MINISTRY OF COMMUNICATIONS
Republic of Ghana

NATIONAL CYBER SECURITY WEEK

2017 REPORT

"SECURING GHANA'S DIGITAL JOURNEY"

People, Businesses, Government

MINISTRY OF
COMMUNICATIONS
Republic of Ghana

NATIONAL CYBER SECURITY WEEK

2017 REPORT

TABLE OF CONTENTS

CONCLUSION

ACKNOWLEDGEMENT

The Ministry of Communications is grateful to His Excellency, the President of the Republic of Ghana, Nana Addo Dankwa Akufo-Addo for his vision and leadership on cyber security. The Ministry also wishes to thank Members of the National Cyber Security Inter-Ministerial Advisory Council (NCSIAC) for their various roles in the development of Ghana's national cyber security. The Ministry appreciates the work of the National Cyber Security Technical Working Group (NCSTWG) and the event Planning Committee for their excellent work in organizing the National Cyber Security Week (NCSW 2017). We are grateful to our sponsors and our international partners for their support and commitment to Ghana's cyber security. The Ministry highly commends individuals, civil society and businesses for their participation in the event which has significantly contributed to awareness creation on cybercrime trends and cyber security issues facing individuals, businesses and government.

Ursula Owusu-Ekuful (MP)
Minister for Communications

ACRONYMS

AICC	-	Accra International Conference Center
AITI-KACE	-	Advanced Information Technology Institute- Kofi Annan Centre of Excellence
BNI	-	Bureau of National Investigations
BOG	-	Bank of Ghana
CERT	-	Computer Emergency Response Team
CIA	-	Central Intelligence Agency
CID	-	Criminal Investigations Department
CNII	-	Critical National Information Infrastructure
COAST	-	Computer Operations, Audit and Security Technology
COP	-	Child Online Protection
CSIRT	-	Computer Security Incident Response Team
DFID	-	The UK Department for International Development
DPC	-	Data protection Commission
ECOWAS	-	Economic Community of West African States
EOCO	-	Economic and Organised Crime Office
EU	-	European Union
FAQ'S	-	Frequently Asked Questions
FIC	-	Financial Intelligence Centre
GAF	-	Ghana Armed Forces

GDP	-	Gross Domestic Product
GLACY+	-	Global Action on Cybercrime Extended
GSMA	-	Groupe Speciale Mobile Association
ICT	-	Information and Communication Technology
IMEI	-	International Mobile Equipment Identity
ITU	-	International Telecommunications Union
KAIPTC	-	Kofi Annan International Peacekeeping Centre
KNUST	-	Kwame Nkrumah University of Science and Technology
MDA'S	-	Ministries, Departments and Agencies
MFWA	-	Media Foundation of West Africa
MOC	-	Ministry of Communications
NCA	-	National Communications Authority
NCCE	-	National Commission for Civic Education
NCSC	-	National Cyber Security Centre (NCSC)
NCSS	-	National Cyber Security Secretariat
NIA	-	National Identification Authority
NITA	-	National Information Technology Agency
NITA	-	National Information Technology Agency
PIN	-	Personal Identification Number
Q & A	-	Questions and Answers
SDG	-	Sustainable Development Goals

SGI	-	Security Governance Initiative
SOC	-	Security Operations Centre
UN	-	United Nations
UNDP	-	United Nations Development Programme
UNICEF	-	United Nations Children's Fund

REPORT SUMMARY

The National Cyber Security Week 2017 was held from 23rd to 27th October 2017 to raise awareness on cybercrime trends, cyber security issues and cyber hygiene practices as well as to dialogue and highlight on the growing cyber security issues under specific thematic areas. The event was aimed at demonstrating the government's new vision and direction on cyber security and highlighting strategies towards achieving the vision, strengthening partnerships and consolidating cyber security related activities within the country, supporting the government's digitization agenda by building resilience across all levels (people, businesses, and government) and highlighting strides made in Ghana's cyber security efforts, nationally and in line with global best practices.

The event which was opened by the President of Ghana, H.E Nana Addo Dankwa Akufo-Addo saw the inauguration of the National Cyber Security Inter-Ministerial Advisory Council (NCSIAC) by the President and the National Cyber Security Technical Working Group (NCSTWG) by the Minister for Communications, Hon Ursula Owusu-Ekuful. The President highlighted the need for Ghana to build its capacity in the area of cyber security considering the current digitalization initiatives by government. The President mentioned the national identification system, national digital addressing system and financial interoperability system as key national digitized initiatives for formalize the economy. He announced that Ghana would set up a National Cyber Security Centre (NCSC) to coordinate national cyber security response in government and the private sector.

The Minister for Communications outlined a number of activities which the Ministry of Communications has implemented to scale up Ghana's national cyber security. Some of the initiatives outlined included the adoption of a national cyber security institutional framework, capacity building programmes through the GLACY+ Project with the Council of Europe and Ghana's accession to the Budapest Convention.

The event brought stakeholders from government, the private sector, civil society, international partners, academia, students and ordinary citizens to deliberate on current cybercrime trends and cyber security issues affecting the country. Event sessions focused on five key thematic areas, including cyber security governance, conferences and workshops, child online protection, cyber security technology solutions and cybercrime awareness and cyber hygiene practices.

A total of about 1400 delegates participated in the event which was held at the Accra International Conference Center (AICC). Participants at the event recommended for increase in public awareness and capacity building to address cyber security issues. Participants suggested to both government and businesses to adopt cyber security standards and to invest in cyber security in order to protect Ghana's young and growing digital ecosystem. Ghana's international partners also emphasised on the need for international cooperation to address cybercrime challenges since cybercrime is a borderless crime. Participants recommended to government to consider the safety of children online as a national concern. Parents, teachers and care givers were advised to get involved in educating their children about the risks of the internet. The Minister for Communications, Mrs Ursula Owusu-Ekuful lauded participants for their commitment to cyber security through their participation and contribution to the event.

This report details activities organized during the week, various presentations by experts and facilitators, key discussion points during the sessions as well as recommendations from participants to improve Ghana's cyber security ecosystem.

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

I wish to congratulate you on the occasion of Ghana's National Cyber Security Week celebration. As the President of our great country, I am delighted to join all of you to create awareness and to dialogue on issues bordering on our cyber security. My government is fully committed to cyber security for a number of reasons:

• Digitalization is the backbone of my government's economic development agenda. Around the world, the adoption of connected digital services by people, businesses, and governments, has emerged as a major driver and enabler of socio-economic development. Ghana, under my presidency is embarking on a similar journey - the introduction of national identification system, digital addressing system, mobile money interoperability system and e-government initiatives such as the paperless port system, e-procurement, e-justice and e-passport are specific digitalization initiatives of

the government. My government intends to develop a smart economy to meet the aspirations of our citizens. As a result, investing in cybsr security, is an imperative rather than a choice.

• Our commitment to cyber security as a government is also linked to our obligations under the United Nation's Sustainable Development Goals (SDGs). As a co-chair of the SDG Advocates group, I am aware of the crosscutting nature of ICT and how indispensable they are for the full realisation of all the SDGs. According to the World Development Report 2016 on Digital Dividends, increase digitalization is impacting positively on developing countries. The impact of digitalization on developing economies, like Ghana is manifested in direct foreign investment, economic productivity and job creation. In addition, digitalization in government and the public sector has proven to be one of the most powerful tools to fight corruption, a canker which has the potential to derail our socio-economic transformation.

• My government is committed to cyber security because cybercrime is a borderless crime and Ghana has an obligation to secure its cyberspace in order to protect investors and to honour its commitments to the international community. In line with the above commitments, I signed the African Union Convention on Cyber Security and Personal Data Protection when I attended the 29th AU Summit in Addis Ababa. Our intention to accede to the Budapest Convention and our engagement with the United States government through the Security Governance Initiative (SGI) are other manifestations of our commitment to international cooperation as an instrument to address cybercrimes and cyber security issues.

My government is mindful of the fact that, the adoption of ICT as a foundation of our sustainable economic development will be futile without addressing the vulnerabilities emanating from the development and application of ICT systems and services across the various sectors of our economy.

According to the World Development Report 2014 on Risk and Opportunity, cyber-attacks could destroy lives, assets, trust, and social stability. Essentially, Ghana's critical infrastructures are inherently dependent on ICTs and therefore the survival of our economy and its critical systems such as power, telecommunication systems, financial sector, government services and the entire social and security system is dependent on the ability of the government to protect and secure ICT assets and systems.

Ladies and gentlemen, Ghana cannot fully reap the digital dividends associated with our adoption of ICT as a means of our socio-economic

transformation if we fail to mitigate cyber security threats. The UN SDG 9 requires our country to develop resilient infrastructures including ICT systems in order to sustain our economic development. My government therefore is resolved to address these challenges in order to safeguard our digital journey.

My government is committed to address issues of cyber security governance, capacity building, international cooperation, judicial enforcement of cybercrime legislations, research and development and implementation of relevant technical standards and safeguards to secure our digital journey.

To develop a sustainable cyber security ecosystem for Ghana, private sector involvement is key. Therefore, I wish to encourage partnerships and collaboration between the government and the private sector to facilitate information sharing, capacity building and research and development towards self-reliance.

I congratulate the Ministers for Communications, National Security, Interior, Defence, Finance, Foreign Affairs and Justice for their appointment to the National Cyber Security Inter-Ministerial Advisory Council and entreat them to work with the private sector and our international partners to scale up Ghana's cyber security readiness.

I wish all of you an exciting engagement towards securing Ghana's digital journey.

Thank you.

Vice President, Dr Mahamudu Bawumia

Statement – Minister for Communications, Hon. Ursula Owusu-Ekuful

Welcome to the National Cyber Security Week and I am delighted to have all the stakeholders here to share ideas, raise awareness and discuss our cyber security.

The Ministry of Communications has oversight responsibility for the government's digitalization agenda and is actively working to ensure the success of the initiatives being implemented by government including the national identification system, the national digital property addressing system, and a number of e-government projects. We recognise that ICTs are indispensable for development and have a cross cutting nature and are determined to do our best to enable the NPP vision of a massive transformation of the economy through technology succeed.

'It is Digitime' in Ghana. This slogan demonstrates the government's prioritisation of ICTs and the crucial role it plays in accelerated socio-economic development. Through the Ministry of Communications, Ghana is developing a robust framework to support our

digitisation. Mindful of the dangers inherent in increased usage of cyberspace however, the MOC is also leading the national effort to scale up our country's cyber security readiness.

Some initiatives we have undertaken include the following:

• Established the National Cyber Security Secretariat and appointed the Cyber Security Advisor as we begin the implementation of our National Cyber Security Policy and Strategy (NSCPS).

• Set up the National Cyber Security Inter-Ministerial Advisory Council (NCSIAC) made up of the Ministries of Communications, National Security, Justice/Attorney-General, Interior, Finance, Defence and Foreign Affairs, with private sector representatives in attendance to provide policy guidance.

• Instituted the National Cyber Security Technical Working Group (NCSTWG) with representatives from all national institutions with a mandate on cybercrime and cyber security to ensure implementation of policy decision within the various sectors.

• Initiated capacity building programmes for the criminal justice sector through Ghana's partnerships w1th the Council of Europe (GLACY+ Project) and the US Government (through the Security Governance Initiative - SGI) The Ministry of Communications has been actively engaging with government and our development partners on funding for cyber security, within the last few months.

The immediate priority of the Ministry is to undertake a national cyber security risk assessment to identify cyber vulnerabilities and priority areas that require immediate and specific interventions and we are working with the World Bank to conduct a Cyber security Capacity Maturity Model to assess the level of development of national cyber security efforts from the policy, regulatory, end-user, and other perspectives, in order to provide recommendations to government on how to enhance our cyber security readiness.

We will be setting up a National Computer Emergency Response team (CERT) to improve Ghana's cyber security emergency response readiness, review the National Cyber Security Policy and Strategy (NCSPS) to ensure it is compliant with international best practices and develop guidelines on cyber security for government and public-sector officials. This initiative will set the foundation for building a culture of cyber security across the public sector.

We will also implement a number of capacity building programmes to improve cybercrime prevention, prosecution and adjudication and cyber security awareness of individuals, businesses and government officials.

The Ministry of Communications, in collaboration with other stakeholders will set up Ghana's National Cyber Security Centre (NCSC) with full

technical and human resource capabilities to oversee national cyber security operations. This will position Ghana among the elite countries with such a facility and transform the country into a cyber security hub in the sub-region.

The government is grateful to its international partners especially the Council of Europe, the US Government and the ITU for their support for Ghana's cyber security. We also appreciate support from our local partners and stakeholders.

Ghana is on course with its international commitments on cyber security. The accession to the Budapest Convention is currently before Cabinet and ratification by Parliament is expected later in the year. The President has signed the Africa Union treaty on Cyber Security and Personal Data Protection and it is imperative that we work towards achieving the objectives and targets of the Convention. We need to operationalize the ECOWAS Directive on Cybercrime to ensure cross-border investigations and prosecutions of cybercrimes within the sub-region.

I congratulate the members of the event planning committee for their commitment and the enormous amount of work they have put in to ensure the success of this event. We are grateful to all our sponsors for their kind donations which have also helped make this cyber security week happen.

We will build an effective harmonized national cybersecurity strategy only with multi stakeholder engagement and the commitment shown by our various stakeholders so far, gives me the confidence that we can do it. It is an exciting time for our cyber security as a country. The government is committed and it has already set the pace for the country's cyber security development. I therefore urge all of you - individuals, businesses, organizations and our international partners to get involved in our quest to secure Ghana's digital journey.

Thank you.

Hon. George Andah

Deputy Minister

Hon. Vincent Sowah Odotei

Deputy Minister

Mr. Issah Yahaya

Chief Director

MEMBERS OF THE NATIONAL CYBER SECURITY INTER-MINISTERIAL ADVISORY COUNCIL (NCSIAC)

HON. URSULA OWUSU-EKUFUL
Minister for Communications

HON. GLORIA AFUA AKUFFO
Minister for Justice & Attorney General

HON. KEN OFORI-ATTA
Minister for finance & Economic Planning

HON. AMBROSE DERY
Minister for the Interior

HON. SHIRLEY AYORKOR BOTCHWAY
Minister for Foreign Affairs

HON. DOMINIC NITIWUL
Minister for Defence

HON. ALBERT KAN-DAPAAH
Minister for National Security

Statement – National Cybersecurity Advisor, Albert Antwi-Boasiako

I wish to welcome you to the 2017 edition of the National Cyber Security Week! It is exciting that we have joined the global cyber community to celebrate this national event. I am particularly excited that we have different stakeholders, across all levels of the cyber security ecosystem representing at this event. This is a clear manifestation of Ghana's multi-stakeholder approach towards addressing the country's cyber security challenges.

Ladies and gentlemen, it is exciting time for cyber security development in Ghana. The current level of digitalization - both in the public and the private sectors of our economy requires concerted efforts to scale up our cyber security, which is rated below 35% by the International Telecommunications Union (ITU). ITU's Global Cybersecurity Index Report for 2017 provides a good background of Ghana's cyber security landscape - across multiple domains, including - the state of Ghana's

national cybercrime legislations and enforcements, current technical measures, cyber security institutional frameworks, capacity building and cooperation, among others.

The United Nations Sustainable Development Goals (SDGs) require countries to adopt innovation and to secure critical infrastructures including ICT infrastructures. Current trends in Ghana's digitalization is consistent with the requirements of the SDGs. Therefore, it is imperative that our country invests in cyber security.

As the Cyber Security Advisor to the Government, I have set out five key broad objectives, towards improving our country's cyber security readiness:

- Develop an independent, sustainable multi-stakeholder institutional framework for Ghana's cyber security based on international benchmarks and existing institutional arrangements;

- To develop our national cyber security capabilities to protect our critical infrastructures and to respond to both existing and emerging cyber threats;

- To support national institutions with a mandate on cybercrime/cyber security to develop their cybercrime and cyber security response capabilities, consistent with their mandates.

- To foster cyber security cooperation and partnerships at all levels (In-Country, Sub-Regional and International).

- To develop a culture of cyber security in Ghana (at the individual, organizational and government levels).

These objectives are the drivers to secure Ghana's digital journey, which can only be achieved through continuous in-country engagements (public and private sector engagements) and partnerships with Ghana's international friends.

I therefore invite all and sundry to join the new vision on cyber security and to stay on board as we drive Ghana's cyber security agenda forward.

Thank you.

Albert Antwi-Boasiako
National Cybersecurity Advisor
Securing Ghana's Digital Journey

MEMBERSHIP OF THE NATIONAL CYBER SECURITY TECHNICAL WORKING GROUP (NCSTWG)

The following are governmental representatives on the National Cyber Security Technical Working Group (NCSTWG):

- NATIONAL COMMUNICATIONS AUTHORITY
- NATIONAL INFORMATION TECHNOLOGY AGENCY
- NATIONAL IDENTIFICATION AUTHORITY
- DATA PROTECTION AGENCY
- BANK OF GHANA
- NATIONAL SECURITY
- ECONOMIC AND ORGANISED CRIME OFFICE
- FINANCIAL INTELLIGENCE AGENCY
- BUREAU OF NATIONAL INVESTIGATIONS
- CRIMINAL INVESTIGATIONS DEPARTMENT
- RESEARCH DEPARTMENT
- GHANA ARMED FORCES
- JUDICIAL SERVICE
- MINISTRY OF JUSTICE AND ATTORNEY GENERAL'S DEPARTMENT
- MINISTRY OF FOREIGN AFFAIRS

Non-governmental stakeholders including representatives from the Academia, Business Community, Civil Society and International Organizations also serve on the NCSTWG.

DAY 1

FORMAL OPENING & CYBER SECURITY GOVERNANCE

SESSION A:

SPEECH BY NATIONAL CYBERSECURITY ADVISOR – ALBERT ANTWI-BOASIAKO

His Excellency, the President, Nana Addo Dankwa Akufo-Addo

Hon Minister for Communications, Mrs Ursula Owusu-Ekuful

Ladies and Gentlemen,

I'm very pleased to welcome you to the 2017 edition of the National Cyber Security Week! It is exciting that we have joined the global cyber security community to celebrate this national event. The presence of different stakeholders at this gathering is a clear manifestation of Ghana's multi-stakeholder approach towards addressing our county's cyber security challenges.

This gathering has been possible because of collective efforts of a number of individuals and institutions. I wish to recognize the leadership of Hon Minister for Communications – Mrs Ursula Owusu-Ekuful for her

leadership and other sector ministers for their direct involvement in driving this event. The Ministry of Communications has been outstanding in providing direct support and institutional guidance for the programme and I wish to commend members of the planning committee, event partners, sponsors and our international friends for their commitment to Ghana's cyber security through this programme.

