# Introduction

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."

The digital rights ecosystem in Ghana has evolved over the last five years. There have been major investments in infrastructural development by both the government and private sector aimed at improving the lives of people. This infrastructural development has led to an increase in online transactions, e-commerce and financial transactions.

The outlay in infrastructure has been backed by impressive efforts to provide a progressive policy environment for cyber activities in Ghana. Among these efforts is the development of the National Cybersecurity Policy, National Cybersecurity Strategy and the passage of the Data Protection Act 2012 (Act 843).

Apart from these, other measures have been adopted such as the setting up of the National Cyber Security Centre (together with the appointment of the National Cyber Security Advisor), the Ghana Computer Emergency Response Team and the Data Protection Commission. Ghana is thus asserting itself as one of the countries leading cyber development on the African continent.

The National Cyber Security Advisor has acknowledged that the country is very much aware of the growing digital space and some of the potential risks that come with it; and indicated that government, through the Ministry of Communications, is working assiduously to build a robust cybersecurity ecosystem. This system, when complete, will protect Internet-connected systems such as hardware, software and data from cyber-threats; thereby

guarding against unauthorised access to data centres and other computerised systems which harbour sensitive private and national information. The government has also taken an initiative to digitalise systems in Ghana. This has included the national ID system, paperless port, mobile money interoperability etc.

Globally, Ghana is part of the Freedom Online Coalition and in 2019, the country served as the Chair of the Coalition. On June 15, 2020 it was announced that Ghana has been appointed as a member of the Independent Advisory Committee (IAC) of the Global Internet Forum to Counter Terrorism (GIFTC).

Ghana is also part of the Open-Ended Working Group of the United Nations First Committee. In the first substantive session of the Open-Ended Working Group in September 2019, Ghana underscored the need for the rules, norms and principles developed to be rights-respecting. It also said such principles and norms should respect sovereign ties and hold cyber offenders responsible for malicious cyber activity. The State highlighted that rules, norms and principles should be consistent with existing international law and treaties. It also acknowledged that establishing these rules, norms and principles at the domestic level is essential.

Generally, challenges related to cybersecurity persist in Ghana. Issues such as cybercrime, and the limited capacity of state security and justice officials who are mandated to fight cybercrime remain a challenge. This limited capacity, apart from inhibiting justice delivery in fighting the crime, also impedes the promotion of human rights of citizens. There is also low level of cybersecurity awareness and consciousness among many people in the country.

This policy brief, therefore, is aimed at illustrating the links between the United Nations Group of Governmental Experts (GGE) global cyber

norms and human rights and Ghana's national cybersecurity efforts with the view to supporting Ghana to implement the norms in a human-rights respecting manner.

## Current Context

Ghana recorded its first COVID-19 case on March 13, 2020. A few days after the official announcement of the first case of COVID-19 in Ghana, the government announced a COVID-19 emergency call centre. The Ministry of Information later reported that they were facing challenges with prank calls. In response to this and also the potential of cyber-attacks such as jamming of emergency call lines with fake calls and thus preventing genuine patients from receiving emergency, the Ministry of Communication (MoC) launched a COVID-19 Tracker App to facilitate emergency calls and also contact tracing of COVID-19 cases. Many people have however raised data protection and privacy concerns regarding how the app works and how contact tracing is conducted.

Further in response to obvious challenges of the impact of the coronavirus situation, the government announced the following as a relief measure:

- An insurance package, with an assured sum of GHC 350,000 (about US$ 60,000) for each health personnel and allied professionals at the forefront of the fight.
- Frontline health workers received an additional allowance of fifty percent (50%) of their basic salary per month from March to June 2020.
- The absorption of water bills of all Ghanaians from April to June, 2020.
- Partial or full absorption of electricity bills for all Ghanaians from April to May, 2020

Whereas generally there have been no issues with the insurance package and other benefits for health care professionals, there have been serious challenges with electricity and water. The added benefit of all Ghanaians enjoying free water and subsidised electricity costs came with its own challenges. For example, to meet demands which had gone up because more people were home and using electricity and water, the service providers started rationing these services. For many days, households who hitherto had water could not have access to water which is critical utility in the fight against the virus. This severely impacted how people were able to wash their hands and maintain personal hygiene, a cardinal preventive measure.

