Media Foundation for West Africa

Policy Brief

Policy Recommendations on Trending Cybersecurity Developments in Ghana

Supported by: GLOBAL PARTNERS DIGITAL

Introduction and background

The world is getting ever smaller as the internet continues to connect billions of people across the globe. Indeed, the internet plays a crucial role in every aspect of human life. Even though billions are still unconnected, penetration rates are increasing across the world. Ghana, for instance, can boast of over 15 million internet users (an estimated 53% penetration rate) as at Janaury 2022 according to data from Statista.[1]

As connectivity to the internet is increasing, so is cybercrime. Safety and security in cyberspace have, therefore, become critical issues of global and local concern.

Stakeholders within the internet and cybersecurity ecosystem, especially governments, are continuously engaging and discussing ways of increasing stability and security of cyberspace. This has become extremely necessary as reports continue to show the damaging effects that cyber attacks are having on critical national infrastructure, including those of government, tech and telecom companies, financial and educational institutions, among others. According to statistics from Cybersecurity Ventures, cybercrime damage totalled US$6 trillion globally in 2021 – which is estimated to be twice as high as the GDP of all African countries. The damning impact of cyber attacks do not only have economic consequences, but humanitarian and national security stakes as well. Cybersecurity, thus, needs a holistic approach that brings on board the different stakeholder groups in the ecosystem.

The Freedom Online Coalition defines cybersecurity, as "the preservation – through policy, technology and education – of the availability, confidentiality and integrity of information and its underlying infrastructure so as to enhance the security of persons both online and offline." It is, therefore, necessary to ensure the right balance of the issues of protecting national security, critical national infrastructure, economic considerations and human rights in the pursuit of creating and sustaining a stable and secured cyberspace.

This explains why at the global level, the UN Group of Governmental Experts (GGE) and the Open-ended Working Group continue to explore the issue of responsible state behaviour in cyberspace. At the regional and national levels, also, interventions are being made to ensure the protection, stability and security of critical national infrastructure and overall national security in online spaces. A number of them, including Ghana, have introduced cybersecurity

[1] Internet penetration in Africa January 2022, by country, Statista, accessed May 20, 2022, https://www.statista.com/statistics/1124283/internet-penetration-in-africa-by-country/

laws and other regulatory interventions to regulate and develop the sector.

This policy brief highlights developments in the cybersecurity ecosystem in Ghana and calls on policymakers and other stakeholders to collaborate to ensure safety and security of Ghana's cyberspace while respecting human rights.

Cybersecurity at the global level

Cybercrimes are activities perpetrated by criminals onli ne that affect the integrity and security of cyberspace. These crimes take many forms such as phishing, doxing, identity theft, hacking, spamming, distribution of child pornography, sextortion, among others. Nefarious and fraudulent activities in online spaces do not only harm individuals and violate rights, they also impact national security and the stability and intergrity of information and critical infrastructure. In the interest of international peace and security in the field of ICTs, the UN has put in place mechanisms to promote stability and security of cyberspace. The UN Group of Governmental Experts (GGE) and the Open-ended Working Group are two of such mechanisms.

In 2015, the GGE agreed on eleven voluntary, non-binding norms for responsible behaviour of States in cyberspace. The norms are aimed at promoting an open, secure, stable, accessible and peaceful ICT environment. The norms were adopted by the General Assembly and subsequently endorsed by all Member States, including Ghana. Member States are, thus, expected to implement these non-binding global norms at the national level to foster cybersecurity and also, to demonstrate their commitment to responsible behaviour in cyberspace.

The Open-Ended Working Group (OEWG) was set up in 2018 to examine relevant international concepts in order to strengthen the security of global information and telecommunications systems. Its work also revolves around assessing the work and recommendations of the GGE in the areas of awareness of information security issues; developments in the field of information and telecommunications in the context of international security; national level efforts to strengthen information security and promote international cooperation; and measures that could be taken by the international community to strengthen information security at the global level.

Ghana has been engaging in these processes and making relevant contributions on the need for states to act responsibly in cyberspace while respecting the rights of netizens. For instance, in September 2019, Ghana made the following statement at the OEWG - "A responsible state behavior in the cyberspace can only be realised in an environment where rules, norms and principles exist and are consistent with human rights, the rule of law and the protection of the digital rights of citizens."

Cybersecurity and related issues in Ghana

Ghana is recognised globally for its knowledge and expertise in cybersecurity issues and management. The country served on the UN Group of Governmental Experts until 2021. The country is considered a leader in cybersecurity and related issues in the West Africa region. Ghana is ranked third (3rd) in Africa and 43rd in the world on the Global Cybersecurity Index by the International Telecommunication Union (ITU).

Despite its expertise in this area, the country continues to face challenges with cybercrimes. With the rising internet penetration rate in the country (50% as at January 2021), more Ghanaians are connecting to the internet. Unfortunately, there is a corresponding rise in cybersecurity breaches in the country in the form of identity theft, banking fraud, doxing, distribution of child pornography, among others.