Ladies and gentlemen, Ghana's cyber security readiness is rated below 35% by the ITU and this calls for serious business – across all levels – people, businesses and the government. Indeed, the government has a responsibility to lead national efforts to address this huge gap between our ICT development as a country and our cyber security readiness.

As Advisor on Cyber Security to Government, I have a responsibility to help bring stakeholders together on our journey to secure Ghana's investment in digitalization. The National Cyber Security Week is one of such initiatives to achieve the above stated objective.

The MOC has set the following five key broad objectives, towards improving our country's cyber security readiness:

a) Develop an independent, sustainable multi-stakeholder institutional framework for Ghana's cyber security based on international benchmarks and existing institutional arrangements;

b) To develop our national cyber security capabilities to protect our critical infrastructures and to respond to both existing and emerging cyber threats;

c) To support national institutions with a mandate on cybercrime/cyber security to develop their cybercrime and cyber security response capabilities, consistent with their mandates.

d) To foster cyber security cooperation and partnerships at all levels (In-Country, Sub-Regional and International).

e) To develop a culture of cyber security in Ghana (at the individual, organizational and government levels).

These objectives are the drivers to secure Ghana's digital journey. I therefore invite all of you – our stakeholders to join the new vision on cyber security and to stay on board as we drive Ghana's cyber security agenda forward.

Thank you.

SPEECH BY ECOWAS REPRESENTATIVE –
MR ISAIAS BARRETO DE ROSA

His Excellency the president of the Republic of Ghana

Ladies and Gentlemen

It is with immense pleasure that, on behalf of the ECOWAS Commission, I take the floor during the opening ceremony of this National Cyber security Week here in Accra, under the theme "Securing Ghana's Digital Journey". This occasion also affords me the opportunity to thank the Government of Ghana, who is always committed to supporting the Economic Community of West African States, in the implementation of its programs and projects to achieve our common regional integration goals.

Permit me also to thank the Government of Ghana for extending an invitation to the ECOWAS Commission to share its perspectives on the Community Directives on fighting cybercrime.

The ECOWAS vision is to create an integrated West Africa, with free movement of people, free movement of goods and free movement of services, including ICT services. We want to promote regional integration and economic development of our

region in a peaceful and in a democratic environment.

As we all know, ICT continues to be a catalyst for innovation and its application cuts across many sectors of cooperation among our Member States. It is our belief at ECOWAS that ICT is the engine of our regional integration process in West Africa as we move from an ECOWAS of States to an ECOWAS of people. Our ultimate goal as far as ICT is concerned, is to create a single digital market in West Africa.

However, as we all know, ICT and broader access to the Internet raise many challenges in terms of cybersecurity and cybercrime. Therefore, ICT cannot be the engine of our regional integration and development process without a safe cyber environment in our region. There can be no single digital market in the region without the presence of a secure cyber environment.

All ECOWAS Member States need therefore to work together in fighting cybercrimes and in addressing cyber security issues given the sheer borderless nature of cybercrime and the increase in malicious cyber related activities which are currently costing our Governments millions of dollars in losses.

In order to address the increase in these malicious cyber-activities within the region and given the need of protecting the ECOWAS cyberspace the ECOWAS Commission decided to include a number of cyber related activities in its programmes to enhance cyber security and to fight cybercrime in West Africa. Amongst these activities we included for instance capacity building for judges, prosecutors, law enforcement agents and cybersecurity experts; we included the establishment of national CERTS and development of cyber security strategy for all ECOWAS Countries, etc.

A good cyber legislation is also an important component of this efforts to create a safer cyber environment within the subregion. That is why we adopted three (3) Community Acts addressing these issues: the Supplementary Act on Electronic Transactions, the Supplementary Act on Personal Data Protection and the Directive on Fighting against Cybercrime.

I would like to take this opportunity to congratulate the Government of Ghana in its domestication of these Community texts as well as its accession to the "Budapest Convention on Cybercrime" and "Data Protection Convention 108" of the Council of Europe. I also would like to congratulate the government of Ghana for the establishment of a national Computer Emergency Response Team (CERTs).

This National Cyber Security Week will

foster close collaboration and interaction with all relevant stakeholders including public and private entities that are involved in cybersecurity and cybercrime issues.

Moreover, this week will also be a good opportunity to sensitize the citizens of Ghana on Cybersecurity awareness in order to improve each and everyone's digital habits.

The ECOWAS Commission is therefore very much in support of other Member States replicating this type of initiative as cybersecurity remains a borderless phenomenon and coordinated actions are truly required.

At this juncture I would like to sincerely express the gratitude of the ECOWAS Commission to **His Excellency Nana Addo Dankwa Akufo-Addo,** President of the Republic of Ghana for his commitment on enhancing cybersecurity and cooperation on cybercrime. Indeed, high political level commitment is key to tackle cybercrime.

In conclusion, permit me to express the hope of the ECOWAS Commission that this gathering will serve as an avenue to promote the need for collective responsibility not only in Ghana, but also across the region, towards the coordination of cyber security issues and the fight against cybercrime.

This is also an opportunity for us to garner information, to facilitate discussions and to come up with solutions regarding the cyber security issues that we are all facing.

I wish you all a very fruitful National Cyber Security Week and I thank you for your kind attention.

SPEECH BY COUNCIL OF EUROPE-
MR. MANUEL DE ALMEIDA PEREIRA

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

The Minister of Communications of the Republic of Ghana, Ms Ursula Owusu-Ekuful

Ladies & Gentlemen, my dear friends

It's with great pleasure that the CoE stands here today in this very important event, not only for Ghana but also for the entire African continent as a model to follow. We live in very dangerous times today. The world we knew 20 years ago has changed dramatically and criminality has evolved to a degree that tends to be higher than the one where Law Enforcement stands.

Forget the old, but efficient, manhunt where the face in a list could be a deterrent to criminality and an effective way to pursue and arrest criminals; forget publicly identified criminals whose faces could be known by everyone; forget the old way of stealing a wallet in the street where the criminal only wants the money and later ditches the wallet in some corner. Forget the need of bombs to destroy infrastructures, cities and countries.

Crime is now Cybercrime!

Cybercrime has no face in first hand. 95% of the crimes have a component of cybercrime through the use of electronic means. Cybercrime can steal your money while you are sleeping, in a meeting or even enjoying time with your family. Cybercrime can destroy your life, the life of all your dear people and your children without you knowing until is already too late.

Cybercrime Mr. President, ladies & gentlemen, can destroy your government, can stop the functioning of an entire city or even shut down an entire country.

Cybercrime can pose a threat to serious and critical infrastructures such as Nuclear Power Plants, energy in general, release of toxic agents and destroy life and society as we know!
Cybercrime can pose a serious threat to the future of our children. They are the reason we get up every morning, go to work and fight every day for giving them what they need to win in this world we live!

Then what shall we do? What shall we do to be at least in the same degree of the cybercriminals? What shall we do to overrun this dark and tragic scenario I have just painted?

A few words: Cooperation, Commitment, Joint Actions and capacity building to its maximum extent.

Countries should put aside economic and political interests when fighting cybercrime; they should put aside the fear of losing their sovereignty when fighting cybercrime; and why? Because, eventually this may happen anytime to any of them and when A asks B for help, B must know that one day he may ask A also for help.

Countries, governments, law enforcement institutions and all criminal justice entities must join efforts in tackling this phenomenon.

Capacity building is an essential key to fight cybercrime, but not just wild building of capacities. If A trains B, it must be ensured that B will be able after to train C and D and so on and so forth. If a training is delivered to police officers, ensure that live operations are discussed. If a country wants to have legislation against cybercrime, ensure that the legislation is harmonized with your neighbors, within the region where you are inserted. An harmonized legislation makes easier international cooperation, makes easier having one voice against cybercrime.

If you, country X or institution Z have effective countermeasures against cybercrime, share them with your neighbors, share them with the international community, with the entire world. Criminals must know we are in their path that we are watching

them!

If country A needs evidence that is located in country B, do not shield behind the sovereignty of your State to hamper the access; instead, help your neighbor, help anyone who needs.

The Council of Europe through the use of the Budapest Convention is trying to create the conditions to fight Cybercrime in a very effective manner. Putting international and regional organizations together, ensuring countries have their legislation aligned, ensuring training is delivered with a multiplication effect and, after all, ensuring that we are living in a community of TRUST.

The GLACY+ project may be a drop in the ocean but with many drops like this we will build an effective countermeasure to ensure that the desired step is achieved.

I am happy to know, Mr President, that your country and your government is pursuing the right path of acceding the Budapest Convention, taking part in the GLACY+ project as a priority country, having a great national team led by my good friend and colleague Albert Antwi-Boasiako who are directly collaborating with the Council of Europe in the implementation of all activities foreseen under the GLACY+ project which I will have the opportunity and the pleasure to address all of you about tomorrow.

I am happy to know Mr President that your country and your government looks ahead, far ahead in the fight against cybercrime and creating a mark in the ECOWAS region as an example to follow and I am here to acknowledge this in front of all of you.

I finish as I started: We live indeed in very dangerous times today! But fortunately, there is hope; there is a will and Ghana is in the frontline in the fight against cybercrime.

Mr. President, ladies and gentlemen, thank you for your attention.

SPEECH BY UNICEF REPRESENTATIVE-
MRS. RASHAN MUNTAZA

Your Excellency, President Nana Akufo-Addo,

Honourable Ministers,

All Dignitaries,

Ladies and Gentlemen,

It is a great pleasure to represent the United Nations this morning at the launch of National Cyber Security Week. Digital technology and the internet has transformed the way in which we communicate, educate and mobilise in ways generations.

We have seen how digital technology is changing lives and life chances in Ghana. If leveraged in the right way and accessible for everyone, digital technology can be a game changer - particularly for Ghanaian children being left behind. Not only does it provide skills to succeed, adolescent girls and boys in particular are at the forefront of this important technology as both consumers and creators of digital contents in Ghana.

However as we seek to bring

technology to more of Ghana, we want to ensure that children, young people, men and women are being protected from threats. The United Nations is committed to making the Internet more secure, safer and trustworthy, so that every child, woman and man can benefit for its good.

A common United Nations-wide framework on cybersecurity and cybercrime has been established to enhance coordination amongst UN agencies in their response to governments. It is also designed to support up-to-date national cyber security policies and regulatory framework in the rapidly evolving digital technology environment.

While the legal framework in Ghana seems to be stronger in terms of online security, the implementation of this remains a challenge. We hear of cases of child pornography and blackmailing of teenagers far too regularly. Indeed there is a trial currently underway of two men in Accra charged with child pornography and blackmailing a 14 year old student.

If we don't act now to keep pace with rapid change, online risks may make children more vulnerable to exploitation, abuse, and even trafficking – as well as more subtle threats to their wellbeing.

The United Nations is delighted to be playing a role in this National Cyber Security Week. Later today stakeholders at this event will have an opportunity to participate in the National Dialogue for Digital Transformation in Ghana roundtable. This is being organized by UNDP, the Government of Ghana, GSMA, and the British Government.

Meanwhile later in this week, UNICEF in collaboration with the Ministry of Communications and the Ghana Telecommunications Chamber will be organizing a stakeholder conference with the aim of facilitating a collective industry action to create a safer and age-appropriate digital environment in Ghana.

In addition, UNICEF and ITU have released Guidelines for the Industry on child online protection. The UN System in Ghana is committed to supporting the Government of Ghana in making sure that these guidelines are adopted by the telecommunication industry. Further, UNICEF and the telecommunications body GSMA release Guidelines on Company Policies and practices to remove online child sexual abuse material.

Meanwhile, the GSMA Mobile for Development Foundation partnership with UNDP is harnessing the power of mobile technology to accelerate the implementation of the SDGs. UNDP and GSMA will bring together CEOs of mobile operators and policy makers to identify solutions for priority national development challenges, through

mobile technologies in Ghana and Bangladesh.

We congratulate the Government of Ghana for leading the way in safeguarding the cyber security of the nation. By putting in place the necessary functional governance structures, in collaboration with key partners like the National Communication Authority, the Chamber of Telecommunications and the Data Protection Commission we are on our way to a safer online system for Ghana. Yet to fully tackle this ever-increasing threat, we require concerted effort from all stakeholders.

And so we look forward to seeing how coming together over this important National Cyber Security Week we can move Ghana one step closer to embracing a safer digital arena.

SPEECH BY US AMBASSADOR TO GHANA-
MR. ROBERT P. JACKSON

Your Excellency President Nana Addo Dankwa Akufo-Addo,

Honorable Minister of Communications Ursula Owusu-Ekuful,

Colleagues from the Diplomatic Corps and the U.S. Mission,

Distinguished Ladies and Gentlemen,

Good morning. I'm delighted to see so many friends, business leaders, and members of the Government of Ghana here today. Thank you to the Minister of Communications for inviting me to participate in and support Ghana's National Cybersecurity Week Celebration. I also would like to thank Albert Antwi-Boasiako, the Cyber Security Advisor, for his good work over the past several months. Through our joint efforts and the Security Governance Initiative, we are fortifying Ghana's cybersecurity and capacity to fight cybercrime and strengthening the administration of justice.

We all know that cybersecurity issues

can have far-reaching effects. As President Trump noted in May, the United States must work with our allies and partners to create a "globally secure and resilient Internet," as our economic, political, and civil societies cannot thrive if we fail to protect our information infrastructure.

Businesses, governments, and private citizens have come to depend on an Internet that is open, secure, and reliable. Digital technology and connectivity are critical to our daily lives and we must act to protect against malicious actors that use the Internet to commit crimes.

Cyber threats come from state-sponsored actors, criminal organizations, and individual actors. They can harm our security, do substantial damage to our infrastructure, and have an enormous impact on our economies. And there are threats that target internet users like you and me. A main concern in Ghana is debit card fraud. Criminals target retail outlets – stores, restaurants, and gas stations – where they steal our PIN numbers for their own use or to sell to others. Romance scams perpetrated via the Internet are also a real threat to ordinary people. Almost every day an American contacts my Embassy to say that "the fiancé(e)" they met on the Internet had reported being involved in an accident and needing thousands of dollars for medical bills. They sent the money and have not heard from the fiancé since. These fraudsters, often referred to as "sakawa boys", victimize people across the world and hurt Ghana's international reputation. The anonymity offered by the Internet requires users everywhere to be vigilant and take steps to verify and protect online information. As we develop responses to identified vulnerabilities, criminals are already looking to exploit another security gap. No single government or organization has all the resources and expertise required to combat the advanced and persistent cyberattacks that are being launched today. A vibrant partnership between the public and private sectors is essential to the implementation of an effective cybersecurity policy.

Defending against the threat of cybercriminal activity requires a comprehensive and collaborative approach. Ghana is collaborating with international partners to combat cybercrime. Sharing technical expertise and implementing targeted training to conduct a critical infrastructure risk assessment to develop standard operating procedures for the newly created National Security Technical Working Group are critical. Ghana's Computer Emergency Response Team (CERT) stands ready to respond to cyberattacks. From the U.S. experience, I can tell you that staffing and resourcing a CERT is difficult, but it is also vital. I encourage everyone here – public, private and nonprofit – to work with CERT to secure their networks.

It is also vitally important to foster a whole-of-government approach to effectively address these challenges, but there is no "one size fits all" solution to every challenge. Ghana's cybersecurity strategy must be tailored to Ghana's own realities, aspirations, and goals. It is ultimately up to the Government of Ghana, with input from the private sector and civil society, to articulate its objectives, define its priorities, and allocate resources to address the nation's cyber concerns. Ghana has already taken significant steps in this pursuit. The government developed a National Cybersecurity Policy and Strategy, which is a living document that can be built upon as new technology and attack vectors develop.

We applaud Ghana's efforts to accede to the Budapest Convention on Cybercrime, an international treaty designed to address cybercrime by harmonizing national laws and increasing cooperation among nations. This is a significant step in bringing Ghana's already strong cybersecurity legal framework into greater alignment with the international community. When completed, it will form a foundation for our robust cooperation on combatting cyber-crimes against citizens across borders.

Mr. President, Ministers, Ladies and Gentlemen, as we combat cybercrimes, we are mindful of the great benefits that technology offers in connecting people around the world. In fact, internet freedom is a right as well as a necessity for all nations and citizens around the world to prosper. Cyber risks do not outweigh the benefits of an open, secure, and reliable Internet, nor should they discourage businesses and people from using the Internet and digital media. The Internet is a powerful tool to express opinions, share information, and expose corruption. It is also the backbone of the innovative space that we all know as the digital economy.

I am pleased that the Government of Ghana is committed to doing the hard work of identifying and addressing cyber threats to ensure the people of this nation can fully and more securely benefit from their right to access to the Internet and the fruits of information technology. This National Cybersecurity Week Celebration is an excellent time to bring cybersecurity stakeholders together to not only discuss Ghana's cyber threat environment, but also to develop innovative solutions that mitigate cyber threats and promote a culture of cyber awareness. The United States of America is proud to support Ghana's efforts to strengthen its cybersecurity capacity to enable Ghanaians to educate and prepare themselves through internet access to successfully compete in this 21st century economy, thereby lifting this nation's economy to new heights. Together, we can make our shared vision a reality.

Thank you.

SPEECH BY MINISTER FOR COMMUNICATIONS-
HON. URSULA OWUSU-EKUFUL

His Excellency, the President, Nana Addo Dankwa Akufo-Addo

Ladies and Gentlemen,

I am delighted to welcome you to this edition of Ghana's National Cyber Security Week event. As the Chief Host of the event, it is my duty to welcome both our international visitors and residents to this occasion which marks the beginning of the journey towards securing our digital economy. The observation of the National Cyber Security Week in Ghana, in line with global practices, has become necessary in view of government's new vision and strategy to scale up Ghana's cyber security.

In July this year, the President directed the Ministry of Communications to oversee the implementation of Ghana's National Cyber Security Policy & Strategy (NCSPS). It is against this background that my Ministry set up the National Cyber Security Secretariat and appointed a Cyber Security Advisor to provide a focal point for the convergence of all cyber security activities and to coordinate programmes developed or being implemented by the different entities and agencies of government and the private sector within the context of

Ghana's cyber security policy and strategy.

Ghana's National Cyber Security Week event which has brought all of us here together is one of several initiatives being implemented by the Ministry of Communications in collaboration with relevant ministries and agencies as part of the implementations of the policy.

Ladies and gentlemen, the weeklong event which is under the theme – **Securing Ghana's Digital Journey** is significant not only for government but for the entire Information Technology ecosystem of Ghana. The Ministry of Communications has oversight responsibility for the government's digitalization agenda and is actively working to ensure the success of the initiatives being implemented by government including the national identification system, the national digital property addressing system, and a number of e-government projects.