With the surge in cases and its accompanying lockdown, internet use in Ghana has increased considerably. People have been urged to use the internet and telecommunication services responsibly during the COVID-19 crisis. The government has called on telecommunications and internet service providers to ensure optimum service delivery. The government has also cautioned against the "misuse of the digital space."

As experienced in many places in the world, COVID-19 has put enormous pressure on internet services and in Ghana, the situation is not different. As companies and organisations work remotely, conferences go online and students take their courses online, there has been heavy reliance on the internet. On April 20, 2020, the government announced that the National Communication Authority (NCA) had given some spectrum to telecommunication companies in the country so they can provide better internet services during the period. The impact of this increase in spectrum is however yet to be felt.

However, a critical issue that was not addressed was the cost of internet. The average cost of internet is not affordable to the average Ghanaian. As many schools continue to offer lessons online, many students have been left out. Many parents cannot afford to provide computers or laptops and other gadgets and data for their children. This has meant that many students are

in effect, missing out on school lessons. Already, there are many underserved communities in Ghana where internet connection is a challenge. Another challenge is even the use of ICTs in these communities. This has the potential of entrenching further the inequalities that exist offline. There is therefore an urgent need to look at a policy of improving infrastructure, reducing data costs and putting measures in place to ensure meaningful connectivity even for those that have access.

## Recommendations

The Freedom Online Coalition urges states to "develop and implement cybersecurity-related laws, policies and practices in a manner consistent with international human rights law and seek to minimise potential negative impacts on vulnerable groups and civil society, including human rights defenders and journalists." It notes that this intervention should include building, where appropriate, supporting processes and frameworks for transparency, accountability, judicial or other forms of independent and effective oversight, and redress towards building trust. These measures should embed the principles of legitimacy, legality, necessity or proportionality into policy and practice. In this regard, any COVID-19 restrictions by Ghana on the right to privacy should be guided by the legal tests of legality, necessity and proportionality.

### COVID-19 and Future Pandemics

- Government must step up efforts in ensuring effective individual information protection in this era of the coronavirus pandemic, update existing frameworks and work towards harmonising them across all relevant sectors/ digital critical infrastructures.
- Any legislation or policy that is aimed at restricting freedom of expression online generally or during a pandemic such as COVID-19 must meet the human rights principles of legality, necessity and proportionality.

- Any surveillance measure, including contact tracing in response to the COVID-19 pandemic currently being undertaken by the government through the Ministry of Health or the Ghana Health Service, should be prescribed by law, and subject to appropriate safeguards and oversight.
- While dealing with COVID-19 contract tracing efforts and "routine surveillance," it is important that the government and other stakeholders be mindful of the recommendation of the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, to put a moratorium on surveillance technology.
- The state and other relevant stakeholders should strictly implement the principles for the lawful processing of personal information set out in Ghana's data protection laws or regional standards, including the relevant time periods, the way in which the data will be handled, and the conditions of access, storage and security of the information.
- It is important for the government to continue to take measures that make the internet open, accessible and secure.
- To address the urgent issue of high data costs, taxes that have a bearing on internet use, eg the communication tax should be reduced. The continued existence and implementation of this tax and its margins considerably increases the cost of connecting to the internet and contributes to further widening the digital divide and hampers meaningful connectivity.
- The government should continue collaborating with the private sector to improve internet infrastructure to upgrade internet speed and ensure increased access to underserved areas.
- The government should improve community networks to connect the unconnected.

# The GGE Norms

In 2018, the United Nations (UN) First Committee which is one of the six main committees of the UN General Assembly where states address global challenges, threats to peace that affect the international community and seek ways to promote international security and disarmament, set up two mechanisms to discuss responsible state behaviour in cyberspace: The Group of Governmental Experts (GGE) and the Open Ended Working Group (OEWG). Ghana is currently part of the OEWG. In 2015, the country was part of the GGE.

The most significant work done so far by the GGE is the 2015 resolution on the 11 global cyber norms. Cyber norms are socially enforced rules or expectations (norms) that apply to the cyberspace. Cyber norms do not have a precise definition, however, they refer to how actors should or should not behave with regard to their use of information and communication technologies (ICTs).[1]

In 2015, the GGE agreed on 11 voluntary, non-binding norms for responsible state behaviour aimed at promoting an open, secure, stable, accessible and peaceful ICT environment.

