A STUDY ON CYBERCRIME AND ITS IMPLICATIONS ON INTERNATIONAL RELATIONS: THE US – NORTH KOREAN PERSPECTIVES

Ya'u Ibrahim Saleh*

Musa Garba Usman*

Abdullahi Bala Ado**

Abstract

The dawn of information age with its pervasive introduction of digital network have changed every aspect of our life in governments, military, economy, health, personal lives and so on. Information Technology has integrated the world particularly with the use of electronic media. The internet brought about electronic commerce, electronic banking services, electronic government and so on. This has shown the growing importance of Information and Communication Technology (ICT.) However along with this importance, there exist a simultaneous raise of a new wave of crime across the globe in the cyberspace. This new crime perpetrated in the cyberspace manifested from different ramification affecting the economy and national security of nations. Consequently this drastically affects nation's relations at international system. This papers hopes to explore the extent to which some cyber crime threatens nations relations focusing attention to the recent Cyber attack row between the US and North Korea. This paper revealed that the result of increasing technological advancement is taking a new dimension as it starts affecting nation's relation at international system. The paper used secondary source for data collection which emphasizes on documentation and other published and unpublished materials. However, analysis was done based on content analysis techniques. In conclusion, the paper recommends for more international collaboration and partnership between government and private sector to mitigate the menace.

Keywords: Cyber Crime, ICT, Internet Outage, Internet Black Out, Stuxnet.

* Department of International Relations, Faculty of Science and Humanities, SRM University, Kathankullathur (603-203) Chennai, India.

** Department of Local Govt. Studies, SORTED Rano, Kano State Polytechnic, Kano Nigeria.

1. Introduction

The Information age has revolutionalized almost every aspect of our life. The Technological advancement has integrated nations and the world has become a global village. The socio-economic, political, military and even personal lives of individual and group have all been shaped by Information Technology (IT) through the digital network. This brought tremendous development and foster economic well being of nations and society at large. However along with this development, a new challenge is being faced in all these spheres. The emergence of cyber crime that manifests itself in various forms and which at a point in time affects nation's relations at international system. Some of these risks include the rise of extensive cybercrime, fears of terrorists exploiting digital infrastructure, state and corporate cyber espionage, crippling disruption by cyber activists and even suggestions of cyberspace becoming the fifth element of warfare (along with land, sea, air and space) the issue of cyber security has become an extraordinarily important global issue (Sallius, 2012).

The phenomenon of cyber-crime has become global cutting across borders from US to Europe, Africa, Asia, and Middle East etc. This made the crime to be borderless in nature and therefore require a global cooperation in combating it. The intensity of this crime increased since 2001.

One example is the most famous cyber worm attack in recent times, namely that of the worm known as 'Stuxnet' that primarily affected the Natanz nuclear facility in Iran in June 2010. The worm had been called the most sophisticated cyber weapon to date and is credited by some with temporarily paralyzing the Iranian nuclear program; though the Iranian government has repeatedly denied that it caused any severe damage or disruption. Therefore it is hard to know the true scale of the impact of the attack. What is known is that the worm works by infiltrating and gaining remote control of the target system in turn reprogramming it. Stuxnet in particular target centrifuges used in uranium enrichment by changing the frequency of the electric current to them, thereby disrupting their normal operation and potentially sabotaging the enrichment process. Although the source of Stuxnet worm is unknown, some referred it as a military grade cyber weapon, and this lead to speculation that it has been created by some state trying to interfere with Iran's nuclear program (Sallius, 2012). Whatever the origin of Stuxnet may be, the attack proved that cyber weapons can potentially inflict damage in cyberspace and can also be

used to manipulate processes that transfer in to kinetic effects, possibly inflicting physical and real world damage (Ibid).

Another prominent attack that targeted corporations and other private entities include that of an intrusion in June 2011 by unidentified hackers into Citigroup (one of the largest financial services companies in the world) servers saw the mass theft of the credit card as well as other personal information of more than 200,000 of their customers (Kravets, 2011). In addition the attacks that occurred in May 2011 on the US defense and aerospace company Lockheed Martin, which produces several fighter jets such as F-16 and F-22 for the US armed forces is another case in point. While official reports suggested that the damage from the attacks was minimal and quickly responded to, it is reported that restoration of normal employee access to its systems took at least several days following the incident (BBC News, 2011).

Another example was the attack using denial of service, defacement, and other methods launched by group of hackers called Syrian Electronic Army (SEA), also known as the Syrian Electronic Soldiers. Their activities mainly involved targeting political opposition groups and western websites, including news organizations and human rights groups.

In addition to the above cited examples, this paper explored into yet another cyber attacks which subsequently threatens the fragile relation between North Korea and US. This subsequently metamorphosed into imposition of sanction to North Korea from the US in late December 2014.