We have seen significant increase in the adoption of technology by businesses across all sectors. For example, the financial sector has seen a number of e-banking products and services introduced within the last few years. The growing use of smartphones and internet penetration across the length and breadth of this country is a manifestation of ICT growth around which the government's digitalization policy revolves. As a government, we recognise that ICTs are indispensable for development and have a cross cutting nature and are determined to do our best to enable the NPP vision of a massive transformation of the economy through technology succeed. Ladies and gentlemen, It is digitime' in Ghana and the current ICT transformation is impacting on everybody - people, businesses and government.

Mindful of the dangers inherent in increased usage of cyberspace however, the Ministry of Communications is also leading the national effort to scale up our country's cyber security readiness.

The National Cyber Security Week which focuses on five key thematic areas, including **Cyber Security Governance, Workshop Presentations, Child Online Protection, Cyber Security Technology Solutions and Cybercrime/Cyber Security Awareness** is aimed at creating awareness on cybercrime trends and cyber security issues across all levels – people, businesses and government, in line with the theme for the event. This event is also an occasion to demonstrate the government's new vision and direction on cyber security and highlight strategies towards achieving the vision.

Ladies and gentlemen, this year's celebration highlights on knowledge

and information sharing among the various stakeholders within the cyber security ecosystem. In the light of this, we have brought cyber security service providers on board – both local and international providers to showcase what they are doing and the services they are providing to contribute towards Ghana's cyber security.

His excellency, at this point I wish to account for what my Ministry in collaboration with other ministries and representatives from stakeholder institutions have achieved so far and other specific initiatives being implemented towards stepping up Ghana's security:

- The Ministry of Communications has established the National Cyber Security Secretariat and appointed the Cyber Security Advisor who is currently overseeing the implementation of our National Cyber Security Policy and Strategy (NSCPS).

- As part of Ghana's cyber security institutional framework, a National Cyber Security Inter-Ministerial Advisory Council (NCSIAC) – with representations from the Ministries of Communications, National Security, Justice/Attorney-General, Interior, Finance, Defence and Foreign Affairs and private sector representatives has been set up in to provide policy guidance for Ghana's cyber security.

Inauguration of members of the National Cyber Security Technical Working Group by Mrs. Ursula Owusu-Ekuful, Hon. Minister for Communications

• I have instituted the National Cyber Security Technical Working Group (NCSTWG) with representatives from all national institutions with a mandate on cybercrime and cyber security to ensure implementation of policy decisions within the various sectors.

• The Ministry of Communications has facilitated capacity building programmes for the criminal justice sector through Ghana's partnerships with the Council of Europe under the GLACY+ Project.

• The Ministry of Communications has engaged with the United States Government through the Security Governance Initiative – SGI on a number of cyber security governance related issues including workshops and cyber security stakeholder mapping exercises – this engagement is to support effective alignment of the various roles of stakeholders in the implementation of Ghana's cyber security policy and strategy.

• The Ministry of Communications through the National Cyber Security Secretariat is coordinating a number of cyber security initiatives with various institutions – including a project to enhance operational capability of the Computer Emergency Response Team (CERT) for the National Information Technology (NITA) – which will help protect government's digitalization projects. A Computer Emergency Response Team (CERT) is also being set up at the National Communications Authority (NCA) to improve cyber security and response readiness within the telecommunications sector. In line with the national cyber security policy and strategy, the Ministry through the National Cyber Security Secretariat is collaborating with the Bank of Ghana on a Directive on cyber security to improve cyber security in the banking sector, considering the high incidents of cyber-facilitated attacks targeting banks and other financial institutions in the country. Most of these initiatives shall be completed by the end of the year.

• The Ministry of Communications has also secured a 4 million US Dollar credit from the World Bank for cyber security. In addition, Government of Ghana is making financial commitments for cyber security in line with the new vision of the government towards cyber security.

His Excellency, my Ministry has identified other priorities and I am currently engaging with other ministries, agencies, the private sector and our international friends for implementation. One of our immediate priorities is to undertake a national cyber security risk assessment to identify cyber vulnerabilities and priority areas that require immediate and specific interventions.

The Ministry is also collaborating with the World Bank to conduct a Cyber

Security Capacity Maturity Model to assess the level of development of national cyber security efforts from policy, regulatory, end-user, and other perspectives, in order to provide recommendations to government on how to enhance our cyber security readiness.

The Ministry is also engaging with relevant stakeholders to review the National Cyber Security Policy and Strategy (NCSPS) to ensure it is consistent with international best practices considering latest advances in information technology and its impact on all sectors of our lives. The Ministry, through the National Cyber Security Secretariat in collaboration with its stakeholder partners will develop guidelines on cyber security for government and public-sector officials. This initiative will set the foundation for building a culture of cyber security across the public sector. Under my leadership, the Ministry will implement a number of capacity building programmes to improve cybercrime prevention, prosecutions and adjudication and cyber security awareness of individuals, businesses and government officials.

In line with global trends, the Ministry of Communications will set up Ghana's National Cyber Security Centre (NCSC) with full technical and human resource capabilities to oversee national cyber security operations. A National Computer Emergency Response Team (CERT) shall be set up and operate within the Centre. The operations of all constituency CERTs shall be integrated into the National CERT. This will represent one of our national cyber security capabilities as a country. As a result, this development will position Ghana among the elite countries with such a facility and transform the country into a cyber security hub in the sub-region.

Ghana is on course with its international commitments on cyber security. The accession to the Budapest Convention is currently before Cabinet and ratification by Parliament is expected later in the year. The President has signed the African Union Convention on Cyber Security and Personal Data Protection and it is imperative that we work towards achieving the objectives of the Convention. We need to operationalize the ECOWAS Directive on Cybercrime to ensure cross-border investigations and prosecutions of cybercrimes within the sub-region. Other initiatives including collaboration with international technology providers such as Facebook, Microsoft and Google are being pursued as part of government's efforts to improve international cooperation on cybercrimes.

The government is grateful to its international partners especially the Council of Europe, the US Government, UNDP and the ITU for their support for Ghana's cyber security. We also appreciate support

from our local partners and stakeholders especially sponsors who provided direct financial assistance to make this gathering possible.

I also congratulate members of the event planning committee for their commitment, dedication and the enormous amount of work they have put in to ensure the success of this event.

We will build an effective harmonized national cybersecurity strategy only with multi stakeholder engagement and the commitment shown by our various stakeholders so far, gives me the confidence that we can do it. It is an exciting time for our cyber security as a country. The government is committed and it has already set the pace for the country's cyber security development. I therefore urge all of you – individuals, businesses, organizations and our international partners to get involved in our quest to secure Ghana's digital journey.

I wish all of you a successful National Cyber Security Week celebration and remember to stay safe online!

Thank you.

KEYNOTE ADDRESS BY THE PRESIDENT OF THE REPUBLIC OF GHANA –

NANA ADDO DANKWA AKUFO-ADDO

AT THE OPENING OF THE NATIONAL CYBER SECURITY WEEK AND THE INAUGURATION OF THE NATIONAL CYBER SECURITY INTER-MINISTERIAL ADVISORY COUNCIL (NCSIAC)

ACCRA INTERNATIONAL CONFERENCE CENTRE (AICC)
ACCRA, MONDAY OCTOBER 23, 2017

The Minister for Communications, Hon Ursula Owusu-Ekuful

Ministers for Communications from our Sister Countries – Mali, Benin, Burkina Faso

Members of the National Cyber Security Inter-Ministerial Advisory Council (NCSIAC)

African Union Representative

ECOWAS Representative

Representative from the Council of Europe

United States Ambassador to Ghana

Members of the Diplomatic Corps

Members of Parliament

Heads of Security & Government Agencies

Members of the National Cyber Security Technical Working Group (NCSTWG)

Media personnel present

Ladies and Gentlemen,

I am delighted to be here to join you at this very important gathering on cyber security. I welcome our brothers and sisters from our neighbouring countries. The subject that has brought us together here is a good example of a problem that knows no boundaries and has no respect for geography or passports.

I suspect I do not exaggerate if I state that all aspects of our lives are now ruled by information technology. We communicate with each other electronically, we gather and store information electronically, we conduct business electronically and I am told our young people are more likely to meet their partners on the internet or online than at parties or social gatherings.

There is a lot to amaze and shock about the wonders of modern technology. I am amazed that the smartphone you and I have in our hands today is far, far more powerful than the computers that landed man on the moon. I am no less intrigued that I have over three

thousand "friends and followers" and a recent tweet wishing Shatta Wale happy birthday in pidgin would go viral.

The cars that we drive today are more computers on wheels than the mechanical beasts we used to drive. We are not exactly yet at the driverless-car stage, (and I don't know how those of us who do love to drive would deal with that, but I believe we shall deal with that when we get there), but the cars are equipped to take us to addresses we have never been to and help us avoid traffic jams.

It is no exaggeration to state that those who control the cyber space, control the world. Ladies and gentlemen, the many wonders of technology come with attendant dangers as well. Now we know that a bank robber need never take a gun into the banking hall or dig underground tunnels into the vault.

An electronically savvy bank robber, sitting at a computer that hacks into the bank's system can and do regularly cause more chaos and more damage than the old robbers with their guns. They do not even need to be in the same geographic space as the bank, and in truth the bank records are also probably in the clouds and not in the geographic space we identify as the bank.

The danger posed by a breach in security of our cyber-ruled world can be even more dramatic. We have heard of the continuing complaints from the most powerful nation on earth that their elections were interfered with, and there were no invading armies or tanks.

What we once read as science fiction is present day reality. We are making phone calls from the farms and we are sending and receiving money with a few clicks on our mobile phones. We can pay electricity, water and other bills through innovative applications on our phones. It is still a bit difficult for some to accept, but procedures at our port in Tema are now paperless and the Long Room has lost its terror!

A few days ago, we in Ghana finally joined the rest of the world in getting property addresses, thanks to technology. And with the addresses, the long running saga of national identification will be finally resolved.

As we all know, the Vice President and his team of economic management people are determined to formalize our economy and drag us into the modern way of conducting business.

The more we formalize the various aspects of our activities and gather and store information, the more urgent the need for cyber security. For many people, especially, the young amongst us, their virtual life and existence is now very much their reality.

They give away information about themselves voluntarily all the time: from locations, what they like to eat, photographs taken at inconvenient times, their innermost thoughts and all the information that could be used to build an identity. They give them out, I suspect because electronic data is not

tangible and human beings cannot feel data.

Sometimes, all that the breach of cyber security means is that there will be a few embarrassed faces as something we think we were saying or doing behind closed doors is made public. Other times, the breach of cyber security could trigger a banking crisis, a medical emergency, a diplomatic incident, or bring everyday life to a stop. Sometimes it might be a genuine mistake that causes the breach but more often than not, the causes are malicious and deliberate. I expect that this meeting takes into account all these varied sources of insecurity.

Unfortunately, developing countries are the most vulnerable to cyber-attacks because of the fragile nature of our IT systems.

There are new and evolving threats targeting communications and data networks as the world develops towards a digitized global economy. Organized criminal networks have stepped up their activities targeting ICT systems and services. Computer worms, viruses and other malware programmes have been developed as destructive weapons to computer systems and critical information infrastructures, and ransomwares that have been developed to extort huge sums of money from corporations and government institutions.

The introduction of our national identification system, the digital addressing system, e-payments, digital financial services and the various e-government initiatives being undertaken by the government in addition to other critical services constitute critical national information infrastructures as these systems and services form the backbone of our very existence as a country.

The survival of the economy and its critical systems such as power, telecommunication, financial sector, government services and the entire social and security system is dependent on the ability of the government to protect and secure ICT assets and systems.

Ladies and gentlemen, the last few months have recorded major global cyber incidents. For example, the National Health Insurance System of the United Kingdom was brought down, albeit temporarily. There were very anxious days in the Ukraine as much of their most critical infrastructure including the banking sector and national grid systems came under attack.

Whether these attacks were orchestrated by state-sponsored actors or by third party malicious hackers, they affected the survival of those economies. The lesson is clear and unambiguous: cyber security is paramount and we must improve our cyber security emergency response readiness.

But we should not delude ourselves into thinking that these dangers are only from outside our borders. Our country is

experiencing its fair share of cybercrime and cyber security challenges that are home grown. Cybercrime has become one of the most common and pervasive crimes in Ghana. Ghana now counts among prevalent crimes in the country, website defacements, hacking into banking systems and critical databases, ransomware attacks, e-mail fraud, identity theft, SIM box fraud, cyber fraud – normally called Sakawa or 419 and increasingly, identity theft to impersonate government and public officials and abuse on social media. Children are also facing increasing risks on the internet – including risks associated with improper contacts, conduct and contents on the internet.

The task that we face therefore is urgent. The fast pace at which technology is developing means that often the law enforcement officials are struggling to keep pace with the law-breakers. It is critical therefore that those in charge of protecting our ICT security are well equipped with the knowledge and the expertise to do so. The tools and competencies with which we fight crime must necessarily therefore change. We need to train and have a well-equipped corps of cybercrime fighters, but we should go further than that. I dare say it is time to take another look at the qualifications that we require in a policeman for example. If what we used to define as crime has changed, then we should redefine the crime fighters as well. We cannot and should not have policemen who are not computer literate; sending them out into the streets or to man a station without such competencies is to send them out gravely handicapped.

Ghana is transitioning from a traditional economy into an IT-enabled economy. The Ministry of Communications is working on a number of e-government initiatives including e-justice, e-immigration, e-passports, e-procurement and tertiary education connectivity initiatives among others, to transform our public-sector services. The proceedings of Cabinet will not be left out. It is digitime! The private sector is modernizing as well.

We are well on our way to developing a smart economy to meet the aspirations of our citizens.

But according to a World Bank research document – **Cyber Security: a New Model for Protecting the Network,** weak links within the global IT chain as well as hacking activities by both criminal and state actors have the potential to destroy our national critical IT systems. The national identification system, the digital addressing system, e-payments, digital financial services and the various e-government initiatives in which we all take so much pride, can be brought to a halt or undermined by cybercrime.

Ladies and Gentlemen, other crimes such as human trafficking, drug trafficking, terrorism and money laundering depend on ICT to thrive. Cyber security issues are therefore now firmly national security threats. Our country cannot fully reap the digital dividends associated with our adoption of ICT as a means of our socio-

economic transformation if we fail to mitigate both existing and emerging cyber security threats. The UN SDG 9 requires our country to develop resilient infrastructures including ICT systems in order to sustain our economic development. My government is therefore resolved to address these challenges in order to safeguard our digital journey.

We are undertaking specific policy and practical intervention initiatives, including capacity building, international cooperation, judicial enforcement of cybercrime legislations and implementation of technical standards and safeguards.

In July this year, I directed the Minister for Communications, Ursula Owusu-Ekuful to oversee the implementation of Ghana's National Cyber Security Policy & Strategy (NCSPS). This was after we assessed the cyber security landscape and realized that efforts at addressing our national cyber security challenges were fragmented, without a strong national oversight.

Ghana has adopted a multi-stakeholder approach as a foundation for the effective implementation of the various cyber security activities and programmes. The inauguration of the National Cyber Security Technical Working Group (NCSTWG) by the Minister for Communications and the establishment of the National Cyber Security Inter-Ministerial Advisory Council (NCSIAC) is key to the success of our effort. We all have a part to play - ministries, departments and agencies, private sector representatives as well as international partners.

I demonstrated our commitment to international cooperation in addressing these challenges by signing the **African Union Convention on Cyber Security and Personal Data Protection** when I attended the 29th AU Summit in Addis Ababa in July this year. Accession to the Budapest Convention is also on our agenda and after Cabinet approval, Parliamentary ratification will also be sought before the end of the year.

The government has also partnered with the United States government through the **Security Governance Initiative (SGI) and the European union through their GLACY project to** support our national efforts at addressing cyber security challenges. The presence of the African Union, Council of Europe and the United States representatives here at this conference is a testimony of our desire to deepen international cooperation in cyber security. We will also engage with international institutions and technology partners such as International Telecommunication Union (ITU), the commonwealth telecommunications organisation (CTO), Google, Facebook and Microsoft to ensure cyber safety for our citizens especially children.

Criminal justice response to cybercrime is another area of importance. Training for the judiciary, prosecutors and investigators especially on cybercrime legislations and enforcement provisions

is a priority for the government. We will enforce existing legislation as we work to review and update it if necessary. We also intend to improve the forensic capabilities of the Criminal Investigation Department (CID) and other law enforcement agencies including the Economic & Organized Crimes (EOCO) to enable officers to investigate and prosecute cyber-facilitated crimes.

To improve our cyber security emergency response readiness, the government, through the Ministry of Communications is currently working on the establishment of a dedicated Computer Emergency Response Team (CERT) to protect critical national information infrastructures and sectorial CERTs for the various sectors of the economy based on international standards and benchmarks.

Above all we have to promote a cyber security culture among our people. We would not leave the doors to our homes or cars open, nor would we advertise to the public where we leave our prized possessions, we would never dream of exposing our children to known criminals, but in the virtual world, we take these chances daily.

We aim to promote specific initiatives and partnerships to improve cyber security awareness of individuals, businesses and government. We intend to explore new partnerships with the private sector through regular dialogue and information sharing. The government will empower the Data Protection Commission to ensure enforcement of the provisions of the Data Protection Act, 2012 (Act 843).

We intend to establish a National Cyber Security Centre as has been done in some other countries to liaise with relevant state agencies and the private sector to oversee cyber security operations at the national level. This is one of our major priorities in the next few months as we step up our efforts to secure our digital journey.

These initiatives require financial commitment and we will find the money to implement them. I have directed the Minister for Communications to engage with the Minister for Finance to ensure cyber security is captured in the 2018 budget.

I welcome the appointment of the Ministers for Communications, National Security, Interior, Defence, Finance, Foreign Affairs and Justice to the National Cyber Security Inter-Ministerial Advisory Council and urge them to work with the private sector and our international partners to scale up Ghana's cyber security readiness. Ghana can only achieve its vision under the United Nations Sustainable Development Goals (SDGs) if we protect our digital journey.

Thank you.

SESSION B:

National Dialogue for Digital Transformation

Under the leadership of the Honorable Minister for Communications, Ghana had a National Dialogue on Mobile-Enabled Digital Transformation, as part of the Cyber Security Week, in the quest to explore the opportunities offered by mobile technology to leverage digital transformation for inclusive development.