The GGE global cyber norms can have an important influence on what states do at the national and regional level, and – to be implemented – may even require regulatory instruments and model laws at the national level. At the same time, these processes could be an opportunity to ensure positive developments happening at these levels– like the emphasis on coordination among states and among different stakeholders which are now included in

[1] UN First Committee Processes On Responsible State Behaviour In Cyberspace: An Explainer, Global Partners Digital, https://www.gp-digital.org/un-first-committee-processes-on-responsible-state-behaviour-in-cyberspace-a-briefing/

many national and regional cybersecurity strategies – are also reflected at the global level.[2]

Norm E of the GGE global cyber norms indicates that "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,"[3]

What this means is that human rights are to be guaranteed online as well. The cyber space should also offer the same safeguards to human rights as they exist offline. Rights to freedom of expression, access to information, right to privacy, freedom of association, right to education etc, should all be respected, promoted and fulfilled.

It is, therefore, important that Ghana continues to ensure the respect, protection and the enjoyment of human rights on the internet.

Current challenges in the world reinforce the need for the norms that pertain to critical infrastructure; Norms F, G and H.

Norm F states that "a state should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation

[2] UN First Committee Processes On Responsible State Behaviour In Cyberspace: An Explainer, Global Partners Digital, https://www.gp-digital.org/un-first-committee-processes-on-responsible-state-behaviour-in-cyberspace-a-briefing/

[3] Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, https://undocs.org/A/70/174

of critical infrastructure to provide services to the public." Norm G also indicates that "states should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account (the UN) General Assembly resolution 58/199 on the creation of a global culture of cybersecurity and the protection of critical information infrastructures, and other relevant resolutions."

The last Norm that is related to critical infrastructure (H) also recommends that "states should respond to appropriate requests for assistance by another state whose critical infrastructure is subject to malicious ICT acts. States should also respond to appropriate requests to mitigate malicious ICT activity aimed at another State's critical infrastructure emanating from their territory, taking into account due regard for sovereignty.

When there is any attack or damage to a state's critical infrastructure, that attack can violate a number of human rights, including the rights to life, health, and security. It can also undermine critical national processes such as elections. If, by contrast, states work to ensure the security of their critical infrastructure, they can safeguard these rights.

As Ghana goes to the polls on December 7, 2020, it is important that the systems of the Electoral Commission and state security agencies are guarded, as these could potentially be targeted by individuals. Having registered over 16.5 million people this year during the voter registration exercise, in which biometric data was collected, the EC has enormous information about half of Ghana's population. This information, should it get into wrong hands, could be very problematic.

Any tampering with the EC's database, website, backup systems etc, could lead to serious challenges which would lead to disputed elections and possibly a national crisis if it is not managed well. It could potentially lead

to these cyber criminals also accessing bank accounts since many people use their voter identification cards to open bank accounts.

It is, therefore, important that the systems of the EC are strongly protected against any possible attack by cyber criminals or other groups of people who may seek to interfere with election procedures.

As the demand and use of the internet increased during the COVID-19 pandemic, the risks of exposure of the country's digital infrastructure and information systems has also increased.

In response to a cyber-attack in Ghana in March, and obviously being guided by norms on critical infrastructure, the government announced on June 8, 2020 that the Ministry of Communications, through the National Cyber Security Centre, has expedited work on the remodeled Cyber Security Bill, which cabinet is expected to deliberate on. This Bill is expected to be passed into Law by the end of the year. When passed, the Law will ensure that all institutions and businesses put in place mechanisms to secure their digital system from potential cyber-attacks, as well as train and employ qualified personnel to manage cybersecurity. Businesses will also be required to draft policies and embark on routine audits of their IT infrastructure.

Further, the authorities will investigate institutions with critical national information that can meaningfully impact the economy – such as banks, telecommunication companies and public sector institutions – and impose fines on those found to have failed to meet the guidelines.

Also, the Law will among other things lead to the establishment of a Cyber Security Authority which will be the institution mandated to protect critical national information infrastructure. "The regulatory body will ensure standardisation and accreditation of cybersecurity services, with

cybersecurity service providers set to be licensed before they get access to any national data. The Law will also facilitate international cooperation in the fight against cybercrime – i.e. the Malabo and Budapest Conventions which need to be operationalised by the country to meet its international commitments.

Though this Bill is being prepared to be submitted to Parliament, non-governmental stakeholders are yet to be engaged on this process. It is important for the government to demonstrate its commitment to multi-stakeholderism and human rights by engaging civil society, academia and the private sector in the drafting of this Bill and in its eventual implementation.