All the above examples of various cyber incidents indicate the effect of global cyber threats on all types of global actors and this has shown the scope of the problem. There was therefore the need of global cooperation to solve the problem.

1.1 Statement of the Problem

Nations relations at international system are sometime very critical and due to one reason or the other the relation is further becoming deteriorated. Such is the case between US and North Korea. How cybercrime affect nations relations at international system is what constitute the problem which the research hope to explore and analyzed.

1.2 Objectives of the Study

The objective of this paper is to explore the extent at which cyber crime threatens nations relations with a specific reference to the recent Cyber attack row between the US and North Korea. The problem arising from hacking of US base entertainment Company by group of Hackers called the Guardian of peace over the release of satirical movie "The Interview" that show an assassination plot to kill North Korean Leader. This incidence eventually affected nation's relations which produces enmity between the two nations.

2. Literature Review

2.1 Conceptual Clarification

Cyber crime: Is a word that is use each day, however there is no worldwide accepted definition of cyber crime but British police defined cyber crime as an offence committed with the aid of computer network. Cyber crime is also viewed as offence committed due to advancement in computer technology. Various definitions of cyber crime are in existence. In a nutshell, there is no consensus on definition of cyber crime but a working definition from Canadian law enforcement agency defined cyber crime as crime committed via computer or part of the crime is committed using a computer as a tool. Based on the given definitions, cyber crime is divided into two classes as using computer to commit crime already in existence in the physical world using computer and committing of a crime via computers and networks

In the Council of Europe's Convention on Cybercrime (2001), cybercrime is used as an umbrella term to refer to an array of criminal activities including offenses against computer data and systems, computer-related offenses, content offenses, and copyright offenses

According to the convention cybercrime covers four main categories:

a. Offenses against the confidentiality, integrity, and availability of computer data and systems such as illegal access, illegal interception, data or system interference, and illegal devices.

b. Computer related offenses like computer-related forgery and computer-related fraud

c. Content-related offenses (e.g. child pornography).

d. Offenses related to infringements of copyright and related rights. In line with the above explanations a crime committed using computer and networks is referred to as cyber crime.

Internet Outage: This is a term that denotes the sudden and complete halt of internet and mobile 3G network services in a particular country at a particular point in time. The internet outage can last for sometime thereby inhibiting all internet services which could lead to disastrous damage to the economy and government activities.

Internet Blackout: This is a term that denotes the sudden interruption and shutting down of internet services in a particular country at a particular point in time. The internet Blackout can last for sometime thereby inhibiting all internet services which could lead to disastrous damage to the economy and government activities of a nation involved.

Stuxnet: This is a warm virus that is used as malware discovered in 2010. It was designed to attack industrial programmable logic controllers (PLCs) (Wikipedia). Stuxnet target Iranian computer system and wreck havoc to their nuclear enrichment process. It ruined some part of Iran's nuclear centrifuges. The source of the virus is unknown but the disastrous damages it inflicted are real.

ICT: There has been difficulty in finding consensus with regard to the definition of ICT because it depends on where it is used. It is used in education, economic, information technology, socioeconomic development, and governance. However, Information and Communication Technology is generally a term that includes any communication device or application, like radio, television, cellular phones, computer and network hardware and software, satellite systems and so on, as well as the various services and applications associated with them.

3. Methodology

The research methodology is qualitative in nature. The implication of cyber crime in relation to the two nations involved is examined. In doing so available literature related to the topic has been utilized and analyzed. Relevant materials like books, journals, articles News magazine and others have been used during the research and finally content analysis is conducted with a view to providing a comprehensive study.

4. Implementation of ICT in US

United State of America is believed to be one of the technologically developed nations in information technology world over. The United States recorded improvements in many areas

such as business and innovation environment. There were improvements in its ICT infrastructure in terms of wider access to international Internet bandwidth. Overall, the country exhibits a robust uptake of ICTs by all major stakeholders—businesses, government and individuals. These result in a strong innovation capacity and significant ICT-related economic impacts. The ranking of the United States, the largest economy in the world, in the top 10 shows that fully leveraging ICTs is not dependent on small or medium-sized economies, but instead depends on undertaking the right investments and creating the right condition for it. (The global information Technology report 2014)

Most of her activities had been in offering services to the globe in different spheres of life. For example in banking, entertainment and so on. This position earned the country a more recognition across the world. However the opportunity has presented a draw back because with the increasing raise of cyber criminals across the globe, the country has been experiencing the worse threats in the cyber attacks. This necessitates the country to develop a law aimed at combating the act of cyber crime and related offences. The US patriot Act which was passed in 2001 is aimed at combating the menace of cyber crime in US as it expands law enforcement power to monitor and protect computer network. But the increasing threats posed by cyber attacked necessitate the need to cooperate with the private sector with a view to enhancing a best policy toward reducing the menace of cyber crime. Hence The US president Barack Obama re-iterates his determination in this 2015.