Key personalities at the meeting who jointly signed a communique included the Chief Executive Officers of major Telecommunications companies of Airtel-Tigo, MTN Ghana and Vodafone Ghana. The high-level closed-door roundtable discussion at the Accra International Conference Centre had representatives from notably high ranking organizations, who only did not sign the communique but equally give speeches in support of the agenda. These are:

1. The UK Department for International Development (DfID)

2. Groupe Spéciale Mobile Association (GSMA)

3. United Nations Development Program (UNDP)

4. Ghana Chamber of Telecommunications

5. Ministry of Gender

6. Ministry of Planning

The session commenced with introductory remarks by Mr. Goodluck Akinwale, the Head of GSMA Sub-Saharan Africa. He acknowledged the widespread of the mobile industry and noted that the power of mobile phones should be positioned to complement other sectors like agriculture, information and health among others. He further drew attention to a mobile gender gap which ought to be bridged. Mr Akinwale commented that, Ghana is uniquely positioned as government and telecommunication companies are in a discussion to facilitate development through telecommunication. He hoped by the end of the dialogue, stakeholders would sign a communique for mobile enabled digital transformation in Ghana.

Next, Mr. Philip Smith, the representative of the UK and Head of DfID Ghana and Liberia, added that the UK government recognizes how the break out technology of mobile phones can play a vital role in governance. He expressed interest on how to connect the whole country and promote the use of ICT in education, health and industry as well as promoting e-commerce.

Mr. Dominic Sam, the Country Director of UNDP, equally stated that mobile technology for Sustainable Development Goals (SDGs) exhibits

how sustainable development objectives can be accelerated and scaled up when government and industry leaders work together from the onset. In his opinion, though the disruptive nature of technological change is unprecedented, it is significant to channel them for the public good as it can offer opportunities to achieve SDGs through joint actions. He also said 65% of the population of Ghana have mobile subscriptions while 45% of them have access to internet via mobile technology with over 8 million active mobile money accounts in Ghana. Subsequently, Ghana can leverage social and economic benefits. Mr. Sam assured that the UNDP is committed to support areas as:

- Expanding social and financial services through mobile money and digital identity including tailored products for women and marginalized communities to reduce the gender gap.

- Mobile-enabled affordable, clean energy solutions for underserved and off-grid segments of the population.

- Support start-ups and entrepreneurship, as well as big data and innovative data tools, to assess needs and progress in SDG implementation, and to share knowledge and best practices.

Julia Burchell, Senior Manager (Mobile for Development) at GSMA and Derek B. Laryea, Head of Research and Communications at the Ghana Chamber of Telecommunications presented research findings on the immediate opportunities for public-private collaboration.

The research stated the following:

- Government's commitment in achieving the SDGs is evident in the annual GDP growth of 7% over the last 10 years.

- Ghana has played a proactive role in SDGs which aims to end poverty. Though income inequalities continue to increase, the bottom 20% income segment of the population control only 5% of the national wealth.

- Since telephone lines were established in Ghana 25 years ago, 65% of the population have been connected (representing 19 million individuals) and nearly half of the population have connected through their mobile phones and it is the second highest in West Africa. Mobile operators in Ghana have created a means for citizens to access other core services like:

a. Provision of financial services through a mobile platform. This is relevant to 11 of the SDGs-

i. No poverty

ii. Zero hunger

iii. Good health and well-being

iv. Quality education

v. Gender equality

vi. Clean water and sanitation

vii. Affordable and clean energy

viii. Decent work and economic growth

ix. Industry, innovation and infrastructure

x. Reduced inequalities

xi. Partnerships for the goals

b. Facilitating the provision of digital forms of identity in order to access range of services such as healthcare, education, employment, financial services and voting. For instance, birth registration in Ghana is approaching 70%, having risen after the introduction of Tigo's mBirth programme in May 2016.

c. Improving productivity for farmers with mobile platforms by providing up-to-date information on market prices, weather forecasts through services such as Vodafone Farmers' Club.

d. Expanding healthcare access with programmes such as Mobile Technology for Community Health (MOTECH) which has revealed the potential of mobile phones to increase demand and access to health information and services among rural communities.

e. Increasing water and energy efficiency by monitoring air quality, climate change, and water and energy efficiency by improving the productivity of manufacturing and industrial processes by monitoring marine, coastal and forest ecosystem.

f. Closer collaboration between government and mobile operators to offer substantial opportunities to unlock digital transformation for millions of Ghanaians in areas such as

i. Closing infrastructural gaps

ii. Accelerating digital identity

iii. Closing the mobile gender app

iv. Increasing financial inclusion

v. Supporting start-ups and entrepreneurship.

In conclusion, the research showed that the Ghanaian government's active engagement in the SDGs and backing for private sector initiatives shows it is open to permitting sustainable business which will advance development. Telecom operators, meeting to commit to the SDGs, have devoted to continue advancement of social and economic development within communities where they operate. Closer collaboration between government and telecom operators offers substantial opportunities to further digital transformation for Ghanaians.

As part of the dialogue, Mr. Gerald Rasugu, The Director GSMA, Sub Saharan African, moderated an interactive discussion on how the use of mobile phones can transform citizens' lives in the domain of telecommunication operators looking at :

- How mobile connectivity can accelerate the achievement of social

and economic development goals in Africa

• How public-private collaboration can expedite this change?

• What concrete actions can they commit to undertaking today in support of this opportunity?

Below are the responses to the above questions.

Yolanda Cuba- CEO, Vodafone Ghana.

• Gaining identity in the digital world

• financial inclusion, beyond gender barriers

Ebenezer Asante- CEO, MTN Ghana.

• The biggest opportunity is to have a clear vision from the top where as a country, goals are set. Stakeholders must be engaged for payment and partnership.

• E-payment and e-government can be a step to digital transformation.

• Identify all areas too difficult for job operators to venture in through government intervention and policy regulation.

• Mobile money payment for instance has become a healthy method of payments in preventing bacterial transfer.

• The government must make ICT in Ghana more than just one ministry or department but a trans-ministerial department.

• The mobile sector is ready to join government in e-learning and other ventures as the digital journey takes off.

Roshi Motman- CEO, Airtel-Tigo.

The involvement of the mobile industry in improving the lives of subscribers (such as insurance services) in the achievement of social and economic development goals.

Hon. Ursula Owusu-Ekuful, Minister of Communication.

Government is very concerned with development through technology such that there is a building of curricula centered around digital education. Government is exploring some initiatives to give pupils visual (practical) materials of what they are studying in ICT. Government is planning on providing Wi-Fi to students in remote areas of connectivity. Infrastructural building is very important to government as the fibre connectivity map of Ghana is going to be reviewed in order to have knowledge of existing fibre connectivity and possibility of expanding services. The minister advised the use of economies of scale where data costs are reduced for subscribers who would in turn use and buy more data (which has become quite addictive). The minister touched on the fact that gender imbalance in the use of mobile technology needs to be

addressed because in 2007, the average market women in the country were able to comprehend the redenomination of the cedi faster than expected.

Matilda Banfro- Representative, Ministry of Gender

The Gender Ministry has played a role in bridging the gender gap in digital technology since 2012 by initiating 'Women in ICT' sessions where girls and women are trained in ICT

The dialogue ended with the closing remarks by Mr Goodluck Akinwale, Head of GSMA Sub-Saharan Africa. A communique was presented and signed by the Minister of Communication and the telecommunication companies represented by their Chief Executives.

1.1.3 Press Conference

A Press Conference was held after the high profile closed door dialogue. A summary of the dialogue and its outcome was presented to the media after which there was a Q&A session.

Q - What is the importance of the day's meeting for the whole country? -Nana Kweku Aduah,TV3

A - The government and telecommunication operators have discussed how to enable development in education, health, industry and other sectors through telecommunication and signed a communique for mobile enabled digital transformation in Ghana. Electronic payments have also been discussed as a healthy means of making payments. ICT in Ghana has been recognised to be more than just one ministry or department but a trans-ministerial department.

Q - How does this session address mobile money fraud?-Emmanuel Ajarfor, Modern Ghana

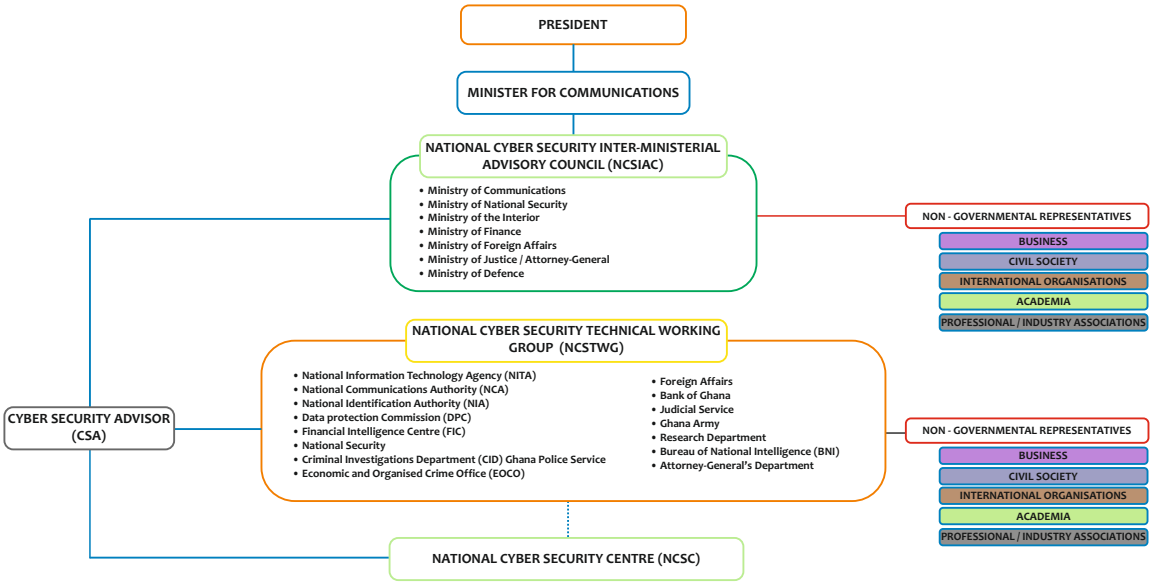
A - Social engineering has been realised as one of the methods of fraud. The telecommunication companies are however educating customers. The system is not compromised but people who have no business with the service pretend to have services to provide for customers.

Q - With Ghana Education Services against the use of mobile phones in school, how will the digital evolution take place as educational apps serve as a learning tool? -Daniel Lartey, Starr FM

A - Conversations are going on to ensure that devices specific to educational purposes are provided to enable e-learning

Overview of Ghana's National Cyber Security Institutional Framework

Presenter: Mr. Albert Antwi-Boasiako, National Cybersecurity Advisor



The Advisor to Government on cyber security indicated that, evidence available points to the fact that Ghana needs a comprehensive cyber security governance and institutional structure to help address its cyber security challenges. According to him, the country is in a better position to effectively implement cyber security initiatives if it has effective national cyber security organization structure. The governance structure is expected to ensure cyber security responsibilities and accountability at the national level, involving both government and other non-governmental actors such as the private sector.

Walking the delegates through the vision of the government on cyber security, he made it clear that these visions were that of the President and were being driven by the Ministry of Communications. This implies that, all cyber security related activities are going to revolve around these visions, he said.

In line with the first vision of the government on cyber security, development of an independent, sustainable, multi-stakeholder institutional framework based on international benchmark is key for effective national response to the growing challenges. According to the Advisor, the institutional framework has been developed along the above

requirements.

The second vision, the Advisor said is aimed at developing Ghana's national cyber security capabilities to protect our critical infrastructures and to respond to both existing and emerging cyber threats.

The vision on cyber security is also to support national institutions with a mandate on cybercrime and/or cyber security to develop their response capabilities. The inauguration of the National Cyber Security Technical Working Group (NCSTWG), he opined will facilitate inter-agency collaboration towards building these capabilities.

According to him, it is essential to foster cooperation on cyber security at all levels including the private sector which controls most data. In the area of cooperation, he was of the view that, Ghana was in the process to accede to the Budapest Convention. Cyber Security Advisor also emphasized on the need to develop the culture of cyber security in Ghana at the individual, organizational and governmental levels.

According to the Advisor, the national cyber security organizational structure encapsulates the following:

1. The President – who is mandated by the constitution to ensure the security of the citizens including security of Ghana's cyberspace.

2. Minister for Communications – who is mandated by government to oversee national cyber security in Ghana.

3. National Cyber Security Inter-Ministerial Advisory Council (NCSIAC) – is responsible for inter-ministerial cyber security policy oversight. The NCSIAC constitutes the Minister for Communications, Interior, National Security, Defence, Foreign Affairs, Justice/Attorney-General and Finance.

4. National Cybersecurity Advisor – responsible for overseeing the implementation of Ghana's national cyber security policy and strategy.

5. National Cyber Security Technical Working Group (NCSTWG) – constitutes governmental agencies and non-governmental representatives involved in cybercrime/cyber security in Ghana.

6. National Cyber Security Centre (NCSC) – responsible for coordinating national cyber security operations. The Centre is responsible for the operations of the National CERT, Critical National Information Infrastructure (CNII), Child Online Protection (COP), National Cyber Security Capacity Building & Awareness, Standardization & Enforcement and Research & Development (R&D) among others.

Panel Discussions:

Cyber Security Governance in the Private & Public Sector

The session discussed about cyber security governance issues in the public and private sectors. Four seasoned panelists contributed to discussions on the topic. The session was moderated by Dr. Kwasi Aning of the KAIPTC.

Panelists:

1. Mr. Joe Anokye- Director General, National Communications Authority.

2. Hon. Vincent Sowah Odotei - Deputy Minister of Communication

3. Mr. C.K. Bruce -Chief Executive Officer/ Innovare

4. Mr. Vincent Omobolaji,-Deloitte

Q1 - What do you perceive as constituting cyber security governance?

Answered by C.K Bruce: Basically he believes it constitutes the leadership structure and processes of organization. The most important being leadership as this is where rightful decisions are and can be made. He continued by saying

governance is creating a well cultured orientation for an organization. It is not an ethical issue but rather a social issue as far as the cyber space is concerned.

Answered by Hon. Vincent Sowah Odotei: In his view, cyber security governance is made up of the processes, leadership which govern the security of our digital space. It is about making sure that multi-sectorial collaboration is enhanced to give confidence to people whenever they are using our digital space. It also gives assurances to the people that their operations in this space are secured.

Answered by Mr. Joe Anokye: He looked at it as a form cooperate governance. According to him, he sees it to be a subset of cooperate governance in that government only provides the guidelines. Also cyber security governance is putting in place some measures to ensure frameworks are working and being managed in a standardized form.

Answered by Mr Joe Ohemeng: In terms of governance, he looks at from the direction of the country in terms of our cyber space. Where is the country now, where is the country going, what do we need to do as a country about our cyber space, who is in charge and what is the nation's target. All these mentioned, to him constitute what governance is to achieve.

Q2 - Let's talk about the threats and how do we use the framework as responding to the threat we know?

Joe Ohemeng: According to him, we need to identify the critical areas. It is about taking into account the things that are being affected or attacked. Questions like

- Are people losing money through cyber fraud?
- Are businesses being affected and more?
- So when it comes to child pornography how is it impacting the society?

So one needs to be aware of what is happening in other countries as well. He believes we must first try to ask questions about what has been identified. If people are losing money then who are those involved in these cyber thefts? In his view, asking the relevant questions is the first step in fighting the crime. He added that the National Cyber Week should have a session on awareness as he thinks that is a way the framework is helping solve the problem

Answered by Mr. Joe Anokye: For him, as soon as one is digitized, one opens oneself to bigger threat attacks. He looked at cyber security development as having a credible national information system. He believes that one thing the framework

will do is to determine how threat levels are established through some analyses. As soon as this is done, it should be followed up by determining how these threats will be mitigated. Questions like:

1. Which threat is it? The type of controls to be put in place.

2. Also in his opinion it is important to have Computer Emergency Response Team (CERT) to help in this field.

Answered by Hon Vincent Sowah Odotei: We live in a digital age and it is important we recognize that key architecture in the digital space that is threatened is the system networks and data. These are the component of the infrastructure. He thinks we need to realize that the problem is on the private and individual level as well. He stated that also the government is making sure it has set up a National Computer Emergency Response Team. Also, the framework allows for a sectorial Computer Emergency Response Team which will deal with threats at various sectors of the economy. Again, the multi stake holder nature of the framework makes it an all-inclusive venture where knowledge will be tapped from other places. On the issue of child online protection, he believes parents go along to pick up their children from schools to their houses as a way of securing them. The issue to him is parents doing so have not thought of the cyber space. How are they securing the space too? That is why the framework encompasses various sides which convinces him that the policy is a good one.

Answered by C. K. Bruce: He thinks the framework is solid. According to him, the inter-ministerial advisory council provides leadership. It covers the main ministries that covers the high risk areas of the country. However, he was quick to add that if care is not taken and the system is hacked, it will cause a major problem. Having said that, he then cautioned that the current threat is aimed at a place where those perpetrators will gain. Also, gone are the days when people hack for fun but now, they do that for financial gains and even there is a payment system that support it. Ransom ware is a way they gain. He stated that some state institutions such as the justice systems, utility systems and the financial sector all are to be safeguarded because if they are hacked, the consequence will be enormous. He stressed that an attack if successful in one sector could be replicated in another and so the need for sharing information among industry players. To conclude, he sees the framework to be workable but the only thing is, there is the need to ensure that everybody within the framework is actually doing what they are supposed to do.

Q3 - How do we change the work ethics? The way we treat information. What do we do to change our general

culture?

Answered by Mr. Joe Anokye: The Board of Directors of various institutions should see guarding cyber space as a crucial responsibility. They should as a matter urgency add to its risk management framework. That is, they must prioritize it at the top. They must have it in mind not just an information technology function but rather to create the position of a Cyber Security Officer who reports directly to the board. In any case, the board is to provide strategic direction to the organization. On the lighter note, he chipped in that he will love to see a course titled Cyber 101 for all board of directors to undertake just to enlighten them on the need to have cyber security at their work places.

Answered by Hon. Vincent Sowah Odotei: On how to carry information about, he believes it demands exhibiting some of leadership quality, being discipline in carrying out our daily tasks.

DAY 2

CONFERENCES AND WORKSHOPS

SESSION A:

Conferences and Workshops

The conferences started with Madam Patricia Adusei-Poku, Data Protection Commission (DPC) of the Ministry of Communications introducing herself as the moderator for the session. She outlined the following thematic areas as issues to be discussed in the various workshops:

1. Data Protection and Cyber Security
2. ECOWAS Directive on Cyber Crime
3. The Budapest Convention and International Cooperation against Cyber Crime
4. Cyber Security and Forensics Readiness
5. Cyber Security and National Wellbeing-National Security Perspective

Data Protection and Cyber Security

Madam Patricia briefed the audience on data protection. She stated that in one way or the other most people give out some amount of information to institutions and industries. This information ranges from personal to somewhat general. However, there are instances we feel threatened and unsafe because these confidential information in the custody of institutions have been intercepted hence the need to pass laws for legal recourse. She highlighted what the law says about personal data. That is, to take steps to secure the integrity of personal data by using the appropriate technology that allows them to secure the data they acquire from us. Technology should help the institutions prevent losses, damages or unauthorized access. In the event of unlawful access to data, the individual as well as the Data Protection Commission is to be notified. Madam Patricia concluded her opening remarks with the fact that the risks in giving out vital information calls for cyber security. The Commissioner advised participants to report data breaches to the DPC and encouraged businesses to register and comply with data protection requirements, since these are essential cyber security practices.

