*International Journal of Precious Engineering Research and Applications (IJPERA)*
*www.ijpera.com ISSN: 2456-2734,*
*Volume 4, Issue 2 (Mar-Apr) 2019), PP. 20-28*

# Cyber Security and Its Challenges posed by Latest Technologies in Post-Ebola Sierra Leone

Ibrahim Abdulai Sawaneh
*Lecturer at the Department of Computer Science, Ernest Bail Koroma University of Sciences and Technology, Magburaka - Sierra Leone*
*Corresponding Author Email: ciddiisawaneh@hotmail.com*

**ABSTRACT**: The Cyberspace is a hostile environment where individual or entity and / or nation performs cybercrime or carryout espionage activities either to achieve competitive advantage or for financial gain. Most nations around the world including; Ghana, Kenya, Rwanda, South Africa, Botswana, Tanzania, Nigeria, and the West over the years have implemented strong policies and legislations to combat cyber related crimes. Sierra Leone as a developing nation needs to move along with other nations providing safer and secure cyberspace that will attract potential investors into the country. Furthermore, if strong cyber related laws are legislated, it will help boost the economy and alleviate poverty, and also improve on the lives of the average Sierra Leoneans. The government should embark on massive sensitization on the safer use of the internet, and how to protect sensitive government and personal information from cyber criminals.

**KEYWORDS:** Sierra Leone National Telecommunications (NATCOM), Office of the National Security (ONS), Cybercrimes, Cybercrimes.

## I. INTRODUCTION

It is evident that cyber-attacks are on the increase in the global cyberspace, either by an individual or state sponsorship. It main goal is for either financial gain or to gain competitive edge over an individual, company, business or state. Others deployed it for espionage purpose. Such as the current trade war between China and the U.S, where the U.S accused China of stealing trade secrets, technological intellectual property rights and Chinese government using Huawei to spy on the U.S and its allies. The accusation which China has repeatedly denied, as the U.S failed to provide tangible evidence.

Locally, some Chinese and Ghanaian fraudsters based in Sierra Leone recently engaged in massive smartphone cyber-attacks, where they used Sierra Leonean mobile numbers to target their victims, calling the victim's once and end the call, if the victim calls back, them the call will be billed in thousands of U.S dollar. They targeted people all over the globe, particularly in Sierra Leone and the U.S. Unfortunately, they were arrested by the Sierra Leone Police Force of the cybercrime unit attached to the Criminal Investigation Department. The cybercriminals are on trial though they claimed that their company is legally licensed and have the mandate to operate in Sierra Leone.

The Sierra Leone National Telecommunications (NATCOM) Office have instructed all GSM operators in the country to register all SIM card users from May to early June 2019. This will help cyber security experts to easily identify cybercriminal operating within the country. Therefore, all the security agencies or departments including NATCOM, ONS, Ministry of Information and Telecommunications, GSM operators, the cyber unit of the Sierra Leone Police Force, and the Military together with the central government are trying to legislate cyber laws that will potentially punish cybercriminals in the near future. Also, massive sensitization and awareness

campaign should be organized in order to acquit the general population on the dangers of failing to protect one's personal data, as most internet users in the country lack the basic skills to protect their data online. The Ministry of Higher and Technical Education and the Tertiary Education Commission (TEC), should design a curriculum in Cyber Security Studies to be taught at certificate, diploma, higher diploma levels in colleges, and bachelor's level in universities. This will subsequently create awareness on cybercrime and cyber security issues in the country.

## II. MOTIVATION

The internet is the fastest growing entity ever in the history of mankind that has engulfed our daily activities and that which we cannot go without. We heavily depend on it ranging from defence, online transactions, banking and finance, healthcare, automation industries, smart cities, aviation, critical infrastructure, civil engineering, telecommunications, news channels, and host of others entities.

Furthermore, protecting the massive data used in our day-to-day activities become difficult as cybercrimes are on the increase. Cybercriminals today viewed invading personal and state data as a lucrative business with the emerging technological innovations such as bitcoins. This is made possible as sophisticated software are used that hide their onlineidentities making them hard to track. Protecting internet user is vital, as most of the internet users in Sierra Leone lack the basic techniques and skills on how to protect themselves against cybercriminals while using the internet.

Therefore, NATCOM, ONS, the Ministry of Higher and Technical Education, and the state security apparatus should draft solid and sound cyber security policies and laws that can potentially punish any cybercriminals operating in Sierra Leone. The drafted cyber policies should be sent to the Sierra Leone Parliament to be enacted into laws, as of now, there is no such laws and policies in existence in Sierra Leone. Noting that the fight against online criminals require a broader scheme. Given that technical measures alone cannot thwart any crime, it is essential that the state security departments are fully mandated by the state constitution to investigate and prosecute cybercriminals without any corrupt practices. Nowadays, most third world nations are legislating strong cyber laws in order to avert the damages associated with cyber-attacks. The ministry of basic education should also incorporate cyber studies in the junior and secondary schools to create more awareness on the danger related to cybercrime and cyber security in Sierra Leone.

