ACT, 2020 (ACT 1038) WITH THE GHANA JOURNALISTS' ASSOCIATION (GJA)

The Cyber Security Authority (CSA) organised a Workshop on the Cybersecurity Act, 2020 (Act 1038), for members of the Ghana Journalists' Association (GJA) to promote capacity building & awareness and educate members of the Ghana Journalists' Association (GJA) on the new Act as part of events marking the National Cyber Security Awareness Month (NCSAM) 2021. The workshop was held at the Ghana International Press Centre, Ridge, Accra.

The meeting was attended by the President of the GJA, Mr. Roland Affail Monney and about 45 members of the Association.

Speaking at the event, Dr. Albert Antwi-Boasiako, the Acting Director-General of the Cyber Security Authority (CSA), explained that, the Act 1038 established the Cyber Security Authority and provides a comprehensive legal framework for the protection of the nation's critical information infrastructure, and regulation of cybersecurity activities in the country which includes licensing of cybersecurity services and service providers as well as ensuring the protection of children on the internet.

In light of Ghana's digital transformation agenda, which is crucial to the country's economic development, he said that Act 1038 also aimed to position Ghana to prevent, manage, and respond to cybersecurity incidents. This is because economic growth is dependent on a secure, safe, and resilient digital environment.

Dr. Albert Antwi-Boasiako emphasised the significance of the media in Ghana's efforts to enhance cyber security. He commended them on work being done and urged them to collaborate with the Authority on cybersecurity matters.

Mr. Alexander Oppong, Lead for Capacity Building and Awareness Creation (CBAC) and Madam Audrey Mireku, Head of Computer Emergency Response Team (CERT) further enlightened the participants on the various provisions of the Act and the ways to identify fraud and the Cybercrime / Cybersecurity Incidents Reporting Points of Contact.

CONCLUSION

The 2021 edition of the National Cyber Security Awareness Month (NCSAM) organised under the theme, Ghana's Cybersecurity Act, 2020; Its Implications and the Role of Stakeholders sought to engage with relevant stakeholders to deliberate on Act 1038 and its implications as Ghana seeks to build upon its foundational cybersecurity pillar. Under the period under review (2017-2020) Ghana's cybersecurity readiness was ranked 3rd on the African continent and 43rd globally, with a rating of 86.69% according to the ITU's Global Cybersecurity Index report, 2020. The month-long event which leveraged on the successes of the previous editions consisted of high-level and regional events strategically targeted at key public and private sector institutions, businesses, civil society institutions, the media and the general public. Activities were conducted via workshops, forums, presentations, media interviews and seminars. The events were organised in a hybrid format comprising physical engagements and the utilisation of virtual platforms.

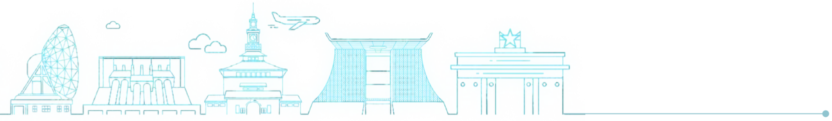
The formal opening took place on October 1, 2021 which gave opportunity to the launch of the Critical Information Infrastructure (CII) Directive which establishes baseline cybersecurity requirements for all designated CII Owners. The Directive further aligns with the five strategic imperatives of Ghana's National Cybersecurity Policy and Strategy, namely Build a Resilient Digital Ecosystem, Secure Digital Infrastructure, Develop National Capacity, Deter Cybercrime and Strengthen Cooperation. The opening also witnessed the launch of the Cyber Security Authority which is established by Act 1038 to regulate cybersecurity activities in the country, promote the development of cybersecurity and provide for related matters.

Regional cybercrime/cybersecurity sensitisation exercises were organised across the sixteen regions of Ghana where about 2,900 participants were reached. These included the Ghana Journalists' Association (GJA), Regional Security Council (REGSEC), State Interests and Governance Authority (SIGA), National Commission for Civic Education (NCCE), Ghana Chamber of Commerce, Ghana Bar Association, Criminal Justice Sector, Ghana National Association of Teachers (GNAT), some selected Senior High Schools, the media and the public. These awareness creation and capacity building activities further consolidated and re-affirmed the CSA's commitment to cybersecurity development.

The High-level events were conducted to extensively cover the four thematic areas of the A Safer Digital Ghana Campaign i.e. Children, the Public, Businesses, Government. The activities were scheduled weekly with each week dedicated to a thematic area. The events comprising panel discussions, workshops and seminars witnessed the participation of about 500 participants from governmental and non-governmental institutions, industry players, the media fraternity, academia, international partners and Ghana's diplomatic corps.

The month-long event which sought to engage relevant stakeholders on the implementation of Act 1038 proved to be unique with an increase in scope and reach with regards to capacity building and awareness creation.