ECOWAS Directive on Cybercrime

Mr. Isaias Barreto, the first speaker and ECOWAS Commissioner for Telecoms addressed the issue of legal framework to fight cybercrime. He gave a brief overview of ECOWAS. The organization was established in 1974 at Lagos to enhance regional integration. Mr. Barreto stressed that ICT is the engine for regional integration within the sub-region and this will encourage a digital single market. Therefore, there is the need to address cybercrime. He revealed statistics by McAfee which depicts that, the cost of cybercrime to the global economy in 2014 was about $445 billion with losses to Nigeria in 2016 being $550 million. Statistics further predict that cybercrime could cost about $6 trillion by 2021 hence the need to protect the cyber environment. He suggested that individuals and countries should invest in critical infrastructure protection. Statistics again indicate that the spending on cyber security which was to the tune of $80 billion in 2016 will exceed $1 trillion between 2017 and 2021 and that there are 1 million cyber security job openings and this will reach about 1.5 million by 2019.

Narrowing it to the West African's

context, Mr. Barreto raised concerns about lack of national cyber security strategy and poor awareness on cyber security issues. He emphasized that in Africa, people use social networks to commit crime, therefore we need to develop capacity in the sub-region to address the issues.

The International Telecommunications Union in 2014 published a cyber-security index. It focused on five main measures. They are: the legal measures, the technical measures (looks at how standards are defined), organizational measures, the need for agency to address cyber security issue and lastly the need to implement capacity building programs to train people in cyber security. He emphasized that international cooperation is needed to help fight cybercrime.

Mr. Isaias Barreto mentioned three legal frameworks of ECOWAS to deal with cyber security. They are: Directive on fighting Cybercrime, supplementary Act on Electronic Transactions and then Supplementary Act on Personal Data Protection. He acknowledged the African Union's complementary role in fighting cybercrime in the region and the Budapest Convention protocols to support cybercrime investigations and prosecutions. ECOWAS aims at fighting cybercrime by promoting capacity building for judges, police officers among others and improving upon the security environment in the sub-region.

He concluded by expatiating on the way forward. He stressed on the need for collaboration in the sub-region to promote the common agenda on cyber security, that is continuing in capacity building and sensitizing our citizens on key issues relating to cybercrime and cyber security.

The Budapest Convention and International Cooperation against Cybercrime

The session commenced with a presentation given by Mr. Manuel De Almeida Pereira, Project Manager at the Cybercrime Programme Office of the Council of Europe. Mr. Pereira presented on the topic: The International Legal Framework on Cybercrime and Electronic Evidence: The Budapest Convention and International Cooperation against Cybercrime.

He spoke passionately on the display of indecent pictures of minors online and child pornography as some of the cybercrime trends that requires attention of countries. He stated that the Budapest Convention provides the framework for investigations and prosecutions of cybercrime. He encouraged Ghana to speed up the process towards accession to the Budapest Convention as it will help the country to enhance its cybercrime investigations and prosecutions response through international cooperation with state parties to the Budapest Convention.

Mr. Pereira further mentioned that, the Council of Europe will continue to support Ghana with capacity building programmes on cybercrime and electronic evidence through the GLACY+ Project.

Cyber Security and Forensics Readiness

The session which was presented by Mr. Alex Oppong, Principal Consultant at Ghana's e-Crime Bureau begun with an introduction on the history of cybercrime from the 1980s where data was being intercepted to 2017 where lives were put on the line at the National Health Service in the United Kingdom with a huge ransom.

Mr. Oppong elaborated on what malware is as they have become a top threat in Ghana with over 150 countries being victims of cybercrime. He revealed the implications of ransomware which has become a tool for extorting many institutions globally using malware such as the WannaCry incident which affected many countries.

He introduced digital forensics (digital investigations) as a legally accepted procedure for investigating and recovering evidence involved in cybercrime. The Electronic Transactions Act 2012 (Act 772) and the Data Protection Act 2012 (Act 843) outlines regulations surrounding the Ghanaian cyberspace and are crucial in prosecutions. In forensic readiness, one is advised always to keep back-up of data which should be isolated from network. In the case where a device has been infected, it is advised that the victims keep calm, report to a cybersecurity experts and not to interfere with the infected device as it would mean tampering with evidence.

During the Q&A session, the following questions and answers were asked and responded to respectively:

Q- Are there laws against sim boxing?

A- Simbox operators do not have operational licenses and that forms the basis of all other offences in the National Communication regulations. Sim-boxers evade taxes, denying the country of revenue and as such are punishable by law.

Q- Is it right for passwords of account holders to be demanded?

A- Depending on the demand, however giving out passwords enables entire access to one's data. Law enforcement, for example is mandated by law to demand passwords to computer systems of suspects.

Cyber Security and National Wellbeing: National Security Perspective

The final presentation of the day was delivered by Mr Kwabena Adu-Boahene, Director for the Bureau of National Communication (BNC). His presentation was in three parts.

The first part focused on the Critical National Information Infrastructure (CNII) and how it related to national well-being. He began this with an illustration of how previously information or data was written on paper and safely put under lock and key in safes, briefcases. Then, along came computers which led us to start computerizing our operations thus a paperless procedure which is now being adopted by many organizations. He indicated that, there are a number of e-transformation projects aimed at changing our day to day business from paper base to electronic base. This dependency has led us to have something critical to our operations hence CNII as everything is now going towards the electronic. For instance, banking these days has been made easier as one does not have to visit the bank as often since almost all transactions can be completed electronically. CNII can therefore be described as those computer systems, the data and functions which are so vital to the country that the incapacity or distraction of which can have adverse effect or impact on national well-being. Therefore, any computer network or system that can align with this definition means that it is a system that is critical to the nation and needs to be protected as it can cripple the country.

The second part of this presentation centered on threats to the CNII. Mr. Adu-Boahene mentioned espionage and intellectual property theft as some of the threats. Mr. Adu-Boahene emphasized on how people can sit in the comfort of their homes and conduct espionage which is now difficult to detect as it may seem that everything is functioning well but your internet could be used to steal your data. Mr. Adu-Boahene also mentioned cyber warfare as another potential threat to CNIIs.

Having identified these risks, he went on to discuss what we can do to adequately protect ourselves from these threats as well as prevent them. He encouraged collaboration between the government and the private sector towards securing Ghana's CNIIs. For instance, a National Cyber Security Technical Working Group has been set up to work hand in hand with the institutions that constitute it in order to put together our collective efforts. He emphasized that, such collaboration will encourage information sharing on these threats for mitigation. He also advised on the development and enforcement of standards to secure the CNIIs. He encouraged government to build and maintain capabilities to conduct cyber space operations.

SESSION B:

Stakeholder Mapping Workshop by the Security Governance Initiative (SGI)

The purpose of this engagement was to assist the Government of Ghana (GoG) in conducting an effective National Cybersecurity Week event, including preliminary assistance by the Security Governance Initiative (SGI) in the development of the National Cyber Security Framework and National Cyber Security Technical Working Group (NCSTWG) charter. Key goals of MITRE's participation in this conference were to help ensure a whole-of-government awareness and understanding of national cybersecurity strategic goals, and to help establish support for the governing role of the National Cyber Security Technical Working Group (NCSTWG).

The conference was held October 23-27, 2017 in Accra, Ghana. The two key activities MITRE facilitated in support of this task were a Ministerial-level Roundtable on validating and refining national cyber priorities, and a Stakeholder Mapping workshop. The intent of the roundtable was to help key GoG leadership reach consensus on cyber security priority areas. The Stakeholder workshop then took these prioritized goals and identified supporting objectives, brainstormed potential initiatives/tasks that would further those objectives, and mapped stakeholders against those tasks.

Summary of Participant Inputs & Recommendations

• Ghana should set a strong example across the region in cyber strategy and cyber security

• The goal of a National Cybersecurity Governance Framework is to create something that is sustainable and not personality based. Cybersecurity should not be considered ad hoc or reliant on particular administrations or personnel.

• Discussion and finalization of the charter of the technical working group is a priority.

• GoG is planning on creating an NCA SOC that can be integrated with the Telecom SOC. Ghana is looking to create CERTs for multiple sectors that will later integrate with each other, but the development is not synchronized, and each is at a different stage.

• The NCA's goal is to use young national service personnel to man the CERT 24x7 (3 shifts) with training on network monitoring. These individuals, who must give one year of service in repayment of college expenses, were mentioned as preferred because they trainable and cost effective.

• Cyber threats are the most serious crimes facing Ghana, but in order to take the fight to the next level, the GoG needs to look to the roots and nature of threats.

• The GoG needs more and better legal remedies to address crimes

• Wants more funding of research and development to evolve cyber security, with the goal of protecting Ghana's interests outside the country, encouraging direct investment from abroad, and working with the banks.

• Workforce development should be considered part of CERT development.

• Integration of cybersecurity concepts into education curricula (elementary, secondary, internships), including teacher training

• Financial assistance for cyber security students through government grants, industry scholarships

• Conduct and publish a cost-benefit analysis to show socio-cultural-economic impact of cybersecurity/cyber incidents

• Train journalists to understand and report on cyber-related events

• Develop social media hash tags and games, catchy phrases

• Identify and create national registry for CI and establish cyber security officer (CISOs) for CI

• Improve physical security, including physical siting/isolation of facilities

DAY 3

CHILD ONLINE PROTECTION

The Child Online Protection (COP) Conference

3.1 Opening Remarks

The Conference proceedings started with a prayer and acknowledgement of some dignitaries by Mr.Derek Laryea which included the members of the high table for the opening ceremony.

First to give the remarks was Mr. Goodluck Akinwale, the head of GSMA Sub-Africa. He set the ball rolling by stating that we rely on the Internet for social and digital transformation. However, he opined that we cannot allow the online space to be unregulated. He suggested a collaborative effort from all and sundry to put in place effective measures to make the online space safer for children.

Mr. Gayheart Mensah who represented the Chairman of the Telecommunications Chamber expressed the excitement of the Telecommunication Chamber to partner in this advocacy of protecting children online. He mentioned digital learning and instant school at Vodafone as some of the tools which gives opportunity to children to learn on their own. Mr. Mensah also made mention of Vodafone's new brand repositioning with the tag line "the future is exciting, ready?" He was of the view that, this will guide customers to take advantage of the positive use of the Internet.

The UNICEF representative, Mr. Mohammed Rafid Khan stressed that this is the time to make the cyberspace a safer place for everyone especially children. He said that the protection of

children online is everyone's responsibility beginning with the parents at home, institutions, private sector and the government. He ceased the opportunity to congratulate the Ministry of Communications for developing the National Framework on Child Online Protection.

Mrs. Ursula Owusu-Ekuful, Hon. Minister of Communications

Key points

Hon Minister for Communications in her welcome statement, highlighted the following key points:

- The conference is an opportunity for stakeholders to discuss issues of online safety especially for children and young people.

- Ghana has tremendous growth in Internet-related infrastructure.

- The Government is committed to securing Ghana's Internet space including the protection of children.

- Everybody is at risk when it comes to the Internet.

- If stakeholders do not regulate the websites children visit and parents do not monitor what their children do online, they will be exposed to unsafe contents online.

-We ought to be mindful of what we share online as some employers often identify their applicants with what they share on their social media platforms.

-She concluded by stressing on the need to learn about online protection so we can teach about a safer cyber space.

-She also expressed gratitude to the partners on behalf of Government for committing to the protection of children online.

What and Why – Child Online Protection (COP)

Ms. Shola Sanni-Senior Policy Manager for Africa at GSMA:

Key points:

- Child Online Protection (COP) is not a new concept but an area which has evolved after the deployment of Internet to Africa and the approach for the protection of children is and should be based on the principles of child protection in an African context.

- In the bid to protection children and young people from the dangers online; one needs to be conscious of the children's Rights as stipulated in the UN conventions.

- The consequences of Internet use could be good or otherwise hence the need to balance the use in order to derive the positives.

- There is no single solution to protection of children online but it is important one adopts a combination of strategies ranging from education with awareness creation to the use of technical tools to creating appropriate digital environment.

- Should technical controls fail, education is the first line of defence couple with the need to have physical infrastructure in a form of system to provide the support children will need.

- Key to achieving Child Online Protection goals systematically requires: legislation, reporting hotline, law enforcement, industry processes and the victims support.

- Ms Sanni ended her presentation with a call on policy makers to be actively committed to COP while encouraging the private sector to conduct self-assessment on COP so that they can put in place self-regulation measures.

Positive Use of Mobile and ICTs

Ms. Shola Sanni-Senior Policy Manager for Africa at GSMA:

Key points

- The internet is not all evil but has its good side and she illustrated this with how the intended use of a kitchen knife is to chop food ingredients in the kitchen but some people use it for other evil purposes like killing. There is therefore the need to balance the perception of the internet and ICT.

- From her perspective as an African, mobile internet is a life changer. For instance, there are countries like Ghana where by mere virtue of owning a mobile device, one can perform financial transactions and also have access to information and education in the comfort of one's home without having to walk to a physical office or school. This has changed or improved a lot of lives, she said.

- ICTs and Internet are key success factors for the transformation of the African continent.

- The reality is that children and young persons have a lot to gain than to lose if we harness the power of ICT and mobile internet, not to disregard the dangers of using the Internet.

- It is however very important that a balancing act is performed to encourage and find ways to promote the positive uses of the internet and ICTs.

- Organizations like UNICEF and ITU for child online protection have put in place very high level guidelines or framework that gives stakeholders an idea of what steps to take in joining the global collaborative effort for COP.

International Perspectives and Best Practices for COP

Ms. Shola Sanni – GSMA

Under this session, different International organizations shared their perspectives

In Africa, there are still a lot of illiterates who are not aware of the social media platforms and the dangers associated with them.

There is therefore the need for a high and immediate level of education and awareness that needs to be created

amongst these people to bring them up to speed.

The general public is also responsible for guiding children on how to behave online. So education and awareness can be seen as the quickest way to facilitate COP, as it is something we can do regardless of where we find ourselves.

Another way is the use of technical tools like control applications. Parents can have technical control of their children's devices in order to be able to monitor the things viewed by their children online. These tools may fail as a child can easily have access to free Internet from their friends so the GSMA believes that when these tools fail, education should be able to save them and cause them to make the right decisions.

Child Helpline International is working in close collaboration with UNICEF and other stakeholders so that children and adults can report online situations.

Support systems like physical infrastructures are needed to address these issues online and help with some support attacks, as education and awareness may not be enough.

Legislation is also a key structure. It is what stakeholders should have in mind when it comes to establishing a strong framework for COP in different countries.

In Africa, there are cultures where child abuse, inappropriate contact with adults are not much spoken about. These crimes against children in the online space are not adequately provided for in the legal framework.

Laws should therefore be made solid enough to punish offenders in order to discourage them from perpetuating crimes against children in the online space.

There is also a need for industry processes because we all as stakeholders increasingly have an understanding of what we need to do, how we need to work together and collaborate but in many instances is not documented. For instance, mobile operators are expected to work with law enforcement agencies or the government in helping to track offenders or take down inappropriate contents for the Internet platform that they provided but unfortunately there is no documented process for that collaboration.

It is very important that as COP stakeholders, we document our collaboration processes.

Stakeholders in both private and public sectors can conduct self-assessment on COP policy and regulations.

Ebele Okobi – Public Policy Director for Africa at Facebook

Key points

She explained how access to technology is the key to the future in terms of how we rise as a continent.

She also added her voice to the need to create a network where children will be safe online.

At Facebook, an issue of COP and safety is dealt with the help different categories namely:

• **Policies** - This is essentially innovation that has been created not just as a Facebook page but in partnership with stakeholders to create an environment on Facebook that maximizes expression and safety as well as community standards.

• These policies are also created for people to express themselves and also to address the issues of people using fake names and accounts. These people indicate wrong ages as age limit required to have an account is 13 years. Such people engage in bullying, violence, harassing people.

• Facebook also has strict policies and zero tolerance for certain types of abusive content which includes political threats, child exploitation imagery like children having sex, pornography and so on.

• **Tools -** This platform helps people resolve their problems. It includes privacy checker, which allows one to continuously check on privacy settings, have control of what they share with visibility so that for every single post you can choose your preferred audience for it.

• You can also block anyone you do not wish to interact with and also be able to report content that violate community standards.

• There are seven hundred thousand people working throughout the day to listen to reports and access them.

• Reports can also be made even without a Facebook account.

• There are also dedicated programs for this kind of safety so they work with safety experts (J Initiative) to develop programs and guides. Some of these include "think before you share", a resource that basically raises awareness amongst young people so that they can think about the kind of content they are sharing and ask themselves questions about whether or not they want to share the post.

• There is also one called "help a friend in need", a resource where young people can learn how to deal with the content and report it for example distressing content like posts of a suicidal friend.

• There is also a Safety Centre and Bullying Prevention Hub. These are all practical dialogues to provide people with tips on how to handle content on the platform.

Camilla Edry-Director of Cyber Projects of IAI

Key points:
She described how intelligence is key in protecting children in the online space.

She encouraged parents and government to work hard to protect children. Parent should be helped to teach their children to be more aware of the dangers of the Internet.

The government should have the capability to go online and get information on who is doing what and get forensic evidence to bring them to justice.

Certain harmful sites could also be blocked to protect children online.

Mohammed Rafiq Khan – Chief of Child Protection at UNICEF, Ghana.

Key points:
UNICEF globally helps governments to prevent child online abuse and also respond to those children who have been exploited or attacked.

They also help law enforcement agencies in prosecuting perpetuators in terms of providing forensic capabilities.

According to statistics, there were 24.6 million people in 2010. 35% of this total population were Internet users. 26% use the Internet every week.

Most children have access to Internet from age 12.

Close to one third of Internet users use their phones to take pictures or videos. Globally, 80% of those 18 years and above are in danger of being externally abused or taken advantage of online. 39% of children have seen indecent images according to the UNICEF child report.

Over 90% of crime committed in Ghana involves the use of mobile phones or Internet.

Whatever happens online is a reflection of the society at large or how we really are offline.

Mr. Khan however stated that opportunities the Internet has to offer are greater than the risks involved.

The Stakeholder Roles for COP in Ghana

Moderator- Derek Laryea, Head of Research and Communications at the Ghana Chamber of

Telecommunications of the Ghana Telecommunications Chamber.