## III. RELATED LITERATURE

Today world is engulfed with series of cybercrime related activities that pose great security threats and challenges in Post-Ebola Sierra Leone [1]. The research basically looks at key security challenges, as seen in the last two decades. Traditionally, national security issue was in the hands of the military focusing only on warfare from 1991 to 2002 when Sierra Leone experienced a bloody civil war. Buzan and Hansen [2] emphasized on security rather than defense or war, or war as its key concept, a conceptual shift leading to a broader perceptive of political issues, including the importance of societal cohesion and the relationship between military and non-military threats and vulnerabilities" National security is a key feature in protecting territorial integrity of any nation. This means that security matter is state-centric. The world have experienced numerous cyber-attacks in the last two decades, the Ransomware attacks known as Wanna-cry and Disk Coder. C in 2017 led to major financial blow to most government agencies and multinational companies around the world. Millions of internet

users had their personal data compromised in an unprecedented manner, causing series of confrontation among nations and organizations. These attacks raised critical security matters, and further exposed loopholes in the existing security infrastructures. For instance, the Equifax breach that affected most U.S adult population and elsewhere. The HBO attacks compromising actor's roles in scripting and episodes of the game of Thrones Series. The attack on Yahoo user's database revealing personal recordsincluding names, date of birth, email addresses, passwords, and in some scenario, security questions and answers were also compromised. The un-going investigation into the 2016 U.S Elections, as to whether external factor influenced the election results. A threat linking to the WPA2 encryption system, KRACK was discovered, which may compromise the security of Wi-Fi connections.

The innovative advances in modern technological frameworks have made the possibility of cybercrime visible, with several tutorials and software available on the internet that can aid or perhaps the online hate speech that helps to recruit more cyber criminals. Most of these attacks exhibit non-profit motive.

## IV. GENERAL ANALYSIS

The world today is in great danger as we are gradually again moving towards the Cold War era of the 1980s and 1990s. The 9/11 attacks in U.S, the U.S elections melding in 2016, the Ransomware attacks in 2017, the U.S trade war against other countries (China, Mexico, Canada, Australia, Japan, EU ……), the North Korean Denuclearization, the state sponsored killing of Jamal Khashoggi by Saudi Arabia security apparatus in their Istanbul Consulate in Turkey on the 2nd of October, 2018, the tension in the South China Sea, the annexation of the Ukraine Crimea region by Russia and the Sierra Leone Yenga issue with Guinea. For these kind of actions, Sierra Leone is faced with how it should secure its citizens and the country territorial integrity against internal and external cyber related activities. With weak ICT infrastructure, few cyber security experts, poor internet facility, and poor energy supply in the country made it impossible for policy makers to fully combat cybercrimes and cybercriminals.

Referencing the Cold War that ensured NATO provides maximum military power as a deterring force, and to assure a "balance of force" by establishing and maintaining stability and security [3], the EU crisis management operations under the "Berlin-Plus" arrangement [4] and assisting general ad-hoc security operations [5]. The security concept of NATO was further enhanced when The North Atlantic Council proclaimed that terrorism could affect the security interests of NATO members, and Article 5 was invoked after the 9/11 [3]. Article 5 states that attack against any member countries is an attack to all.

With the above narration, which is not applicable in this scenario, though the African Union has similar mechanism to protect individual member countries against cyber-attack. It is incumbent on individual countries in African to develop a counter measures to defend their cyberspace against cybercriminals. Cyber is viewed as a digital platform involving the creation of data, storage capacity, and shared in the cyberspace. It constitutes both virtual and physical space that permits the virtual data to flow [6]. More devices are interconnected and more cyber threats surfaced on a daily basis that is linked to computers and internet usage, technological innovations and essential security breaches have widening the concept of "cyber" to virtually anything connected to the digital and electronic platforms. Sierra Leone in the realms of technological advancement, find common ground to secure its cyberspace, as cyber security has gained prominence and relevance in societal developmental programmes, peace, security and economic development, implying that Sierra Leone must deal with its emerging cyber related security issues.

## V. CYBER SECURITY RISK

Cyber security risk assessment classifies the numerous information paradigms that could be targeted by a cyber-attack including; hardware, systems, laptops, customer data and intellectual property, and also locates the various security threats [7].

## VI. CYBER SECURITY RISK ASSESSMENT

Risk Assessment, a practicethat identify, analyze and evaluate risk. It helpscyber security expert to choose the right control measures that can prevent a possible cyber –attacks in an organization.

Without a risk assessment to alert cyber security choices, time, effort and resources will be wasted; i.e., aslight point to implement a security measures in order to protect against situations that are questionable to occur or won't have much substantialeffect on your organisations [7].Moreover, it is likely that one will underrate or overlook risks that could cause substantial damage to a particular organisations. This has resulted to numerous best-practices, standards and laws – such asGeneral Data Protection Regulation (GDPR) and Data Protection Act (DPA) of 2018are vital for cyber security protocol [7].