The Ministry of Communications and Digitalisation (MoCD) on behalf of the Cyber Security Authority (CSA) extends its gratitude to all stakeholders, sponsors and partners for the immense support and financial commitment that led to the successful organisation of the event and most importantly towards the development of the country's cybersecurity for A Safer Digital Ghana.



RECOMMENDATIONS

Below are some of the key recommendations made during the NCSAM 2021:

- Increased education and awareness on the Cybersecurity Act, 2020 among stakeholders, children, the public, businesses, and the government.
- Enhanced Government contributions towards the overall improvement of cybersecurity posture in Ghana.
- Increase awareness on provisions for the designation and protection of Critical Information Infrastructure (CII).
- Enhance collaborations both local and international for improved cybersecurity preparedness.
- There is the need to consider cybersecurity as a developmental and national issue.
- The facilitation of the accreditation and licensing of Cybersecurity Professionals and Practitioners by the CSA as mandated by Section 57 of Act 1038.
- The need for establishment of an Industry Forum as provided for in Section 81 of Act 1038.

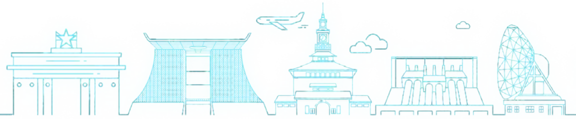


PHOTO GALLERY

MINISTRY OF COMMUNICATIONS & DIGITALISATION
NATIONAL CYBER SECURITY CENTRE
NATIONAL CYBER SECURITY AWARENESS MONTH 2021
GHANA'S CYBERSECURITY ACT 2020
TS IMPLICATI O THE ROLE OF STAKEHOLDERS

ERSECURITY ACT 2
MPLICATION HE ROLE OF STA RS
MR. JOE ANOKYE
NATIONAL COMMUNICATIONS AUTHORITY (NCA)
HON. URSULA OWUSU-EKUFUL
MINISTER FOR COMMUNICATIONS AND DIGITALISATION (MOCD)

PHOTO GALLERY

PHOTO GALLERY

PHOTO GALLERY

PHOTO GALLERY

PHOTO GALLERY

PHOTO GALLERY

PHOTO GALLERY

PHOTO GALLERY

PARTNERS

FREEDOM AND JUSTICE
NATIONAL COMMUNICATIONS AUTHORITY
WORLD BANK GROUP
COUNCIL OF EUROPE
CONSEIL DE L'EUROPE
CEDEAO
ECOWAS
GIFEC
unicef
NITA
DATA PROTECTION COMMISSION
GCNet
ITU
GDNR
WORLD ECONOMIC FORUM
UNITED NATIONS
FREEDOM ONLINE COALITION

ORGANISING PARTNERS

CRIMINAL INVESTIGATION DEPARTMENT
GHANA POLICE
POSTAL & COURIER SERVICES REGULATORY COMMISSION
GHANA ARMED FORCES
ECONOMIC AND ORGANISED CRIME OFFICE
GHANA POLICE
SERVICE WITH INTEGRITY
FREEDOM AND JUSTICE
GhanaPost
Ghana Journalists Association
NATIONAL IDENTIFICATION AUTHORITY
ChildOnline Africa
aiti
ADVANCED INFORMATION TECHNOLOGY INSTITUTE
GHANA-INDIA KOFI ANNAN CENTRE OF EXCELLENCE IN ICT
Financial Intelligence Centre
Republic of Ghana

SPONSORS

BANK OF GHANA EST. 1957

HUAWEI

Rayzone Group

innovare

IPMC I.T. Learning Center

GHANA CHAMBER OF TELECOMMUNICATIONS

EY Building a better working world

EMWA

e-Crime Bureau Cyber Security & Investigations Bureau

MTN

ISACA Accra Chapter

GLOBAL PARTNERS DIGITAL

MEDIA PARTNERS

JOY NEWS

METRO tv

GHANA BROADCASTING CORPORATION

GhanaWeb

PEACE FM 104.3 THE STATION WITH A VISION!

Hb HOMEBASE TELEVISION

GHone TV

103.5 fm STARR Simply The Best

GraphicOnline www.graphic.com.gh

YEN

Citi 97.3 fm

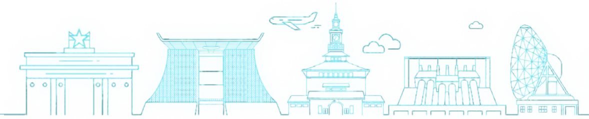
B&FT Business & Financial Times

pulse

DailyGuideNetwork

Publisher

THE NEW CRUSADING GUIDE



CYBERCRIME/ CYBERSECURITY INCIDENT REPORTING POINTS OF CONTACT

E-mail
report@csa.gov.gh

Whatsapp
050 160 3111

SMS
292

Online Form
www.csa.gov.gh/report

CALL
292

Mobile App
CSA Ghana