Presentation: Ms. Rhoda Gavor –Deputy Director at Ministry of Communications:

The draft Child Online Protection framework for Ghana.

Key points:

The 1981 Convention that the United Nations developed for the rights of the child outlines the right of the child to have access to information.

It defines Child Online Protection as an initiative to protect children online and challenges facing them, like exploitation.

The number of children online have increased, with a high level of curiosity.

There are threats on the cyberspace which may lead children into sexual exploitation, kidnapping and other related crimes. Therefore, there is a need to keep children safe online.

This initiative requires global effort, so the Ministry of Communications has partnered with various institutions to protect children online.

Ghana has a framework developed around these pillars namely:

• Legal Measures: making policies and inculcating it into legislative framework for child online protection.

• Technical and Procedural Measures: setting up institutions

• Organizational Structures

• Capacity building and awareness creation

• International cooperation: collaborating with partners all over the world to protect the rights of children online.

The Ministry, in collaboration with stakeholders are in the process of implementing the framework.

Mr. Eric Akumiah – Computer Emergency Response Team at Ministry of Communications.

Incident reporting system:

Key points

CERT being in existence in Ghana for 4 years as a point of contact in national cyber security issues and keeps good relationship with other countries to resolve cybersecurity issues, daily monitoring based on daily feeds from international servers.

CERT has a pre-determined plan on approach to solve, having worked with National Information and Technology Agency (NITA) to investigate problems.

CERT sends alerts and advisory to public and privacy services to reduce their vulnerability to cyber-attacks.

CERT provides a platform for reporting cybercriminals on a web platform www.cert-gh.org where CERT and the

cybercrime unit of the Ghana Police CID to investigate and resolve the issue.

The Ministry of Communications through the National Cyber Security Secretariat is in the processing of enhancing the functional capability of the National CERT through effective coordination with sectoral CERTs to ensure effective incident response at the national level.

Awo Aidam Amenyah – Executive Director at J Initiative.

Stakeholder roles in Child Online Protection in Ghana:

Key points

J Initiative works to protect children and young people online by introducing them to Digital Literacy & Safety in a manner they can easily comprehend.

J Initiative was involved in the process of incorporating Child Online Protection in the National Cybersecurity policy and strategy for Ghana.

The Internet is open, it is prudent for children and the youth using the internet to do so in a safe and responsible manner so the J Initiative liaises with software content creators to make software tailored for educational purposes which are installed on devices for safer online navigation.

In order to have an effective COP system in place as a country, there is the need to build capacity for the following groups of people because their actions will support the child who may be abused online and offline: Policy makers, Social welfare, industry, civil society, parents/guardians, teachers/educators, Academia, Law enforcement and children &young people.

As part of the sensitization and awareness on COP, J Initiative collaborates with other partners including the Ministry of Communications to celebrate Safer Internet Day (SID). Such events have been used to highlight issues of child online safety.

J Initiative has also been involved in weekly social media broadcasts to educate children on COP issues.

Mr George Baiden- Childline Ghana.

Key points

Childline Ghana gives counselling services to children in some parts of the country both online and off-line who call

their helpline and also connects these children to child protection services such as the Police Service, Social Welfare, Domestic Violence and Victim Support Unit.

The child helpline operates in many countries by dialing 116. In child online protection, though Childline Ghana has low funding, it is equipped for services and can take up to a hundred calls simultaneously.

Dora Boamah Mawutor – Media Foundation for West Africa.

Key points

MFWA works to protect the freedom of expression both online and off line in collaboration with stakeholders, with the aim of ensuring everyone can freely use the internet for personal development.

MFWA engages through documentation like articles, news stories, and policy brief to draw the attention of specific stakeholders to take actions.

MFWA had organized training sessions for civil societies, the media and other stakeholders on child online protection issues.

There was a question and answer session at the end of the presentations and panel discussion. Find below these questions and the responses to them.

Questions & Answers

Q - What has MFWA done on television to draw attention?

A - Most of MFWA's television work are geared towards media professionalism

Q - Can Internet café be monitored to avert children from illicit access?

A - Guardians need to sensitize young ones as they go online and should be responsible for their movement.

Q - Can CERT monitor security of downloads from app stores?

A - Softwares would be monitored and all malware detected will be reported accordingly.

Q - Are there mechanisms put in place for cell safety and can children who are taught to use the internet be taught netiquettes or cyber hygiene?

A - J Initiative educates both children and adults in the most convenient language. The initiative creates awareness for content development as their inputs brings its associated results.

Q - Are there any gaps in stakeholder initiatives how can it be bridged?

A - Mainly communication gaps and with that stakeholders are being connected to ensure the spread of the word on COP.

Q - Is there a reward and punishment system for child online hygiene?

A - Primarily, parents can have a reward system for their children when they practice online safety and have them

punished for malpractices online.

Q - Why is child online protection not heard on television?

A - Due to the expensive cost of airtime on television, much of the television education side should be taken by NCCE.

Q - How can an illiterate parent control child online issues?

A - Online protection involves a lot of stakeholders, even with the teachers of such children which is why it is imperative to carry out a lot of awareness in all forms and shapes.

Q - How is the child online protection framework implemented?

A - The government is mandated to provide an enabling environment. The Ministry is engaging will all stakeholders on the implementation of the framework.

Q - How can CERT be proactive with lack of infrastructure?

A - The government intends to scale up the capability of CERT to be able to proactively detect and mitigate cyber security incidents, including COP issues.

School pupils present were given the opportunity to contribute to the child online protection session since they are directly involved. They were asked if they feel safe online and what measures they think is needed to be put in place to make them feel safer online. The children admitted they did not feel safe especially with people posting nudes online recently.

The pupils appealed to the government and stakeholders to ensure child online protection laws are passed and perpetrators are severely dealt with.

Below are their questions, answers and a contribution:

Q - MFWA should emphasize their role in child online protection

A - It is a non-profit, non-governmental organization that works with stakeholders to help make the internet environment safer for children.

Q - Who are stakeholders?

A - A group of people working on a particular goal, like in child online protection, children are stakeholders.

Q - What is capacity building?

A - Capacity building means giving the desired education to stakeholders.

Dr. Gustav Yankson, Head of the Cybercrime Unit, CID Headquarters added that there are punishments being meted out for every cybercrime, even possessing pornographic materials on mobile phones. He added that extortion online is punishable by law and hoped future sessions would have a discussion with legal practitioners in order to know the laws concerning the issue.

Industry Proposals for Safe and Responsible Use of Internet by Children and Young Persons

Demonstrative Session by Facebook

Ebele Okobi, showed how reporting a post on Facebook is done. In a brief demonstration, she revealed that clicking on the icon with three dots in the corner, leads to the next menu with 'report' option. Upon selecting the report option, it leads to variety of issues that has been labeled- whether it is a scam, not appropriate for Facebook, etc. A chance is given for more information to be given. It can then be sent, after which a feedback system will send an acknowledging receipt.

The process is confidential.

Shola Sanni- GSMA

The GSMA representative at this point read out the stand taken by ICT providers (telecommunications operators) that looked forward to collaborating with the right stakeholders to:

1. Promote responsible business practices

2. Create an enhanced safer and age appropriate online environment for children and youth in Ghana.

3. Prevent online abuse of children.

4. Deploy educational and awareness programmes in order to create the culture of safe and responsible use of Internet among children and youth.

5. Promote useful technology as a platform for self-empowerment geared towards children and youth
Telecommunication companies have already engaged in a high-level dialogue with the hopes of beginning a new level of collaboration.

There was a suggestion, question and answer session at the end of the presentations. Find below these questions and the responses to them

Q - Can Facebook review content before post?

A - Due to the large numbers of posts per minute, it will be extremely difficult to do so. Though Facebook constantly monitors posts and deal.

Towards a Comprehensive National Strategy

Presentation by Mr. Mohammed Rafi Khan; UNICEF representative.

"We protect framework"

Key points

"We protect framework" is an initiative where UNICEF and other

partners have put in place to help government put measures in place for the protection of children online with following components:

1. Policy Endorsement; a legislative framework in Ghana is strong because the Electronic Transaction Act (Act 772) has been promulgated so that it can fully be used for prosecution.

2. Criminal Justice System; including the judicial service and the police who must be trained to be able to acquire evidence from devices accurately.

3. Victim Protection; to support victim

4. Societal Component

5. Industrial Component

6. Media/Communication

Awo Aidam Amenyah – J Initiative

Expectations for Ghana's COP Strategy

Key points

Looking forward to see a national framework for students, protecting and securing them.

The framework should make provision an effective community of practice to make child protection holistic.

Responsibility for service providers to be accountable for the right things to be done within the space.

All users regardless of educational background should be able to take action whenever they feel threatened.

DAY 4

CYBER SECURITY TECHNOLOGY SOLUTIONS

SESSION A:

Cyber Security Technology Solutions

Opening Remarks by Brigadier General Dr. E. W. Kotia

The session begun with Brigadier General Dr. E. W. Kotia, the Deputy Commandant of the Kofi Annan International Peacekeeping Centre (KAIPTC), giving introductory remarks. The General's remarks focused on how crimes have moved from the physical environment to the cyberspace. He was of the view that, stakeholders need to work together to mitigate the threats from the cyberspace in order to ensure the security of Ghana's cyberspace. Gen. Kotia proposed capacity building within the military to ensure Ghana scale up its cyber defenses. He also advised the Criminal Investigation Department (CID) of the Ghana Police Service to be resourced to be able detect and investigate cybercrimes. Businesses, he advised, should invest in their cyber security by training their employees and deploying automated cyber security systems to detect and prevent fraud.

Panel Discussion: Countering Mobile Money Fraud- Perspectives from stakeholders.

The Moderator for this session was Hon. George Andah, Deputy Minister for Communications

Panelists:

1. Mr. Eli Hini, General Manager- MTN Mobile Money Service

2. Ms. Matilda Wilson, Head of IT- National Identification Authority

3. Dr. Setor Amediku, Head of Payment Systems- Bank of Ghana

4. Mr. Joe Anokye, Ag. Director General- National Communications Authority

Hon. George Andah gave a preamble of the Mobile Money service from 2008 when he was part of a team sent by MTN Ghana to East Africa to study the Mobile Money system which was to be introduced in Ghana the following year, 2009. Though it has become a convenient method of financial transaction, unscrupulous persons have infiltrated the service with dubious means of making money from unsuspecting victims.

Mr. Joe Anokye described how efforts have been made to make the services convenient with interoperability, where all mobile money networks shall be integrated to facilitate sending and receiving of money among mobile money patrons.

Dr. Setor Amediku added that financial inclusion in Ghana is 58% but from the introduction of Mobile Money, the rate keeps shooting up. He further expressed the Central Bank's concern about fraudulent schemes that have hit mobile money services. He touched on the importance of Mobile Money interoperability which will simplify mobile money transactions.

Ms. Matilda Wilson revealed that, the National Identification Authority is ready to roll out the Ghana Identification Card to citizens of Ghana as well as foreigners who have resided in Ghana for 90+1 days by mid November 2017. According to her, this will become the sole ID card for national identification to be used to synchronize a national database. She stated that the card will become a basis for registering SIM cards and that would place valid identities to Mobile Money wallets.

Mr. Eli Hini disclosed that, Personal Identification Number (PIN) required for Mobile Money transaction has become the weakest link on customers' end of the service as it gives total access to one's wallet. He however mentioned that, agents are being trained to give customers the best services while customers are also being educated on how to detect and prevent Mobile Money fraud.

MTN Ghana however keeps monitoring Mobile Money dealings and with the help of the Police Service, they have been able to trace and punish perpetrators who are caught in the act.
It was stated that, Ghana is the first country to introduce interests on Mobile Money with an annual rate of 7% which is paid quarterly to subscribers.

Questions & Answers

Q - How ready is MTN to combat Mobile Money fraud and interception of data?

A- Customers are advised to only deal with accredited dealers. Customer education and awareness is key.

Q - How is MTN addressing SIM swapping, and how can one avoid falling victim to mobile money fraud since the fraudsters are very smart in their dealings?

A-

1. MTN observes Mobile Money dealings and investigates suspicious activities. They trace and have offenders punished.

2. MTN advises customers to always ask callers who require information from them to get in touch with service providers and must not reveal any sensitive information such as customer PIN to them.

3. MTN allows a 48-hour window in SIM swapping actions to allow necessary precautions.

4. MTN customers are constantly being educated on how to avoid falling victims to Mobile Money fraud.

Q - What form of identification is the National Identification Authority going to use to validate identity during registration of the Ghana ID card?

A-

1. The birth certificate or passport of the person. However, the old National ID card is also valid for registration.

2. If the one registering has neither of the documents, a registered relative can guarantee on the applicant's behalf.

Q - In Nigeria, the Central Bank uses a biometric number to identify account holders regardless of the number of accounts they hold, would that system be helpful to combat fraud if Bank of Ghana adopts that system?

A- The Bank of Ghana is supporting the National Identification Authority to make the National Identification process successful to place valid identity on all financial accounts, making it easier to trace fraudulent activities to perpetrators.

Hon. Andah concluded the session and highlighted the concerns of stakeholders relative to mobile money fraud. He indicated that, the government through the Ministry of Communications will be working with stakeholders including the central bank, telcos, NIA and mobile money patrons to mitigate mobile money fraud. He encouraged Ghanaians to download the GhanaPostsGPS app and take advantage of the digital transformation.

Cyber security technology solution - I
by Ida Moore, Director of Sales-Kaymera

• He presented on various threats that tend to affect mobile connectivity, using a scenario of connecting to a Wi-Fi network at an airport which one is ignorant of. The other parties connected to the network may lead to hackers getting access to delicate information from one's phone. Such infiltration through devices may pose serious risks even at the national level as it could expose sensitive data belonging to government.

• Due to internet connectivity, cyberattack has become prevalent so he advised that, one should be careful when downloading apps from the internet since some of these applications may be veiled with malware. The apps may have access to some vital parts of a device, may intercept communication, and have access to real time video recordings. It is therefore prudent for one to frequently update operating systems and have preference for end to end encryption. He recommended that permissions for apps should be reviewed by users before installing.

Cyber Security Technology Options for People, Businesses, Government

by Mr. Edward Ansong, Senior Lecturer KNUST

Mr. Ansong explained that cyber safety is a set of practices and actions that is intended to protect our personal information. Cyber safety practices can be global (Budapest Convention), Regional (EU, ECOWAS Council on cyber security), National (Ghana's Data Protection), or even institutional (Bank's policies on cyber security). In cyber safety, it is important one takes caution in joining networks like free Wi-Fi with no prior knowledge of the source or even the third parties on the network who could pose threat to one's data.

There should be a lot of precaution when downloading materials on the internet and mail attachment from unknown senders as any click may lead to phishing. He advised the use of complicated passwords that cannot be linked to biodata like name, date of birth etc. which should be changed regularly and not shared.

For the business front, Mr. Ansong alluded cybercrime to the corporate email being infiltrated, and employees' devices being connected on the company's network, exposing it to vulnerabilities. He also mentioned that, companies sometimes put their vulnerabilities out to their potential scammers by informing them knowingly or unknowingly about their system structure. He also advised that security measures should be strictly enforced when practicing Bring Your Own Device since devices can be compromised and in effect compromise the network.

In government cyber security, it is a known issue worldwide that nations have attacked other nations through cyberwarfare. As a country moves into a cyber age, its attack space increases. It has been observed that cybercriminals target government organizations, penetrate their system, crypto lock it and ask for bitcoin payment.

He advised that, Government should collect data on all cyber professionals and also continue to train departments and the general public on cyber safety. Government must also establish an inter-sectorial cyber task force to coordinate cyber security issues.

Cyber security technology solution - II

by Dani Paslev, Israel Aerospace Industries (IAI)

• Cybercrime has become a challenge to national cyber security and as such every nation should be prepared for cyberwar which involves the use of technology. Since cybercriminals are sophisticated, constant preparations must be made to fight against them. The nation needs to pay attention to the cyberspace and have capacity building for its people since educating the people prepares them against cyber threats. The urgency of young people to be on social media to update their post leaves them vulnerable in the cyberspace. He advised that countries must keep surveillance on national infrastructure to have real time awareness of the state of cybersecurity.

• The key to success in cyberwar is to bring different methodologies and tools combined to form end-to-end solutions in the field of cyber protection. Mr. Paslev recommended that government set up a national forensic lab and getting a working model for critical infrastructural protection. The other side of cyberwarfare is the justice system where cybercriminals are prosecuted. He concluded the presentation by explaining how cyber threats can turn aircrafts in a country into weapons against the country itself.

Smartphone Security Risks & Technology Solutions by Philemon Hini, Technical Ops; e-Crime Bureau

• The presentation was delivered by Mr. Hini, Cyber Analyst at the e-Crime Bureau, a cyber security and forensics firm. The session began with an introduction to the various operating system (OS) on the mobile platform; Android OS, iOS, Blackberry OS and other third-party OS usually a hybrid of existing operating systems. According to Mr. Hini, research reveals Android OS has more users; followed by Apple's iOS. Due to the open source nature of Android OS, app developers are able to develop malicious applications under the guise of useful software. He further explained that, mobile phones have become a platform for performing many daily activities which comes with associated risks like downloading malicious applications, connecting to unknown Wi-Fi, or even having the phone stolen.

• Mr. Hini indicated that that the use of smartphone apps has better security than using web browser versions. Keeping passwords on mobile phones is very important as it puts a level of security on phones, and it must be changed as often as possible. Phones to be discarded should be reset to factory settings to remove vital data from it, he advised. He recommended for regular review of application permissions since they may at times request more access to one's device than necessary.

• Mr. Hini demonstrated how malware infection can take place on a smartphone without the explicit concern of the user. Mr. Hini created an app which rested on his computer, and under the guise of charging his phone, he inserted a USB cord into his phone and connected it to his computer. After removing his phone, he realized an application has been installed on his phone which was a calculator. He neither downloaded it nor installed the app himself but it was operating on the phone as a calculator. From the back end he created on his computer, he was able to monitor the phone in real time. He had access to the phone contact lists, messages (SMS and WhatsApp), media gallery and other apps. The 'calculator' could also intercept his on-going calls and have them recorded at the backend. This was a demonstration of high level surveillance which could be started through basic social engineering schemes like charging someone's phone via USB.

• He recommended the use of strong/licensed antiviruses on phones and vigilance when installing apps on devices.

Dealing with Insider Threats-Technology Solution by Mr. Roger Oteng Baah, Internet Society of Ghana

• The presentation began with an insight to who an insider is: A trusted member of an organization who has access to detailed information from within the organization. Research shows that a lot of attacks in a corporation comes from within. Some of these may not be intentional as there may be instances where the computers may be left accessible to infiltrators.