### Cyber Security Risk Assessment Components

A cyber security risk assessment examinesseveral information paradigms that could be targeted by cyber-attack including hardware, systems, laptops, customer data and intellectual property, and further examines several risks that would affect those paradigms. A risk assessment and estimation is generallyexecuted, followed by selectingthe appropriate control measures to treat the risks identified. Continuous supervision and monitoring is essential, as it enhances cyber security expert to review the risk environment by detecting changes in the context of the said organisations, and to upholda complete overview of the risk management process.

It is vitalfor organizations to record detail information relating to the information security risk assessment process,ensuring that they comply with the security risk requirements. Furthermore, the security experts must follow a number of security prevention methods, creatingpertinent documentation that will serve as part of the information security risk management process.

#### IT Governance Risk Assessment Services

Performing cyber security risk assessment is a difficultpractice that entailsextensive planning, specialist knowledge and stakeholder buy-in to suitablyinvolving people-, procedure and technological-based risks. Without proper security guideline, this will only be possible through a trial and error method. IT Governance offers a series of risk evaluation methods, and cyber security practices suitable to the needs identified.

#### Cyber Health Check

IT Governance's fixed-price, three-phase Cyber Health Check combines consultancy and audit, remote vulnerability examinations, and an online staff assessment to evaluate the cyber risk and detect a practical route to mitigate the risks. Their approach will identify the cyber risks, audit the effectiveness of the responses to those risks, analyse the real risk assessment and make a selectedschemes for addressing the risks identified in consonant with the business blueprint.

## VII. THREATS AND CHALLENGES

Generally refers to objects or people who pose potential threat to assets via attacks.

### Threat Agents

Refer to object, or person who poses great riskvia an attack. DDoS attacks are a threat. For example, if a hacker performs a DDoS attack, he is called a threat agent.

### Types of Threats agent

Threat agent varies according to the different motivations for performing malicious acts. The most remarkable are those engaged in the act for monetary reward, and some are inspired by political, ideological, religious, national security reasons. Their aim or motive hinged on what they want to achieve in an attack [8]as presented by Marinos, Belmonte and Rekleitis in their eight different threat agents.

### Cybercriminals

The cybercriminals utilize advanced methods, tools and software to profit from their illegal activities [9] [8]. Normally, the cybercriminals are well organized and have access to massive data resources, while being technically skilled and experienced. The motivation lies in monetization and "show-of-skill". This kind of highly organized crime is a large player in fraud and the collaboration enables the spread and depth of attacks. The methods and techniques evolve with the advancement in technology and business, such as e-finance, e-commerce, e-payment, and bitcoins. They often use ransomware that encrypts the victim's data, where the victim must pay to get his or her data back. Cybercriminals have created a business around the cybercrime as-a-service and can potentially be involved in espionage-as-a-service [9] [8]. The group also develop malicious tools to exploit their victims using the internet. The anonymization, encryption and virtual currencies, such as bitcoin, makes the cybercriminals difficult to identify and significantly delays or hinders the detection process.

### Insiders

Insiders are individuals or groups associated to a particular organizations or entities, and may include; employees, suppliers, contractors, consultants, business partners and customers [8]. These internal or external users have abused their system credentials or user rights. The motivation behind these acts are mainly monetization, revenge, or the convenience of bypassing the existing restrictive procedures. There is a potential risk that

other threat agent groups will try to recruit insiders for their agenda. The insider are usually end-users, customers, cashiers, and executives. It is less likely that a system admin abuses their system rights [8].

**Online Social Hackers**

This group plays vital role in the deployment of other cyber threats [9]. They are normally classified as highly skilled and talented hackers who analyse the behaviour and psychology of their victims. The main tool is analysis of information, profiling of users via loggers, social media accounts, or breached data. The importance and frequency of phishing has increased and enables further exploitation [8]. The group are large players in identity theft and in collection of confidential personal data and user credentials.

**Cyber Spies**

Cyber spies are on the increase that is extremely resourceful and have access to huge budgets, whether it comes from a nation or a corporation [9]. They developed into a more resourceful and talented group, as more advanced mechanisms and platforms of attack technics and the increased focus on cyber-physical systems [8]. Nations have developed their cyber intelligence capabilities and is motivated by gaining intelligence regarding state secrets, military secrets, healthcare systems, trade secrets, and critical infrastructure, as well as information on a corporate level. This enables nations to potentially gain psychological and political advantages. There are no clear international cyber espionage policies and judicial guidelines that limits these kinds of activities. Because of these lack of international policies, nations in the past and present have accused each other of spying as seeing in the latest trade war between China and the U.S. This prompted the U.S to banned Huawei, a Chinese tech giant which is the second largest smartphone producer in the world.