Trends in cybersecurity breaches

Cybercrimes in Ghana have evolved over the years from basic romance scams targetting unsuspecting foreigners and even the wealthy in Ghana and the diaspora to trade in minerals (gold or diamond-buying schemes) to mobile money fraud, fake online e-commerce activities and quick money schemes.

The current phenomenon of fraud is mainly perpetrated through mobile money (popularly referred to as momo) platforms operated by the telecommunication networks in Ghana. The criminals send messages indicating a transfer has been made to the unsuspecting victim and follow up with calls instructing them to unveil their momo PINs or resend the said transferred amount (which was never done) to their [criminals'] wallets. In some instances, instructions are given for tokens to be generated to be withdrawn by the perpetrator at a payment point.

Another emerging trend is the setting up of fake online or e-commerce shops via some social media platforms, particularly Instagram. On such social media platforms, several merchandise are put up for sale with the caveat that clients need to pay for the items bought before delivery is made. The means of payment is usually via momo. Once the client makes payment, the fake online shop blocks the victim's number or the online shop account is pulled down to prevent the victims from reaching the fraudulent online shop.

Also, Whatsapp accounts without "the 2-step verification" are hacked by some criminals who send messages to individuals or groups about quick money schemes such as “World Remit” to get unsuspecting victims to transfer an amount of money to an account for the amount to be doubled or tripled. Unfortunately, the victims whose accounts are hacked for such fraudulent activities do not inform their contacts or authorities of the crime and this leads to multiple hacks of other WhatsApp accounts the victim is linked to. In other instances, the hacked accounts are used to make online payments which lead to loss of funds once the payment is authorised on the victim’s phone.

Impersonation or identity theft across social media platforms, particularly, Facebook is also on the rise in the country. The modus operandi of the perpetrators is to create or clone an account of someone’s social media profile, and use it to send out a request to males or females proposing a relationship. At the point where private images or some damaging information is obtained from their target victim, they make demands for money by threatening to go public with the private images if the sum demanded is not paid.

At the corporate or institutional level, cyber fraud and scams persist, even though organisations continue to upgrade their security measures. Attempts are still made to defraud financial institutions. In particular, Business Email Compromises scamscontinue to plaque businesses in the country and elsewhere on the globe. Some originate from the country[2] while others are from other parts of the world. Fortunately, the number of attempts made on these institutions have dropped vastly over the past few years – from 112 cases recorded in 2019 to 28 cases in 2020 indicating a drop of 75 percent[3]. It is, however, worth noting that due to reputational damage, a number of businesses or organisations do not report some of the breaches to the appropriate authorities for the fear of losing public trust in their operations or systems.

These fraudulent activities are often made possible as a result of limited or low digital literacy on the part of victims, and by extension, the general public. For organisations, it is often a result of lack of investment in cybersecurity systems, regular updates and/or lack of corporate consciousness/ culture of best cybersecurity practices.

Cybersecurity sensitization efforts

Despite the general dearth in digital know-how and cybersecurity

[2] Ghanaian Citizen Extradited in Connection with Prosecution of Africa-Based Cybercrime and Business Email Compromise Conspiracy, The United States Department of Justice, accessed May 18, 2022, https://www.justice.gov/opa/pr/ghanaian-citizen-extradited-connection-prosecution-africa-based-cybercrime-and-business-email

[3] The 2020 Banking Industry Fraud Report, Bank of Ghana, accessed May 18, 2022, https://www.bog.gov.gh/wp-content/uploads/2021/08/THE-2020-BANKING-INDUSTRY-FRAUD-REPORT.pdf

consciousness among the general public, not much is being done in the country to improve digital literacy so as to empower the public on how to navigate cyberspaces safely and securely. The media have not helped much in this direction as many journalists themselves lack the know-how.

The government, through the Ministry of Communications and the Cyber Security Authority (CSA), has instituted the Cybersecurity Awareness Month (October each year) to create more awareness about cybersecurity issues. Although this is a laudable step by government, only few people benefit from it. Civil society organisations like the Media Foundation for West Africa (MFWA) also complement governments sensitisation efforts through forums and training workshops. But there is still a lot to be done to reach the masses.

Ghana's Cybersecurity Act 2020 and global cyber norms

As part of measures to address cybersecurity challenges in the country, the Parliament of Ghana passed the Cybersecurity Act 2020 (Act 1038) which was assented to in December 2020. The Act was passed to help in cybersecurity development and to respond to cybersecurity issues. Fortunately, the implementing authority, the Cyber Security Authority (CSA) has also been set up to implement Act 1038 and regulate the cybersecurity ecosystem in the country.

Ghana's Cybersecurity Act strongly aligns with the global cyber norms as almost all the norms are reflected in the various sections of the Act. For instance, the Act is very strong on Norm 5 of the global cyber norms as it has a number of provisions that protect human rights and privacy. The Act also makes provisions for securing critical information infrastructure and that is consistent with global cyber Norms 6, 7 and 8.

