

Esther N. Appiah, Moses Ayiku, Osei B. Dickson, Esq. and Dr. Ebenezer Appiah-Denkyira

## CYBER SECURITY MANAGEMENT IN GHANA

### A. Introduction

In this Briefing Paper we focus on cyber security. Indeed under the Security Governance Initiative (SGI) executed on February 18, 2016 between the United States Government and Government of Ghana, cyber security was one of the key focal areas under the Joint Country Action Plan (JCAP).

In a brief, cyber-security has been interpreted as consisting of the technologies, processes and practices designed to protect networks, computers and data from attack, damage or unauthorised access. It is estimated that, Ghana loses about \$50 million to cyber-attacks annually, which brings into sharp focus a number of national security issues. Some of these security issues include the following:

- Inadequate technical know-how
- Recurrence of cyber-attacks and hacking especially on the financial industry
- Improper and inadequate network security
- Inadequate expertise in email security and cyber threats

### B. Key Agencies

In the area of cyber-security we identify the following as some of the key government agencies around whom issues of cyber security will develop over the next 5 years:

- Ministry of Communication
- Ministry of Foreign Affairs and Regional Integration
- Ministry of Justice and the Attorney General's Department
- Ministry of Finance and Economic Development
- The National Communications Authority (NCA)
- National Security Council Secretariat (NSCS)
- National Cyber Security Secretariat

- Computer Emergency Response Team, Ghana (CERT-GH)
- Bureau of National Investigations (BNI)

#### C. Laws and Policies on Cyber Security

We identify a number of existing laws and policies which attempt to govern the cyber space as follows:

- The National Communications Authority Act, 2008 (Act 769)
- The Electronic Transactions Act, 2008 (Act 772)
- Data Protection Act, 2012 (Act 843)
- The National Cyber Security Policy and Strategy, which seeks to protect Ghana from attacks on its cyberspace.
- The Information Communications and Technology for Accelerated Development (ICT4AD)

#### D. Strategies for Mitigating Cyber Security Threats in Ghana

As a result of the globalized nature of the security threats implicated in cyber security, in particular the influx of “hackers” around the world, Ghana needs to secure its cyber space. This will ensure that Ghana and its institutions are free from cyber-attacks with its devastating effects. Some of the strategies that should be put in place, must involve among others:

- Effective Governance - GoG should focus on ensuring that it has a strong focal agency and governance structures to ensure long-term sustenance of activities
- Effective Legislative and Regulatory Framework - This can be achieved through the setting up of cyber law review committees to do regular studies on current law of Ghana relating to cyber security.
- Ensuring that Ghana has the right Cyber Security Technical Framework
- Ensuring Cyber Security and Capacity Building
- Enhancing of National Cyber Security Emergency Readiness
- Enhancing Compliance and Enforcement. This could be done by the development of a uniform risk assessment framework for Ghana; as well as through
- International Co-operation

#### E. Conclusion

Again we hope you found this issue helpful. The Center aims to empower readers to understand and navigate a continuously changing and complex global security environment

**Esther Nyantekyiwaa Appiah**  
Co-Executive Director