There is a growth in corporate financed espionage that targets other corporation's information [9]. Generally, the corporations are involved in reconnaissance activities, intrusion, and data breach. The motivation is to gain business intelligence, steal competitive information, and breach intellectual property rights, even cause sabotage or damage to competitors [9]. This group is also driven to buy services from other threat.

**Hacktivists**

This groups seeks media attention for high visibility in their actions [9]. The common methods are DDoS, leakage and publishing information. The group is motivated by political ideologies, social injustice, and aims to influence political decisions. These groups are dynamic in the sense that they does not necessarily have a centralized organizational culture. Sometimes they consist of other threat agents, joined by a common cause, but with different motives. They can form during political decision or crises, and when there is assumed injustice or unfairness towards specific social groups. They spawn during riots, international sports events, and other major events with international attention [9]. In 2015, hacktivists focused on alleged wrongdoings, promotion of freedom of expression, and an open internet [8]. For an instance, the Arab Spring that resulted to several anti-government demonstrations, and armed rebellions across the Arab countriesin late 2010. It started as a result of the oppressive governmentsthat inflicted low standard of living, starting with demonstrations and protests in Tunisia [10] [11].

**Cyber Fighters**

This group is identified as motivated citizens who possess significant striking power [9]. The group falls between cyber terrorists, hacktivist, and espionage. They are motivated by politics and will engage in sabotage if they feel their political, national, or religious values are threatened. The purpose of these attacks is to do harm, but also to attract media attention. Typically, these individuals are supporters of totalitarian regimes, and may act on their behalf [9]. This threat agent is growing and their attack methods are becoming more sophisticated. Example, the North Korea hacking group.

**Cyber Terrorists**

This group targets nations, society and critical infrastructure and engage in large-scale sabotage to inflict harm and promote violence [9]. Their objectives are motivated by influencing political decisions and actions based on their own politics or relations. Their main cyber related activities are communicating while avoiding state surveillance, recruiting new members internationally, and collect and distribute anonymous financial truncations [9] [8]. The growing threat in that this group is communication knowledge about malicious tools and attack methods. This group is a candidate to take advantage of the growing availability of cyber-crime-as-a-service.

**Script Kiddies**

The group is identified as teenagers who are fascinated by hacking and the use of malicious tools [9]. They are motivated by achievements, show-of-skill, and hacking for the fun of doing it. Vast of tutorials and software are available on the internet on how to perform cyber-attacks and how to acquire malicious software. This group is susceptible for purchasing and utilizing malicious tools and services. The characteristics of script kiddies is that they are unpredictable because of their assumed low knowledge of consequences, overestimation of skill-level, and their lack of self-control. However, it is not expected a great impact from this threat agent [9].

**In Addition - Non-malicious events**

Digital systems are susceptible to human, organizational, and technological errors. Natural disasters such as fires, floods, hurricanes, and earthquakes can cause failure in systems and contributes to risk in digital systems, as well as, management decisions, technical and human errors.

## VIII. CYBER AWARENESS ISSUES IN DEVELOPING NATIONS

There are, however, several challenging factors surrounding the enhancement of cyber threat awareness. Some of these challenges are outline below:

Firstly, there is a communication gap between the public and privateentities. A vastamount of critical infrastructures are private sector owned. As the private sector is concerned about security risks, there is an unwillingness to disclose any information which could give competitors a financial advantage. In consequence, knowledge of cyber threats and their potential impacts is often not freely shared.

Secondly, one of the main awareness issues facing the security of critical infrastructures, in particular, is the integration of web-facing interfaces into key control devices, meaning they can be accessed from anywhere. Devices are connected online for a variety of reasons, particularly due to infrastructures being dispersed over wide geographic areas. This enables remote connection and control, saving on cost. The result is; engineers do not necessarily have to be dispersed to solve a problem, but instead can monitor the infrastructure from a central control location, which houses a control system. However, often critical infrastructure owners have little realization concerning the security of devices connected remotely.

Thirdly, a misplaced trust in existing security systems shows an awareness issue of the level of prevention methods in place and how effective they are. Infrastructures are protected through an in-depth defence approach. Different technology is used on each layer of the infrastructure to ensure that if an attacker penetrates one layer, they are not automatically able to access the next one. As a result, critical infrastructures are often described as having a harder outer shell with a ‘softer’ internal system, in terms of security. However, each of the layers of security provided through, either multiple Intrusion Detection Systems (IDS) or Unified Threat Management Systems (UTM), are known to have vulnerabilities which can be exploited through zero-day attacks.

Fourthly, on a community level, spear-phishing attacks are used for cybercrime purposes to disclose passwords, account details and ascertain payment details. Phishing attacks are becoming increasingly commonplace, and one specific type of phishing attack is known as a spear-phishing attack. This involves a targeted form of a phishing attack [12], where the success rate of the attack is higher compared with the generic bulk approach often used. Spear-phishing attacks are designed with a specific target in mind and associated with human error and lack of threat awareness to be successful. Their aim is to trick the victim into thinking an email-based scam is legitimate by ensuring that the information inside is specific to that person or organization [13].