• To demonstrate how regular update of password is very necessary, an instance was cited using Yahoo!'s request for all its clients to change their password. Those who did not change their passwords became vulnerable to intrusion and from a simple device such as a smartphone using google dorks, total access to Yahoo! Accounts whose passwords have not been changed in the past year. Insiders such as web developers can also pose threat to clients whose websites are left with gaps which can be penetrated by cybercriminals. Fired employees who held technical positions can be insider threats due to the desire for revenge. Ghana lost an estimated amount of US$50 million in cybercrime. These insider threats include credential theft, hanging transactions in e-banking which were mishandled, university grades being changed by insider accounts outside working hours.

• Insider threats can be controlled through denial of access, use of firewalls, using reactive measures such as punishments of perpetrators as well as control through the human interface.

Questions & Answers

Q - Technically, are we to trust MTN if they say mobile money fraud are not from insider threats?

A - Technically, one would need a lot of information to confirm such an issue, but there is always a possibility of insider involvement in fraud cases. You need investigations to be conducted to establish this, in the first place.

Issues of Digital Footprints and Digital Reputation by Dr. Ezer Osei Yeboah Boateng

• Establishing that everyone contributes to their digital image online, Dr. Boateng explained that whatever one does online connected by one's internet history either deliberately or not, makes up the digital footprints left behind.

• It is important to note that digital footprints are used in background checks by employers to examine prospective employees. It is also used by advertisers to make tailored adverts to market for people. Digital shadows are details about people which are not created by them and of which they have no control in creating. Once made, digital footprints are made, they are forever.

• Some negative implications of digital footprint can be the fact that

1. Information may be misinterpreted or blown out of proportion.

2. Advertisers may pick up too information and market undesired products

3. Loss of reputation

• According to Dr. Osei Yeboah Boateng, more digital footprints are left on smartphones than on computers due to IMEI numbers which are unique to the device and traceable to the SIM details. However, some highlighted misconception about online activities encompassed posting things on social media for the viewing of people within one's circles. Also, another misconception is the deletion, which is in reality temporarily masked and could be unveiled at any given time.

• Dr. Boateng advised that internet visits should be as anonymous as possible with security and privacy settings well reviewed. One must ensure all chats have end to end encryption, and any photo taken should be rid of metadata.

Questions and Answers

Q - What can be done about Facebook selling information to government and advertisers?

A - Facebook does not 'formally' sell data to government nor do advertisers, advertisers rather use cookies to pick information to be used in marketing.

Q - With digital footprints, how can one be secured on WhatsApp?

A - WhatsApp has end to end encryption but one has to be cautious.

SESSION B:

This session had a touch of private stakeholders enlightening the audience on the theme:

SecureGhCyberspace. Mr. C.K. Bruce; CEO of INNOVARE moderated the session with Mr. Bless giving the opening prayer. Mr. Paapa Arkhurst, Director, Chuck Solutions was present to act as a guide.

Opening Remarks

Mr. Carl Sackey, president of ISACA reminded the audience that National Cyber Security is a worldwide event observed in the month of October. He reiterated that its importance cannot be overlooked and as such there need for education and engagement with private-public partners. Mr. Sackey commended the government for his promise to allocate some funds for cyber security in the 2018 budget. Also, upholding the view of shared responsibility of all stakeholders, Mr. Sackey disclosed that ISACA and INNOVARE have come up with a new programme to train professionals who will acquire the necessary skills and knowledge to secure Ghana's cyberspace.

He introduced the key personalities who briefed the audience on the theme.

Remarks by Key Personalities

Mr. Sam Amanor, the CEO of BlueSpace Africa, stated clearly that technology is a tool to help us and how we use this tool matters a lot. In addition, he said that information is critical hence the need for cyber security.

Mr. Albert Antwi-Boasiako, The National Cybersecurity Advisor, reminded the gathering that cyber security is not a domain to be fought

by the "old mindset" of government effort only but the effort of private sector is key. He said the private sector's role will scale up cyber security. He mentioned that the institutional framework is composed of an inter-ministerial advisory council which includes seven (7) key ministers, a technical working group and a national cyber security committee which is yet to be set.

Dr. Paul Danquah, the Technical Director, IT Council Ltd presented on the topic: An Overview of Cyber Security in Ghana, A Researcher's Perspective. He obtained data from the law enforcement agencies and the information was on convicted and non-convicted cyber criminals. The findings of his research revealed that cyber criminals employ social engineering. The prominent trend is that organizations breached keep it to themselves. The National Communication Authority records a total mobile data subscribers to be about 20 million with a penetration rate of about 70%. Despite the various Acts on cyber security: Acts 772, 775 and 843, no record from the police is based on the law. The question to ask is: does it mean no one breached the law or they did but were not caught? Evidence of this research points out that there are inadequate logistic for forensic investigations. Also, knowledge on cyber security law is restricted to a few unit of the law enforcement agencies. Dr. Danquah said five years now the cyber security landscape will have changed thus, standard training is required for IT professionals, formidable information security database and finally institutions include security training.

Cyber Security Regulations in Ghana

The panelists included:

- Madam Patricia Adusei-Poku, Data Protection Commission
- Kenneth Adu-Amanfoh, National Communication Authority
- Dr. Paul Danquah, Technical, IT Council Ltd.
- Owusu Bediako-Poku, Ecobank Infossurance

The panel discussion took the form of question and answers. Owusu-Bediako-Poku started the discussion by commenting on the fact that Ghana has the best law but poor enforcement and proceeded to ask what can be done about it? The panelist unanimously said that there must be awareness creation about the law and skills training.

Owusu-Bediako-Poku quizzed Madam Patricia whether the Data Protection

Commission trains personnel within the commission or auditors from other firms. In response to the question, Madam Patricia said the Commission create awareness and as such every firm should make efforts in complying with the law.

Concerning the electronic transaction Act 2008, Owusu-Bediako-Poku asked Mr. Adu-Amanfoh whether the public is aware of such act. He responded that the National Communication Authority creates awareness among Internet Service Providers.

Furthermore, within the Electronic Transaction Act 2000, the moderator asked Dr. Danquah whether we are aware of what is expected of us in the light of cyber security policy. Dr. Danquah replied that there are so many information security professionals but there is the need for dynamism in the field for us to fully appreciate the cyber security policy.

Owusu Bediako-Poku again asked the banks regulated by Bank of Ghana are aware of the controls in protecting vital information. Mr. Adu-Amanfoh said that the central bank's effort in that respect is commendable, however, there is more room for improvement.

When Owusu-Bediako asked what the plan is to control health-related data, Madam Patricia said that a large proportion of the health-related data are in the manual form. Also, the Commission has recently launched series of database to ensure safe-guarding of such data.

"Does National Communication Authority play a role with Bank of Ghana?" asked Owusu-Bediako-Poku. Mr. Adu-Amanfoh replied affirmatively that the authority regulates the spectrum and the Central Bank takes care of the financial aspect.

Last but not least, the host asked what can be included in the regulation. Dr. Danquah said in response to the question that the regulations should comply with international standards and then it should be localized.

For the closing remarks, Madam Patricia said all stakeholders should train people to protect data and she entreated the audience to get in touch with the Commission. Kenneth Adu-Amanfoh also mentioned remarked that the policy is ready and a multi-stakeholder approach should be used to implement it.

Key Elements of an Efficient Cyber/Information Security Programme

Mr. Bruce, CEO of Innovare educated the audience on Key Elements of an Efficient Cyber/Information Security Programme. He defined ISO 27001 as a standard for Information Security Management System. Information Security requires the commitment of top management as the top-down approach to enhance proper

governance. He highlighted that the values of IT asset management are responsibility, accountability and the reducing the incidence of people with questionable moral behavior.

Profiling System users using Digital Forensics

Mr. Alex Oppong; Principal Consultant, e-Crime Bureau gave a presentation on the topic: Profiling System users using Digital Forensics. He said we leave digital footprint wherever we go and what digital forensics does is to collect and examine digital evidence residing on electronic device in a way that is legally accepted. A forensic expert must identify what files and application users are accessing and then do a full analysis using forensic tools like Encase Forensic, FTK, Autopsy Cyber cop, Belkasoft among others.

Capacity Building on Security Blueprint

Mr. Victor Addison, Lead Security Consultant, Bluespace delivered a presentation geared towards Capacity Building on Security Blueprint. He complained that often training is focused on top managers who rarely support staff's education. Mr. Addison opined that for a reliable security blueprint, there need to be a security team of experts. These cyber security professionals have specific roles to play such as monitor user activity, perform periodic audit and assessment of the organization. He concluded by listing the domain for cyber security, among them are IT governance& risk management, access control, network security, mobile security, physical security and cryptography.

At about 4:45pm, the Chairman gave the closing remarks, highlighting a few things worth noting. Without any further contributions and questions, the session ended at about 5:00 pm.

SESSION C:

Workshop by the Security Governance Initiative (SGI) and National Information Technology Agency (NITA)

• The workshop was organized by the SGI, a cyber security collaboration between the United States and the Government of Ghana and the National Information Technology Agency (NITA) at the Kofi Annan Centre of Excellence in ICT. The moderator for this event was Mr. Kwadwo Osafo-Maafo from the National Communications Authority (NCA).

• The workshop began with opening remarks by the Chief Technical Officer of NITA, Mr. Kofi Otchere and Mr. Eric Akumiah of the Ministry of Communication.

•

CSIRT Development

• The first session started with a presentation by Tracy Bills of the Software Engineering Institute of Carnegie Mellon University on the topic Foundational Concepts of Computer Security Incident Response Team, CSIRTs.

• She defined incident management as well as the model processes

involved. Incident management was described as the ability to provide total management of events and incidents across an enterprise that affects information and technology assets within the organization. Ms. Bills explained that, incident management functions can be performed by IT staff, HR staff, auditors, criminal investigators, victims or involved sites, just to mention a few.

• Ms. Bills explained that, CSIRT as an organization provides services and support to a defined constituency for preventing, handling and responding to computer security incidents and communicates information assurance-related information to its constituency. So in general CSIRTs provide a single point of contact for reporting cyber security problems as well as identifying and analyzing what has happened including the impact and threats and finds solutions while creating some awareness to minimize and control the damage.

CSIRTs also operates to prevent such events from happening in the future. She also made us understand that all CSIRTs are different in the sense that one does not fit for all so you take what makes sense for your situation. Ms. Bills explained the five general stages of CSIRT development. The first is educating the organization followed by the planning effort then implementation of the plans, operational phase and finally the evaluation and improvement.

She explained that, National CSIRTs are those that have been designated by a country to have specific responsibilities in cyber protection for the country. They have the ability to serve more than one constituency like government organizations and the public in general. Ms. Bills also discussed the key principles of developing CSIRTS.

CSIRT Outreach and Communications

• Ms. Tracy Bills representing the also presented on the common principles of outreach and communication in CSIRT operations. According to her, these are to build trust among internal and external partners, provide constituents with relevant information, and provide subject matter experts advice to inform decision makers as well as understand the needs of partners.

• She discussed about the planning considerations for outreach and communication. First of all, she advised that one needs to identify the specific need in order to have the right CSIRT for communication purposes as there are different CSIRTs for different purposes. For instance, a product CSIRT will require communications to focus on information necessary to help their customers mitigate issues with their products whiles a national CSIRT will require communications to focus on broad topics intended to improve

the overall cyber security posture of the nation.

• Also, in planning an outreach and communication team, your primary audience should be considered that is both internal stakeholders like upper and middle management, software development groups and human resources as well as external stakeholders or partners like affiliates, contractors, vendors and law enforcement agencies. The information you provide is also important. This includes high-level details, technical details, available resources, the extent of damage reported and many others.

Cyber security within the Public Sector

In the third session, there was a presentation by Kweku Kyei Ofori, Acting Deputy Director General for NITA on cyber security within the public sector. According to his presentation, the public sector faces a number of cyber security challenges including lack of awareness, lack of skillset in cyber security, lack of standardization and almost non-existent incident management system to support CSIRT operations.

Mr. Ofori mentioned that, NITA intends to address some of these cyber security issues by training enough people for IT roles for government institutions. This is because we need to develop the public sector IT team and equip them to ensure the security of government e-government initiatives.

Questions and Answers:

Q- Does the CERT share their difficult experiences and lessons they had to learn the hard way?

A- Yes they do. There are books and other materials online that have captured these challenges they faced.

Q- What is SOC?

A- These are Security Operations Centers that are sometimes more focused on the networks that are running and have incident response functions as well.

DAY 5

CYBERCRIME, CYBER HYGIENE & AWARENESS

SESSION A:

Cyber Trends in Ghana by Dr. Herbert Gustav Yankson, Head, Cyber Crime Unit, CID HQ.

- Crimes have now become borderless and nonphysical according to the CID head of the Cyber Unit.

- According to the CID, The cybercrime landscape in Ghana currently are as follows; cyber fraud, cyber stalking which involves harassment, web attacks, hacking, data breach where normally some banks and financial institutions are targeted. There is also the unpleasant situation of insider threats where employees connive with external perpetrators to commit attacks. The insiders know the loopholes in their organizations and sometimes send confidential information out to these criminals. Other issues include publication of fake news and child pornography.

- Dr. Yankson also raised issues about ATM fraud, SIM boxing as well as various impersonations and identity fraud on social media platforms including Facebook.

One of the most widely spread malware that people are not aware is malware which normally comes with online adverts, once you click on such malicious programmes, they execute to infect the target systems

- According to the CID, 419 scams are still leading with the number of cybercrime cases reported followed by social media fraud and mobile money fraud.

- According to the CID, job losses and money laundering are some effects these criminal activities have brought to bear. He advised business to train their employees on cyber risks in addition to background checks on their key staff, including IT officers.

- He advised the citizens to report cybercrime cases to the police for assistance.

Awareness of cybercrime legislations by Francis Blay, Certified Information Systems Security Personnel

• The presenter voiced out how impressed he was on the presentations done and the success of the conference as compared to others he had attended outside Ghana. He iterated the President's keynote address during the opening ceremony of the 2017 National Cyber Security Week that cybersecurity practitioners should explain cybersecurity in very simple terms. He presented a simple demonstration on "How do they get to you".

• He remarked that somethings are presented as legitimate but in reality, contains malware. Since one cannot control what they do not know, one must be careful when accessing some applications.

• He stated that it is very vital to keep backups to help with incident response.

• He advised that a complex password must be with mixed characters and change it regularly (90 days for corporate entities). Password recovery questions are very essential since answers may be exposed on social media, he added.

• One should maintain a regular website for specific functions. He also advised that sensitive data should not be exposed on public Wi-Fi. In conclusion, he recommended that software should be updated often to patch up vulnerabilities.

Cyber Security and Universal Access - GIFEC Perspective by Yahaya Zakaria Osman, Ghana Investment Fund for Electronic Communication (GIFEC)

Mr. Zakaria Osman thanked the National Cyber Security Secretariat for organizing this very important event and recognizing GIFEC as a key stakeholder. He indicated that GIFEC is established by the Electronic Communications Act, 2008, (Act 775).

• Among other functions, GIFEC provides financial resources for the establishment of universal service and

access for all communities. It also facilitate the provision of basic telephony, internet service, multimedia service, broadband and broadcasting services to these communities.

• According to him, the internet has created a new domain (cyberspace) that has revolutionized the world we live in. Ghanaians have become more connected to the internet with the explosive growth in the use of computers, smartphones, PDAs, electronic devices and other communication equipment.

• Very unfortunately, this new domain is being used not only by ordinary people in managing the complexities of the modern life, but is also being used by criminals and terrorists to commit crimes. According to him, committing crime has now become a lot easier. What is even more disturbing is that, the cyberspace has made it possible for cybercrimes to be committed from anywhere at any time anonymously.

• He indicated GIFEC's commitment towards building a resilient cyber security for Ghana through cooperation and information sharing with other government agencies and non-governmental stakeholders.

Cyber Security Awareness in the Public Sector (1)
by Mr. Angel Hueca, Software Engineering Institute (SEI)

• The presentation by Mr. Angel Hueca from the Software Engineering Institute (SEI) on the topic Cyber Security Awareness For Various Audience described cyber security awareness as having an understanding of what these cyber threats are and taking the right steps to prevent them.

• This awareness applies to students, parents and educators, young professionals, businesses, government, law enforcement and many others. According to him, people are susceptible to these scams on a daily basis because they are mostly not aware of these threats. Cyber security is therefore very important, he emphasized.

• It is also important to note that threats do not discriminate so all users are susceptible to cyber-attacks hence the need for cyber security awareness. Cyber security awareness is very difficult because of the human factor. Malicious actors are very skilled at social engineering and human error is responsible for about 95% of all security incidents. Some employees are also unable to identify suspicious activities online, he indicated.

• He indicated that, the European Union also came up with a catchy phrase for the cyber security month in October 2017 called "Be Aware, Be Secure." This was also to generate

general awareness about network and information security, to promote safer use of the internet and build a strong track record. Another phrase from Canada was "Get Cyber Safe" to create awareness.

• The United Kingdom version of this campaign was called "UK Get Safe Online." This source was made up of unbiased, factual and easy-to-understand information on online safety. Australia also came up with "Stay Smart Online" where simple to understand advice on how to protect oneself online as well as up-to-date information on the latest online threats and how to respond were provided to citizens.

• He advised Ghana to adopt a similar approach to enhance awareness campaign efforts.

Cyber Security Awareness in the Public Sector (2)

by Mr. Kofi Otchere, (NITA) and Mr. Osafo- Maafo, (NCA)

• Mr. Kofi Otchere and Mr. Osafo-Maafo, both from NITA presented the second part of this topic. They advised that before assessing the internet, one must have some idea of how to secure one's self online. First one has to make sure that the password being used is secured.

• Again, normally at public places where there are free wireless, one must be careful when accessing it. Most of them are not secured and so he advised that if you feel you have some confidential things on your phone then is better you do it somewhere.

• He advised that there is the need to log off from our mails every time even if the devise being used is a personal one.

Doing otherwise makes because us vulnerable to some attacks.

• It was advised that, whenever we receive emails we need to be very vigilant and exercise some form of due diligence. Criminals may get hold of your personal details such as bank account details and try to outsmart you. One way to be vigilant is to exercise some level of diligence by taking some time to verify any information you are unsure of.

• Some companies auction their computers without knowing that they are giving information to someone for free. So he advised that before one dispose of computer systems, one needs to make sure the system is completely wiped because if some data is leaked out, criminals could use that to attack them.

• Mr. Otchere of National Information Technology Agency touched on what NITA does. He explained that NITA has a role to ensure the various Ministries and Agencies are secured in the cyber space. NITA works in partnership with National CERT he added.

• The presenters advised businesses to ensure that their staff are given some awareness training.