Further, the establishment of computer emergency response teams, sectoral emergency response teams and reporting cybersecurity incidents nationally and internationally are also consistent with Norms 1, 2, 3,4, 10 and 11 respectively. So implicitly, the implementation of Ghana's Act 1038 also means the implementation and furtherance of the global cyber norms.

The Act is in full force now, though the implementation and sensitisation about it have been relatively slow and low. A pre-event survey that was conducted by the MFWA ahead of a recent forum on the Implementation of Ghana's Cybersecurity Act, for instance, showed that a number of civil society organisations (CSOs) and journalists know very little about the content of the Act. The forum also highlighted the need for greater awareness creation, collaboration with CSOs, the media and other stakeholders to deepen awareness and contribute to the successful implementation of the act and overall improvement in cybersecurity in the country and across the world.

To improve the security of Ghana's cyberspace, a collective and collaborative effort from all stakeholders is required. In consideration of the above cybersecurity landscape in Ghana, the following policy recommendations are made to help improve the safety and security of Ghana's cyberspace.

Policy recommendations on implementation of Ghana's Cybersecurity Act

- To get all stakeholders on board to, first appreciate the tenets of Act 1038, and then support in the implementation process, government, through the CSA, should have more direct engagements with stakeholders to get their cooperation.

- The CSA, should develop an action plan/ a roadmap for the implementation process through a multistakeholder approach. This will guide stakeholders, especially CSOs, in incorporating specific activities into their programmes and also supporting collaborative efforts that will facilitate the implementation process.

- The CSA should also proactively disclose information on the implementation process.

- Whereas the Act has been described as human-rights-respecting (as it strongly aligns with Norm 5 of the global cyber norms), the CSA should ensure that its implementation is equally human-rights-respecting in line with these resolutions: "States, in ensuring the secure use of ICTs, should respect Human Rights Council resolutions 20/8 and 26/13 on the promotion, protection and enjoyment of human rights on the Internet, as well as General Assembly resolutions 68/167 and 69/166 on the right to privacy in the digital age, to guarantee full respect for human rights, including the right to freedom of expression."

Policy recommendations on sensitisation and improving the cybersecurity landscape

Getting people to be cybersecurity-conscious requires them to be empowered with the right information. Education and awareness creation on the trends within the cybersecurity environment must be intensified, timely and all year round. Most cybercrimes recur due to a lack of information on how it occurs and the way to prevent them. It is, therefore, recommended that:

- The CSA should organise training workshops for the media, civil society organisations, businesses, market women, artisans, and other groups on cybersecurity issues generally, and the provisions in Act 1038 that they can resort to in cases of cybersecurity breaches.

- The Act should be translated into local languages, and have brail formats, sign language formats and audio versions for the sensitisation process. A bottom-up approach to educating and sensitising the public will address the digital literacy issues and go on to improve the state of cybersecurity within the country.

- The CSA should produce abridged versions of Act 1038 factoring in the different audiences (age group, digital literacy level or digital challenge level etc) and the technological maturity of the audiences so the Act can be easily understood and relatable to that each segment of the audience.

- The media's role in educating and informing the citizenry is ever so crucial in this technological era. Unfortunately, the media's knowledge and engagement on cybersecurity issues and the Cybersecurity Act is low. The media must, therefore, make a conscious effort to engage with and understand the law. Then they must create platforms or programmes on their networks, websites and newspapers to educate the public on cybersecurity and related issues. This will help in building the capacity of the general public and empower them to identify and report cybersecurity issues while ensuring that they themselves are not culprits.

- The CSA should, also, liaise with the media and CSOs to drive sensitisation efforts. Government should make financial commitments towards awareness creation of the Act so the public can be well informed. Also, government should collaborate with the media to widely publicise activities of the Cybersecurity Month so it can benefit the masses.

- CSOs and academia should do more research into the cybersecurity sector so they can provide timely scientific information to inform policy and advocacy interventions.

- Institutions should invest in routine training of their staff on trending cybersecurity issues and Act 1038 to help improve the security and integrity of the organisation's systems. Almost all cyberattacks require a loose link within an organisation for them to succeed. The periodic training will bring staff up to date on current threats and preventive measures needed to stay safe.

- Telecommunication companies must invest more in the sector in terms of infrastructure to ensure the integrity of their systems is robust to protect subscribers' data from being accessed illegally.
- Businesses across all sectors must come together periodically to discuss peculiar cyber threats within their respective sectors and provide the funds needed to build robust systems to address the threats. They should also ensure that all cyberattacks suffered by their businesses are reported to the CSA so appropriate measures can be taken for the collective good of all.

MFWA
Media Foundation for West Africa

Media Foundation for West Africa
32 Otele Avenue, East Legon,
Telephone: +233 (0) 302 555 327
Twitter: @TheMFWA
Facebook: Media Foundation for West Africa
info@mfwa.org
www.mfwa.org

@themfwa

www.mfwa.org

themfwa