As a result of successful spear-phishing attacks, several private and government entities have been breached; and each penetration is the direct result of lack of understanding about the nature of the attack, which leads to sensitive information being disclosed.

## IX. CYBER ATTACKS IN MODERN DAYS

Cyber-attacks occur in various forms in modern time as people continue to make a ground breaking records in technological innovations and sciences, and some of these forms are:

**Denial of Service (DoS)**

Denial-of-service (DoS) attack refers to a cyber-attack where the cybercriminal attempt to make an online resource - machine or network out of reach to its legitimate users by momentarily or indefinitely hurting services of a host connected to the network of networks. DoS attacks is normally done by "flooding" the resource with a large number of requests [14]. This makes the server unable to respond to some or all of the authorized requests. Legitimate or authorize clients intending to use the pool of resource are thereby denied access to those resources. An attack coming from a single DoS attack is easily tackled, and that coming from a distributed denial –of –service attack (DDoS attack), where the attacks originate from several sources. DDoS attacks can be conducted by having computer users voluntarily join forces to participate in the attack. More commonly, DDoS attacks are normally organized using botnets - networks of compromised computers whose users are not even aware that their machines are involved in an attack [15]. Unauthorized attackers often target high profile web servers, sites or services – online payment systems that use credit card systems, banking industries, state departments engaged in revenue collection, blackmail [16] [17][18]by using malicious software installed on computer that allows a third-party to have total control of the machine.

**Website Defacement Attack**

Website defacement attack is an attack on a website that changes the content of intended website. This normally happens when the defacer or attacker break into a particular website, changes the contents with their own intended to mislead the owner and people visiting that site. It is another form for electronic vandalism normally intended to convince or motivate "cyber protesters" or hacktivists [19], as evident in the 2016 U.S Elections when a sets of cybercriminals in Russia spread hate or propagandas via Facebook in certain states in the U.S. Most religious and government websites are attacked by politically or religiously motivated cybercriminals to spread political or religious beliefs, whilst defacing the views and beliefs of others.

SQL injection method is most prevalent in website defacement attack. Here, the attacker placed a malicious data in a web form [20]. Theoretically, SQL injections are easily protected, as they only occur as a result of programming error in the website. However, in practice many websites are vulnerable to them due to lax security practices.

Unlike DDoS attacks, a website defacement means that the attacker actually succeeded in getting access to the target computer. However, as explained above, being able to get into an organization's webserver is not the same as breaking into that organization's internal network, since webservers are usually hosted on a different network.

**Other Break-Ins**

Other major issue is break-ins into computers other than ordinary webservers and / or break-ins into webservers if these machines are used to store data other than just the public website. Such break-ins can be done using schemes similar to those used in website defacement. The difficulty of a break-in depends on the IT security level of the target system. Once an attacker has gained access to a machine, they may be able to access other computers on the same network, steal confidential data, and install malware to turn machines into zombies for a botnet, or cause other damage.

## X. CYBER ATTACKERS

Cybersecurity issues are having great challenges for governments and businesses around the world. Indication show an increase in hacked and breached data from source are on the rise due to the break-in in technological innovations and sciences. Research shows that most organizations'data are unprotected and follow poor cybersecurity practices, exposing them to data loss and theft [21] in the cyber ecosystem.

The cyberspace has become a platform where negative consequences costing billions are just wasted as a result of cybercrimes and security. An average expenditures on cybercrime drastically increased on a daily basis, and costs associated with such crimes can possibly cripple entities who have not made cybersecurity a priority in the annual budget.

**Cybercrime**

Cybercrime is becoming a big threat to business and government entities globally. In 2017, cybercrime costs accelerated with company's expenditure increasing nearly by 23% more than 2016 — on average about $11.7 million [22]. The average cost of malware attack on a company worth $2.4 million [23]. From 2016 to 2017, there were 22.7 percentage increase in cybersecurity costs globally [24]. The most costlyelement of a cyber-attack is information loss, representingabout 43 percent of costs [25]. Ransomware damage costs surpassed $5 billion in 2017, 15 times the cost in 2015 [26]. Damage related to cybercrime is estimated to reach $6 trillion annually by 2021 [27].

**Hacktivism**

Hacktivism is coined from hacking and activism. Hacktivists are malicious individuals engaging themselves in hacking activities, as a way to allowunlawful access to a computer or a network, in order to promote social or political agendas.

The rise of digital activism and social media used to publicize and promote political groups; the Arab Spring rising in the Middle East and the anti-austerity movement in Europe. Activists including the recent French labour demonstrations, live streaming videos of their actions using social media applications such as Periscope allowing internet users to contribute to their debate. The party of the new mayor, Ada Colauin Barcelona, succeeded his electoral campaign with more than 5,000 people in the online platform, including the creation of network of cyber activists [28].