## Recommendations

Promoting human rights at the national level would require maximum efforts from the government and other stakeholders. As mentioned earlier, COVID-19 has underscored the need for greater collaboration between government and non-governmental stakeholders such as civil society, academia and the private sector. In the development and implementation of cyber- related legislations and policies, 'meaningful stakeholder engagement', which requires timely information sharing, transparency, accountability and engagement of stakeholders throughout the development and implementation processes is crucial. There should be greater transparency, accountability and inclusivity in cyber policy development and implementation in Ghana.

The importance of non-governmental stakeholders in the development and implementation of human rights-based cyber policies cannot be over-emphasised. Many studies have shown that when it comes to cybersecurity capacity building measures especially, civil society has proven to be a formidable partner. An important component of capacity building is

ensuring that state institutions that have the mandate to promote, protect and fulfill human rights are adequately resourced and strengthened. Ghana has on many occasions indicated its commitment in reflecting the global cyber norms in its national cyber efforts. It is crucial that non-governmental stakeholders are involved in the implementation of the global cyber norms in Ghana.

Civil society and human rights defenders also play a role in implementing Norm E, by documenting state practices at the national level, conducting research and litigation, and using mechanisms at the regional level such as the African Commission on Human and Peoples' Rights and at the global level, such as the UN Human Rights Council, the Special Procedure system, the Treaty Body System, the Universal Periodic Review and the Office of the High Commissioner for Human Rights, to highlight both good practices and violations of human rights. The research and advocacy work conducted by civil society in this regard is crucial in providing the evidence base that promotes compliance with the human rights commitments referred to in Norm E.[4]

To effectively implement the global cyber norms:

- Measures should be put in place to ensure that state security, the legislature and the judiciary are adequately trained on the cyber norms and principles of cybersecurity and internet rights and their role in protecting human rights and international peace and security.

[4] Efforts to Implement Norms of Responsible State Behaviour in Cyberspace, as Agreed in UN Group of Government Expert Reports of 2010, 2013 and 2015, https://www.un.org/disarmament/wp-content/uploads/2019/12/efforts-implement-norms-uk-stakeholders-12419.pdf

Civil society has already been undertaking this activity and the state is encouraged to partner with civil society to achieve this aim.

- An enabling environment should be created and nurtured to support human rights defenders to help shape policies, build the capacity of both governmental and non-governmental stakeholders to implement frameworks in a rights-respecting manner, providing technical and policy solutions to existing challenges, and raising awareness of existing initiatives and commitments.
- Strengthen the data/cyber security systems of institutions such as the Electoral Commission, Ghana Police Service, Parliament etc to protect their systems from potential attacks.
- Take measures to improve data security systems of other critical institutions such as financial institutions (particularly banks), telecommunication companies, hospitals, as well as the Ghana Water Company and the Electricity Company of Ghana.

## Cybercrime

Ghana is a signatory of the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention) and the Convention on Cybercrime (Budapest Convention) becoming the 5th country on the continent to ratify the Treaty.

These protocols guide the formulation of country specific cybersecurity frameworks and data protection policy.

The Convention on Cybercrime of the Council of Europe (CETS No.185), known as the Budapest Convention was adopted in November 2001, by the Committee of Ministers of the Council of Europe. On November 23, 2001, it was opened for signature and entered into force on July 1, 2004. It is the only binding international instrument on the issue of cybercrime and serves

as a guideline for any country developing comprehensive national legislation against Cybercrime and as a framework for international cooperation between State Parties to this treaty.

In 2014, the African Union member states adopted the African Union Convention on Cyber Security and Personal Data Protection, also known as the Malabo convention. The convention encourages AU member states to recognise the need to protect critical cyber/ICT infrastructure, personal data and to encourage free flow of information with the aim of developing a credible digital space in Africa.

Cybercrime is a serious problem in Ghana.

In March 2020, there was a major hacking of ATMs of some banks in Ghana. The hackers reportedly also hacked some telecommunication companies, while the cost of these attacks is not clear, it was one incident too many that raised a lot of concern.