Panel Discussion: Responsibilities in the Cyber Space (People, Business and Government)

The session was moderated by Mr. Abel Yeboah-Ofori, Cyber Security professional. Panelist included:

- Mr. Victor Nyamadi Gordon, National Computer Emergency Response Team
- Mr. Benjamin Cobblah, University of Ghana- I.T Security and planning
- Mr. Serge Phillipe, Country CEO, of Standard Chartered Bank, Cote d'Ivoire

- Mr. Eric Akumiah, National Computer Emergency Response Team
- Mr. Osafo- Maafo, National Communications Authority (NCA)

Mr. Eric Akumiah stated we must identify the risk to be able to find the solution. We must first look at the risk factors and steps must be taken to mitigate them. For instance, when it comes to business we must try to protect trade secrets, data informatics etc. especially when it comes to the bank. He added that the National Cyber Security Secretariat has now been setup to oversee cyber security implementation at the national level.

Mr. Cobblah suggested that if individuals are made aware of their contribution to the cyber space, they will begin to appreciate why they have to be responsible for the security in the cyber space.

It was suggested that government can take up its responsibility on cyber security by ensuring the setting up and operationalization of CERTs.

Mr. Cobblah suggested to look at the issue from the educational perspective. He believes from child hood when an individual starts schooling through to secondary to tertiary, little effort is made when it comes to creating cyber security awareness. He preferred that some measures are put in place to ensure when students get online or on the web, they look out for certain traits that raise suspicion. A case in point according to him is when a student was told to have gotten admission to the school only to realize he has been tricked after he has paid money as registration fees to some bank account which was provided to him by fraudsters, as it was later discovered.

Mr. Philippe explained that cybercrime has become a global issue and therefore Ghana needs to cooperate with other countries to fight the menace.

Panelists suggested to participants to adopt a culture of cyber security. This applies to individuals, organizations and the government.

Computer Security at the Workplace- Round Table Discussion

This session focused on a brief round table discussion on the challenges faced by MDAs in securing their cyber space. Mr. Luqman Mahama of NITA moderated the session. Participants included representatives from the Cyber Security Division of the National Communications Authority, the Kofi Annan Centre of Excellence in ICT, the Software Engineering Institute, Ghana Revenue Authority, University of Ghana Computing Systems, the Royal Bank and the Ghana Immigration Service.

The under-listed are highlights from the discussion

- Most people see cyber-security as a financially intensive endeavor as it involves a lot of buying of firewalls, antivirus software and many others. However, we should know that cyber-security is big business for hackers hence the need to develop strategies to solve these network issues.
- It was discussed that, top management buy in is required for effective implementation of cyber security initiatives at the corporate level.
- Businesses were advised to invest in cyber security especially in the area of staff training, cyber security technology and other capacity building programmes
- Panelists advised businesses to implement cyber security and data protection policies.

Social Media- the Good, the Bad and the Ugly

by Prince Adu- President of the Young Professionals of ISACA

Social media has become a vital part of the day to day activities of the average person in the digitally evolving world. It has merits such as connecting with old friends, current news, entertainment and even job employment offers.

But social media has also been the cause of social anxiety, depression, low productivity and loss of jobs. Businesses with Facebook accounts could be compromised when the Social Media Administrator leaves the company hence access should be changed as soon as possible, he advised.

Cybercrime has also infiltrated social media and as such, much caution is needed when using social media. It is advisable to look out for signs of verification before following some accounts. Giving too much information on social media may be imprudent, it was advised. It is smart to check permission settings on external apps added to social media as they may be either tools for malware or a tool to subvert social media accounts. The following are tips to follow on social media:

- Be skeptical
- Check privacy setting
- Use different passwords for different accounts
- Think before you post
- Be wary
- Stay updated
- Educate others

See Technology, See Risks by Mr Ebo Richardson- Chief Information Security Barclays Group Ghana

• The presentation was aimed at the challenges professionals face when they move into modern technology to make business transactions easier. He cited an instance where a SME which used to transact simple business by producing and selling will move into web systems to market their products and account for their sales, exposing the business to cyber and therefore putting it at risk.

• Though he recommended how some technological risks can be tuned to positives, he brought to light how dreadful some of these risks can develop. The session became interactive with various points of view from participants.

• In mitigating risks, he advised against unauthorized disclosure of information and scaling up of security measures against malware. To ensure the effective moderation of negative risk, one needs an effective framework of monitoring, reporting, and taking good decisions since significant value can be created as opposed to material damage when such risks are not controlled.

• A case was shared as there are times where security may be relaxed to give staff the chance to upgrade to the novelty. It was advised that no loopholes were to be created in such situations to allow unwanted infiltration of both internal and external attackers.

Virus Entry Points- We Open the Doors

by Michael Kwofie- Group Manager for Business Information Security, Ecobank Ghana

The presentation was meant to explore the ways through which people leave room for malware to infiltrate a system and the means by which it can be controlled. He begun by distinguishing between the various types of malicious software:

• Adware- malware presenting itself as adverts

• Spam – unsolicited email

• Spyware- spies and copies information to remote server

• Trojan- applications that hold malware attached

• Zombies- malwares that lay dormant till it is triggered by an action of the user as part of its formation

• Worm- malware that moves in networks to accomplish malevolent tasks.

• Recent events show malware attacks are being targeted at specific corporate bodies and they are granted access through various weakness such as human weakness like social engineering, misconfiguration and vulnerability.

• The use of USB is a common way of infiltrating one's network, as well as instant messaging and social media where information is shared. Mr. Kwofie displayed a timeline of malware over the years to 2017 where ransomware has become a big deal in cybercrime.

• He also refuted the fact that Linux and Apple based operating systems (OS) are not susceptible to malware attacks since over the years they have been proven to be vulnerable. He advised businesses to patch up system vulnerabilities with urgency when updates are released.

• Ultimately, in order to prepare against malware attacks, one needs to patch up software as soon as updates are released, back up vital data more than often, and also create awareness among system users.

Data protection, what can we do?

By Victor Nyamadi, Professional fellow, Commonwealth Telecommunications

• Due to exposure of oneself on the internet, data from individuals are being used in ways to exploit people such as to advertise specific goods or services to them.

• Data controllers should handle personal data collected with the utmost security measures. The Data Protection Act requires that data breaches must be reported but unfortunately, some companies do not report such incidents. The following data protection best practices are recommended:

• Restrict access as much as possible

• Availability of data to only authorized personnel

• Password protection

• Monitor access around data

• Take necessary steps to remove unwanted access

• Store data in secure storage which is isolated from network. E.g. pen drives

• Delete information from any device before handing it over to third parties

• It is vital to practice cyber hygiene

• Report data breaches to the Data Protection Commission or the National CERT

SESSION B:

Workshop by e-Crime Bureau & AfricaCert

In line with the NCSW theme - "Securing Ghana's Digital Journey," e-Crime Bureau partnered with AfricaCERT to organize a workshop to sensitize IT professionals with techniques, tactics and processes related to Network Forensics and Incident handling.

• e-Crime Bureau is a cyber security and digital forensics firm with services in cyber security consulting, cybercrime investigations and litigations support, financial crimes management and training among others. AfricaCERT is the pan-African institution aimed at coordinating CERT activities across the continent.

• The subject matter for this workshop was chosen in recognition of the spate of cyber threats targeting businesses in Ghana today. With the government's vision to use technology

as a key driver of economic growth, the need to bring relevant professionals up to speed with how to deal with everyday cyber threats is key. e-Crime Bureau and AfricaCERT carefully selected thematic areas for the workshop which are referred to below.

• The objectives of the workshop was to expose participants to practical case studies and real-world scenarios that cover identification and investigation of attacks on networks; equip participants with requisite skills relating to forensic investigations and incident response on corporate networks; enhance the skillset and knowledge base of participants to practically identify network threats and maintain secure IT infrastructure and services and to provide participants with skills in investigating logging systems as well as network devices for electronic evidence which can be admissible in the court of law.

The workshop covered the following thematic areas:

• Concept of Cyberspace, Cyber Security and Cybercrime

• Computer Security Incident Response Team (CSIRT – Introduction)

• CSIRT Organizational Framework

• CSIRT Services and Tools Selection Mechanism

• Cyber Security Incident Handling Process

• Computer Network Breaches & Investigation Procedures

• Practical Network Investigative Strategies

• Network Traffic Analysis

• Network Forensics Tools

• About twenty (20) IT professionals from key corporate institutions participated in this free workshop. Participants came from Securities & Exchange Commission (SEC), National Insurance Commission (NIC), Ghana Revenue Authority (GRA), Volta River Authority (VRA), Ghana Civil Aviation Authority (GCAA), National Pensions Regulatory Authority (NPRA), Goil and CalBank.

• During the workshop participants were allowed to discuss issues that affected them as IT professionals. There were a number of issues that the participants raised which can however be summarized under the following broad areas:

• There is a general lack of skills in digital forensics and incident response among IT professionals;

• Participants raised concerns about the current situation of CERT, as very few businesses and individuals are aware and have limited knowledge

about the infrastructure;

- Capacity building in digital forensics and incident handling is required particularly among public sector institutions.

- This workshop was beneficial to participants because they acquired techniques in monitoring traffic using open source tools, acquired skills in conducting packet analysis and detection of network attack and gained knowledge in review of network device controls.

- Some contributions to National Cyber Security Agenda were made and they include to develop a culture of cyber security that is critical to preventing network related breaches; to create a foundation for incident response; to improve the forensic capabilities of professionals to investigate existing and potential cyber-threats and to provide best practices in digital forensics in line with required international standards.

Summary of Conclusions & Recommendations

On the last day of the event, Friday 27 October, the Minister for Communications, Hon Ursula Owusu-Ekuful presented the summary of Conclusions and Recommendations from the event.

Below highlights the key themes and recommendations presented:

DAY 1: Cyber Security Governance

1. The President announced plans by government to set up a National Cyber Security Centre (NCSC) to coordinate national cyber security operations.

2. The Minister for Communications inaugurated the National Cyber Security Technical Working Group (NCSTWG) and advised the group to collaborate effectively to achieve Ghana's cyber security goals.

3. The President underscored the need for capacity across all sectors to mitigate the current threats from cybercrime.

4. Ministers for National Security, Defence, Attorney-General and Interior were among top-government officials who participated in the official opening of the event.

5. Security Governance Initiative (SGI) organized a Stakeholder Mapping

Workshop for representative of the NCSTWG. The Workshop was organized to help develop a Charter for the operationalization of the work of the working group.

6. The President inaugurated the National Cyber Security Inter-Ministerial Advisory Council (NCSIAC).

7. The draft National Cyber Security Institutional Framework was presented to the public by the National Cybersecurity Advisor.

8. Participants and stakeholders recommended for the development of cyber governance in both the public and the private sector.

DAY 2: Conferences & Workshop Sessions

1. Representatives from the Council of Europe, ECOWAS Commission and other stakeholders presented on specific thematic areas including regional and international cooperation and security of critical infrastructures.

2. There is the need for continuous sensitization and cooperation among ECOWAS member states to improve upon the sub-regions cyber security environment.

3. International cooperation such as police to police, international judicial Cooperation and interactions with international service providers (such as Facebook, Google, etc.) must be strengthened.

4. The cyber security framework developed by the government should be a 'living document' that will adapt to change.

5. Stakeholders recommended for the government to accede the Budapest Convention and the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention) to enhance regional and international cooperation on cybercrime investigations and prosecutions.

6. Engagement with both the public and private sector on the need for forensic readiness is important for Ghana's cyber security readiness.

7. Government should prioritize its efforts to protect Critical National Information Infrastructures (CNIIs) from cyber-attacks.

8. Government is advised to partner with tertiary institutions in providing certification for cyber security courses to be taught in order to build cyber security capacity of the country's workforce.

DAY 3: Child Online Protection

1. Empower children and young persons and also care givers to know how to navigate the internet safely and responsibly.

2. Enforcement of legislations to punish perpetrators of crime against children on the internet is recommended.

3. There should be just one unique helpline to address child online related issues.

4. Computer ethics should be included into syllabus for schools, across all levels, it was suggested.

5. A team should visit schools to educate students periodically on cyber security related subjects, participants recommended.

6. There should be a full representation of the Ghana Education Service in the next edition of the cyber security week to further deepen consultations and deliberations on COP issues involving school children.

7. Media should not expose children who have been abused.

8. Responsibility for industry or service providers should be clearly spelt out to make them accountable for COP.

9. Implementation of Ghana's Child Online Protection framework was recommended during the session on COP.

10. Social media based COP awareness creation programmes were suggested.

DAY 4: Cyber Security Technology Solutions

1. There should be a central point to collate credible data for cybercrime and cyber security analysis.

2. Businesses should play an active role in enforcing data protection provisions (Act 843).

3. There is a need for standardization and compliance to international standards such as ISO 27001, NIST, etc.

4. Stakeholder engagements on cyber security should be done more frequently, with all stakeholders' involvement.

5. Top management and executives must show interest in cyber security and they should be involved in building capacity of their staff.

6. Businesses were advised to implement appropriate cyber security solutions to address the technology components of cyber security issues facing businesses.

7. Individuals, businesses and government are advised to invest in cyber security.

DAY 5: Cybercrime, Cyber Hygiene & Awareness

1. Cyber security units should be established across the regional

capitals of the country to enhance effective investigations and prosecutions of cybercrimes.

2. Private sector engagement should be enhanced to support government efforts in the fight against cybercrimes.

3. Stakeholders recommended to government to step up national efforts develop a culture of cyber security across the government itself, businesses and individuals.

4. Regulations on crypto-currency were recommended by some participants.

5. Involvement of religious and traditional leaders in the fight against cybercrime was recommended.

6. Cybercrime awareness and outreach programmes are recommended in order to reach many target groups as part of national cybercrime awareness campaigns.

7. Organizations were advised to organize cyber hygiene programmes for their staff on regular basis. This is expected to help improve employee awareness of cyber risks and expected behaviors in the cyberspace.

8. Stakeholders recommended for the creation of a dedicated point of contact to report cyber security incidents.

President Akufo-Addo (3rd right) in a group photo with the members of the National Cyber Security Inter-Ministerial Advisory Council (NCSIAC) at the opening of the 2017 National Cyber Security Week in Accra

1. Hon. Ursula Owusu-Ekuful, Minister for Communications
2. Hon. Gloria Afua Akuffo, Minister for Justice & Attorney General
3. Hon. Albert Kan-Dapaah , Minister for National Security
4. Hon. Ambrose Dery, Minister for the Interior
5. Hon. Dominic Nitiwul, Minister for Defence

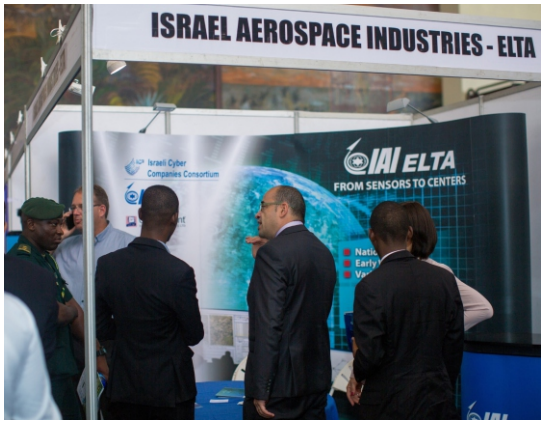
President Akufo-Addo (middle) in a group photo with some dignitaries at the opening of the 2017 National Cyber Security Week in Accra

From left: Mr Isaias Barreto De Rosa, ECOWAS representative
Mr. Manuel De Almeida Pereira, Council of Europe representative
Mrs. Rashan Muntaza, UNICEF representative
Hon. Ursula Owusu-Ekuful, Minister for Communications
Mr Albert Antwi-Boasiako, National Cybersecurity Advisor
Mr. Robert P. Jackson, US Ambassador to Ghana

Some Selected Photos of the event

NCSW 2017 Exhibitions

NCSW 2017 Exhibitions



National Cyber Security Week
Event Planning Committee Members

1. **Hon. Vincent Sowah Odotei**
   Ministry of Communications
2. **Albert Antwi-Boasiako**
   National Cyber Security Secretariat
3. **Eric Akumiah**
   CERT-GH
4. **Patricia Adusei-Poku**
   Data Protection Commission
5. **Katherine Headley**
   US Embassy Ghana
6. **Awo Aidam Amenyah**
   J Initiative
7. **C.K Bruce**
   Innovare
8. **Gustav Yankson**
   CID
9. **Alex Oppong**
   E-Crime Bureau
10. **Nana Defie-Badu**
    National Communication Authority
11. **Valerie Hudson**
    Ministry of Communications
12. **Rhoda Gavor**
    Ministry of Communications
13. **Kwadwo Osafo-Maafo**
    National Communications Authority
14. **Owusu Bediako-Poku**
    ISACA Ghana Chapter
15. **Derek Laryea**
    Telecoms Chamber
16. **Patricia Adafienu**
    CERT-GH
17. **Louisa Efua Hughes**
    National Cyber Security Secretariat
18. **Eno Brago Attrams**
    National Cyber Security Secretariat
19. **Adwoa Assan**
    Ministry of Communications
20. **Daudi Yahaya**
    Ministry of Communications
21. **Nuhu Mahama**
    Ministry of Communications
22. **Nana Ntim**
    Ministry of Communications
23. **Yawa Haligah**
    Ministry of Communications
24. **Machel Davids Fearon**
    State Protocol

National Cyber Security Admin Team

Patricia Adafienu

Eno Brago Attrams

Rhoda Gavor

Louisa Efiua Hughes

Valerie Hudson

Elizabeth Mante

Sponsors

PLATINUM

IAI ELTA

GOLD

Rayzone Group

BANK OF GHANA EST - 1957

unicef

UNDP

SILVER

Deloitte.

margins GROUP

BRONZE

MTN

KPMG

SpearHead

SUPERTECH LIMITED
Ghana's Leading Company in Cyber Defence

HYSEN
www.hysen.info

GENERAL

EY
Building a better working world

KAYMERA
Mobile security redefined

SKYLINKS TECHNICAL SERVICES LTD

Partners

GHANA CHAMBER OF TELECOMMUNICATIONS

NATIONAL CYBER SECURITY WEEK

The National Cyber Security Week (NCSW) is an annual event by the Ministry of Communications to raise awareness of cybercrimes and the importance of cyber security to individuals, businesses and government. The event brings both local and international stakeholders together through various initiatives and activities to ensure a secured cyberspace for Ghana. The event is one of the initiatives to secure government's investments in digitalization of the economy.

NATIONAL CYBER SECURITY CENTRE

Securing Ghana's Digital Journey...

Ministry of Communications
Website: www.cybersecurity.gov.gh
E-mail: info@cybersecurity.gov.gh
Tel: +233 (0) 50 318 5846
Digital address: GA-079-0539