The so-called hacktivist groupsincluding the anonymous regularly attacking computer networks of the rich and powerful class, and even terrorist groups such as the Islamic State. The recent Panama Papers follow analogousdisclosures by WikiLeaks and Edward Snowden as examples of "leaktivism". Here, the internet serve as a podium where sensitive data are obtained, leakedincluding confidential recordscontaining political ramifications. The Panama leaks have led to massive demonstrations resulting to the Iceland's prime minister to resign and calls for similar action in the UK [29].

**Cyber Espionage**

Espionage is viewed as an attempt by an individual or state "to penetrate an adversarial system for purposes of extracting sensitive or protected information" [30]. Cyber espionage is acceptable behaviour, unlike cyber-attack which is unacceptable according to international law. The United States has raised objections to certain types of cyber espionage activity: Chinese economically-motivated cyber espionage; the (feared) transfer of data taken from the U.S Office of Personnel Management (OPM) and provided to criminals; and Russian doxing attacks, particularly against the Democratic National Committee (DNC).

Therefore, the United States has been edging towards advocating a new class of standards for cyber espionage – countries may carry it out, but not use the results for other than traditional intelligence purposes, that is for informing national security decision making. Cyber espionage is becoming a normal practice among the U.S, China and Russia. In May 2019, an ex-CIA agent pleaded guilty spying for China according to the U.S justice department in a case linked to the dismantling of a U.S espionage network. Jerry Chun Shing Lee was recruited by Chinese agents in 2007 in Hong Kong.

According to the U.S Prosecutors, a naturalized U.S citizen was paid to divulge information on U.S covert assets. This resulted of China dissolvinga network of informants from 2010 to 2012. Roughly, 20 informants lost their lives or jailed during that period, which is seen as one of the greatest failures of U.S intelligence in moderntime [31].

## XI. DISCUSSIONS

**War against Cyber Crime**

In order to combat mobile fraud and online mobile-money laundering in the country, the National Telecommunications Commission (NATCOM) instructed all Mobile Network Operators (MNOs) to conduct a robust sim cards registration and verification across the country to ensure that sim cards are owned by legal means.The exercise was conducted to ensure that Mobile Network Operators strictly follow their obligations under the SIM Card Registration Regulation of 2009.It also directed at ensuring that the provision of secured telecommunications and mobile financial services, to reduce and possibly eradicate the proliferation of fraud and ensure national security in the country [32].

Addressing a news conference held at the National Telecommunications Commission's Headquarters on Tuesday 21st May 2019, the various MNOs (Africell, Sierratel, Q-Cell and Orange) pledged their commitment in addressing SIM registration/verification issues in the country. The Director of Regulatory Administration at NATCOM, Mr. Sahr Sewah stated cybercrimes relating to the use of mobile telecommunications services has increased for the past months, prompting NATCOM in instructs all MNOs to carry out the sim card registration and verification exercise. "We are giving support to MNOs and also send a clear message to their customers that it is mandatory to register all sim cards," he said.

Mr. Abdul Kamara, NATCOM's Manager for Information Cyber Security said the commission is fighting against impersonation and ensuring collective security and protection of customers in society irrespective of their status. Mobile Network Operators remain committed to providing the best mobile telecommunications services to meet everyneed of Sierra Leoneans. Operators are further committed to supporting NATCOM and the government's agenda to ensure national security safety. Emmanuel Marah of Q-Cell said their system on sim card registration is unique, adding that un-registered sim cards are deactivated prompting the sim card user to register forcefully.

### WAEC Fraudsters

Most lazy students of the West Africa Examination Council (WAEC) candidates normally involve in examination malpractices using social media applications via mobile phone. Some cybercriminals answer questions relating the exams and send it via social networking sites; mostly WhatsApp. This is against the "New Direction Government" policy which prefer "Free Quality Education for all". This policy demand all students to study hard and not the other way round. Paying people to write for you in an examination and also involving yourself in examination malpractices will only land you into trouble", AIG Brima Jah of the Sierra Leone Police cautioned pupils and parents. He called on parents to support the government by monitoring their children and make sure that they study very well so that they will not involve themselves into such a menace [33].

Therefore, the researcher recommends that the West Africa Examination Council officials ensure that during examinations, students are not allowed to enter with their cell phones into examination hall. Also, the cybercrime unit at the Criminal Investigation Department (CID), the Office of the National Security (ONS), Ministry of Information and Telecommunication and NATCOM should draft strong cyber laws for parliamentary approval, and monitor such internet fraudsters.

### Financial Intelligence Unit to Combat Money Laundering and Terrorism Financing

The introduction of OrnageMoney and AfricelMoney transfer as mobile money transfer system into the public domain is aiding massive cyber corruption into the country. Most banks in Sierra Leone today have extended their banking facilities on mobile platforms using mobile phone to check their banking transactions, deposit, collect and make online payment or transfer. Some uses this facilitate to siphon the country's wealth. A well fortify mechanism should be introduce to monitor and prevent such money laundering, financial terrorism and corrupt practices in the country via the Financial Intelligence Unit[34].