According to the Cybercrime Unit of the Criminal Investigations Department of the Ghana Police Service, Ghana lost approximately US$97million to cybercrime in the first seven month of 2018. This figure was an increase from US$69million lost in 2017 and US$26million in 2016. The actual figure of these loses may be high as the figures are only based on reported cases. There have been also been cross border cyber-attacks on banks in West Africa leading to loss of huge sums. This is an indication of how serious the problem is. These cases include forgery, cyber fraud, remittance fraud, sextortion and romance fraud among others.

Cybercrime attacks are sometimes not reported due to fear of regulatory sanctions, potential customer panic (especially for banks) as well as loss of investor confidence.

Attacks on banks is a serious economic issue. Economic issues are a human rights issue as people's livelihoods are affected. Beyond the increase in phishing attacks targeting online bankers, there is also an increase in number of mobile money fraud cases.

Mobile Money was introduced into the Ghanaian market in 2009. It is estimated that about GHS79 billion worth of mobile money transactions took place in 2016. This grew to nearly GHS156 billion in 2017, representing a staggering 97% growth.

The latest data from Bank of Ghana's payment system shows that the registered number of mobile money accounts increased to 29.9 million in June 2018 from the 21.3 million recorded in June 2017. While there were no official records at the end of September 2020, projecting a further increase based on yearly trends will not be far-fetched. The total registered mobile money accounts across the three major telecommunication companies in 2020 is reported to have outstripped the Ghana's total population.

With the increase in online and other digital payment platforms such as mobile money, has also emerged mobile money fraud. According to the Cybercrime Unit of the Criminal Investigations Department, mobile money fraud cases have increased exponentially with hundreds of victims.

These fraudulent activities have ranged from the duping of unsuspecting users with promotion scams to impersonation of officials of the telecommunication companies, which make users disclose their pins to these fraudsters, who then get access to their accounts. Mobile money users who link their bank accounts to their mobile money accounts have also become the biggest targets of these cyber criminals. There is a need to urgently address this issue.

## Recommendations

To reduce the increasing cases of cyber-attacks and fraud, the government must strictly enforce and monitor compliance of the Ghana Electronic Transactions Act to ensure safer and more secure online transactions.

- Intensify cybercrime and cybersecurity awareness measures.
- Digital literacy training interventions should be increased to educate people on using digital payment platforms.
- Improve the data/cyber security systems of state institutions such as the Electoral Commission, Ghana Police Service, Parliament.
- Take measures to improve data security systems of other critical institutions such as banks and other financial institutions, telecommunication companies, hospitals, as well as the Ghana Water Company and the Electricity Company of Ghana.
- Collaborate with other states to put in place measures to investigate cross-border cyber-attacks and prosecute culprits to reduce incidents of cross-border cybercrime.

## Conclusions and Summary of Recommendations

The GGE Norms are important to increase the state's responsibility in protecting human rights of Ghana and also promoting international peace and security in the cyber space. In view of this, we recommend to government to:

- Take measures that make the internet open, accessible and secure.
- Improve the data/cyber security systems of state institutions such as the Electoral Commission, Ghana Police Service, Parliament.
- Take measures to improve data security systems of other critical institutions such as banks and other financial institutions, telecommunication companies, hospitals, as well as the Ghana Water Company and the Electricity Company of Ghana.
- Continue to collaborate with non-governmental stakeholders such as civil society, private sector, academia etc in implementing the 11 GGE Norms in Ghana.
- Ensure that any legislation or policy that is aimed at restricting freedom of expression online generally or in a pandemic such as COVID-19 or to fight crime meets the human rights principles of legality, necessity and proportionality.
- Ensure that surveillance measure, including contact tracing in response to the COVID-19 pandemic are prescribed by law, and subject to appropriate safeguards and oversight.
- Work with other relevant stakeholders to ensure strict implementation of the principles for the lawful processing of personal information as set out in domestic data protection laws or regional standards.
- Reduce or waive taxes that have a bearing on online use, eg the communication tax as a way of increasing internet access and meaningful connectivity in Ghana.

- Collaborate with the private sector collaboration to improve internet infrastructure to upgrade internet speed and ensure increased access to underserved areas.
- Strictly enforce and monitor compliance of the Ghana Electronic Transactions Act to Reduce the increasing cases of fraud and ensure safer and more secure online transactions.
- Increase or improve measures aimed at increasing Cybercrime and cybersecurity awareness.
- Collaborate with other states to put in place measures to investigate cross-border cyber-attacks and prosecute culprits to reduce incidents of cross-border cybercrime.


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


@TheMFWA


www.mfwa.org