## XII. CONCLUSIONS

With new discoveries in science and technological innovations everyday has made it difficult to protect ones' personal data from possible intrusion by an attacker commonly known as cyber criminals. Cybercrime nowadays are given more concern globally; with growing digital threats disrupting global economic, in the tune of billions of U.S dollars [35]. In the United Kingdom, cyber threats are ranked as one of the top four risks to nationwide security, which is higher than that of a nuclear attack.

The main challenges for governments globally is how to improve the awareness of their citizens and businesses on the existing cyber threats in the cyberspace. Most organizations lack the expertise to address cybercrime and cyber security issues due to the costs involved in implementing a security system or training their staff in security measures.

Fortunately, NATCOM have instructed all GSM operators in the country to register all sim card users from May to early June 2019. This will help cyber security experts to easily identify cybercriminals in the country.Therefore, all mobile network operators (Africell, Sierratel, Orange and Q-Cell), the security agencies and departments including NATCOM, ONS, Ministry of Information and Telecommunications, GSM operators, the cyber unit of the Sierra Leone Police Force and the Military together with central government should legislate proactive cyber laws that will potentially punish cybercriminals in the country. Also, massive sensitization and awareness campaign should be organized in order to acquit the general population on the dangers of failing to protect once personal data, as most internet users in the country lack the basic skills to protect their data online. Furthermore, the Ministry of Higher and Technical Education and the Tertiary Education Commission (TEC) should design a curriculum in Cyber Security Studies to be taught at certificate, diploma, higher diploma levels in colleges and bachelor level in universities. This will subsequently provide awareness on cybercrime and cyber security issues in the country.

The use of CCTV cameras in public offices including financial institutions will possibly help curtain cybercrimes in Sierra Leone. To mitigate cybercrimes rate requiremaximum cooperation among the government security agencies and /or between neighbouring countries such as the Republic of Liberia and the Republic of Guinea. High quality education among Internet users will also help create awareness on the preventive methods that will definitely curtail the various crimes associated with online platforms. Other keyproblem is the compliance with privacy and security as most telecommunication companies in developing countries breached people's privacy.There are no strong laws to defend such acts. Also, cyber security should be part of all information systems and electronic system within the country. The government should ensure that active firewalls and other preventive applications and measures are designed to protect the citizens' information. Cyber security is therefore the order of the day where hackers get huge amount of monies illegally and it should be mitigated or even eradicated completely to provide a free and safe country for possible investors.

## RECOMMENDATION

The respective government departments and agencies together with private institutions should embark on massive awareness sensitization both television and print media on the negative effects of cybercrimes in Sierra Leone. NATCOM, ONS, Ministry of Higher and Technical Education, the Ministry of Information and Telecommunications and Tertiary Education Commission (TEC) should draft a curriculum on cyber security that will be taught in tertiary institutions. The government should at least employ one cyber security expert or analyst at all the various government departments. Firewalls must also be installed on all government servers.

The mobile network operators should be vigilant in protecting their client's personal data and privacy, and report any suspicious actions to the security agencies for possible action.Internet user should also be careful on clicking on suspicious mail or link. The government should also levy substantial fine on any telecommunication companies failing to register all their subscribers, which enhance state security agencies to easily track cybercriminals via their mobile phone numbers, social media accounts, and email. Therefore, a though and effective policies and preventive measures will be the ultimate solutions to minimize cybercrimes in Sierra Leone.

## FUTURE WORK

As cybercrime is on the verge to spread in Sierra Leone because of lack of proper understanding on the implications and effects by internet users. The researcher recommends in order to get the primary and secondary coursesof cybercrimes, the security agencies should be professional as that of the Western countries. Therefore, the researcher hope to conduct extensive research on more sophisticated methods on how to detect and prevent cyber-attacks within the cyberspace in Sierra Leone.

## ACKNOWLEDGMENTS

The author is grateful to Professor Paul Abass Kamara and Professor Roseline Umeh Uyanga at IAMTECH. Special thanks and appreciation also goes to Professor EdwinJ. J. Momoh, Vice Chancellor and Principal of Ernest Bai Koroma University of Science and Technology for promoting education in the country. Finally, the research acknowledges Mrs. Elizabeth Guma-Sawaneh for her continuous moral and financial supports to pursue higher education. Much thanks and appreciations go to Dr.Peter Umaru Kamara at IAMTECH for his tireless technical support to young researchers nationwide.

## REFERENCE

[1] Visit report, Sierra Leone Security and Intelligence Service Reform, September 1999.

[2] Buzan, B. & Hansen, L. (2009), *The Evolution of International Security Studies*, Cambridge University Press, Cambridge

[3] Yost, David (2010) NATO's evolving purposes and the next Strategic Concept. International Affairs, 86 (2) 489 – 522

[4] http://www.nato.int/summit2009/topics_en/21-nato-eu_strategic_partnership.html

[5] NATO (2016) NATO Defence Ministers Agree to enhance collective and deterrence. Last accessed 14.7.16 from http://nato.int/cps/en/natohq/news 132356.html? selected Locale=en

[6] Singer, Peter and Friedman, Allan (2014) Cybersecurity and Cyberwar. Oxford University Press.

[7] https://www.itgovernance.co.uk/cyber-security-risk-assessments. Accessed June 2, 2019.

[8] Marinos, L., Belmonte, A., Rekleitis, E., 2016. *ENISA Threat Landscape 2015*. [pdf] Available at: https://www.enisa.europa.eu/publications/etl2015

[9] Marinos, L., 2014. *ENISA Threat Landscape 2014.* [pdf] Available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2014

[10] "Peddler's martyrdom launched Tunisia's revolution: Reuters. 19 January 2011.

[11] "Uprisings in the region and ignored indictors" Payvand.

[12] Mahmoud Khonji, Youssef Iraqi, and Andrew Jones, "Mitigation of Spear Phishing Attacks: A Content-based Authorship Identification Framework", Proceedings of the 6th International Conference for Internet Technology and Secured Transactions (ICITST), 2011, pp. 416–421.

[13] Jingguo Wang, TejaswiniHerath, Rui Chen, ArunVishwanath, and H. Raghav Rao, "Phishing Susceptibility: An Investigation Into the Processing of a Targeted Spear Phishing Email", IEEE Transactions on Professional Communication, Vol. 55, No. 4, 2012, pp. 345– 362.

[14] "Understanding Denial –of –Service Attacks". US-CERT. 6 February 2013.

[15] For a good introduction to the subject of botnets, see Ramneek Puri, "Bots & Botnet: An Overview.", SANS Institute, 8 August 2003, http://www.sans.org/reading_room/whitepapers/ malicious/bots-botnet-overview_1299.

[16] Prince, Mathew (25 April 2016). "Empty DDoS Threats: Meet the Armada Collective". Cloudflare.

[17] "Brand.com President Mike Zammuto Reveals Blackmail Attempt". 5 March 2014. Archived from the original on 11 March 2014.

[18] "Brand.com's Mike Zammuto Discusses Meetup.com Extortion". 5 March 2014. Archived from the original on13 May 2014.

[19] Romagna, M.; Van Den Hout, N. J. (October 2017). "Hacktivism and Website Defacement: Motivations, Capabilities and Potential Threats". Proceedings of the 27th Virus Bulletin International Conference: 41 – 50.

[20] My colleague Thomas Steinbrenner once explain SQL injection in the following way: "Computers know two things: instructions and data. Simply speaking, an SQL injection is when the computer expects data as input but you provide instructions instead and trick it into executing them."

[21] https://info.varonis.com/hubfs/2018%20Varonis%20Global%20Data%20Risk%20Report.pdf

[22] In 2017, cybercrime costs accelerated with organizations spending nearly 23 percent more than 2016 — on average about $11.7 million. https://www.varonis.com/blog/cybersecurity-statistics/ via @varonis

[23] The Cost of Cyber Crime Study. https://www.accenture.com/us-en/insight-cost-of-cybercrime-2017?src=SOMS

[24] The Cost of Cyber Crime Study. https://www.accenture.com/us-en/event-cybertech-europe-2017?src=SOMS#block-insights-and-innovation

[25] The Cost of Cyber Crime Study. https://www.accenture.com/us-en/event-cybertech-europe-2017?src=SOMS#block-insights-and-innovation

[26] Top cybersecurity facts, figures and statistics for 2018. https://www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html

[27] Cybersecurity Ventures Official Annual Cybercrime Report. https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

[28] http"//www.twitter.com/somcumuns

[29] Beyond hashtags: how a new wave of digital activists is changing society. https://theconversation.com/beyond-hashtags-how-a-new-wave-of-digital-activists-is-changing-society-57502

[30] (Rid 2012, p. 20).

[31] Ex-CIA agent Jerry Chun Shing Lee admits spying for China. http://www.bbc.com/news/world-us-canada-48130068.

[32] Kargbo A. B. 2019. Mobile Phone Operators on Massive Registration Exercise …. War against Cyber Crime, Standard Times. Vol. 83. No. 43, pp 7, Wednesday May 22, 2019.

[33] Samura A. A. 2019. WAEC Fraudsters, Standard Times. Vol. 83. No. 43, pp 7, Wednesday May 22, 2019.

[34] Bah M. J. 2019. Financial Intelligence Unit to Combat Money Laundering and Terrorism Financing, Awoko Newspaper. Vol.25, No. 96, pp 2, Wednesday May 29, 2019.

[35] E. Commission, "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection: Achievements and next steps: towards global cyber-security", 2011.