5. Implementation of ICT in North Korea

This is a country that came into existence as a separate entity after the Korean Peninsula was divided into two zones North and South in1948. In 1950s Korean war erupted over conflicting claim of sovereignty between the North and South Korea. North Korea was accepted into the UN In 1991. In terms of technology, the country is very tech-savvy (one in 12 North Koreans have smart phones) and computers are not uncommon. The country's relations at international system are very critical especially with the western power. This is because of her stand in the issue of nuclear enrichment program. There has been numerous misunderstand especially between North Korea and US over the issue of nuclear proliferation and consequently North Korea has been

under so various sanctions from the US. This has absolutely weakened the relationship between the two nations.

With this weaken relation, toward the end of 2014; there was yet another incident that has further deteriorated their fragile relations and which resulted in imposition of another sanction the first of its kind in the history of any two nations. The event that led to this sanction was the issue of cyber crime which resulted into cyber row between the two nations and eventually US enforce sanction on North Korea over the cyber attack incidence. This development has clearly showed that the issue of cyber crime is taking a new dimension as it is beginning to affect nation's relations at international system.

6. US -North Korea row over the cyber attack

The event have started when a group of hackers called "The Guardian of Peace" launched an attack over a US entertainment studio called Sony Picture for its attempt to release a satirical comedy called "*The Interview*", which involves a plot to assassinate North Korean leader Kim Jong-un. The hackers made threats against cinemas showing the film. This was after the initial hack which exposed embarrassing emails and personal details about some of the world's biggest movie star. This event turns into one of the most difficult and damaging episodes in recent Hollywood history. Because, On 22 November 2013, there were signs that Sony's computer system had been compromised when skulls appeared on employees' screens with a message threatening to expose "secrets" from data obtained in a sophisticated hack. This caused crippling computer problems for workers at Sony, who were forced to work with pen and paper. At the initially stage, Sony said they were dealing with an "IT matter", but later acknowledged the hack to staff, calling it a "brazen attack" comprised of "malicious criminal acts". (BBC News, 2014).

"Guardians of Peace" claimed they would attack cinemas showing the Sony film. They alluded to 9/11 in their message and said it was a response to the "greed of Sony Pictures".

This development compelled the management of Sony to announce that it had decided not to move forward with their plan of releasing the movie "The *Interview*", However this decision was vehemently rejected by individual and the US government including the US president Barrack Obama. Some individual utter that the hacker won, some said refusing to show the film was an

Un- American act of cowardice which validates terrorist action and set terrifying precedent. The US president Obama also called the decision of the company of not releasing the movie a mistake. He warned that freedom of expression was under threat if the movie was shelved (BBC News, 2014).

It is important to note that this Movie "The Interview" features James Franco and Seth Rogen as two journalists who are granted an audience with Mr Kim. The CIA then enlists the pair to assassinate him.

North Korea is the prime suspect behind the cyber-attacks, as Speculation has been mounted that North Korea may have had a hand in the attack as a form of retaliation for Sony's release of The Interview. A North Korean foreign ministry spokesman called the movie an "***act of terrorism***" , promising "merciless" retaliation if it was released. However, eventually the country denied its involvement but praises the hack and called it a "righteous deed" (Ibid).

Prior to "The Interview" controversy the hactivist had stolen some of the company's prime assets of data that are considered confidential. For example an early version of a script for the next James Bond movie, Specter, was leaked. In addition, five Sony films**,** including the new and unreleased version of Annie, turned up on illegal file-sharing sites and were downloaded up to a million times. Brad Pitt's Fury, which had already hit cinema screens, was also shared (Sallius, 2012).

Furthermore, the whole host of Sony's private company information has apparently been exposed to the public, including bosses' salaries and employees' social security information. Strings of confidential emails between Sony workers have also been circulated and proved to be the most sensitive and embarrassing leaks. (BBC News, 2014)

Following this unprecedented hacking attack on the Sony pictures and the threaten attempt to carry out a terrorist attack on cinemas showing the film on its scheduled release date of Christmas Day 2014. The US Federal Bureau of Investigation (FBI) has starts investigation and it said its analysis pointed a finger to North Korea although many cyber-security experts disputed this and have been skeptical about it. North Korea had also proposes joint inquiry with US into

hacks but was rejected by the US. The result of this was a severe internet outage in North Korea lasting for some hours on Saturday (Ibid).

The US was in essence confident that North Korea was behind the Sony Pictures cyber-attack because the hackers "got sloppy". The FBI director James Comedy said the group posted material from servers used exclusively by the North Koreans. In an International Conference on Cyber Security in New York, The FBI director Mr. Comey while addressing delegates said there was evidence the hackers had used proxy servers in an attempt to disguise the attack's origins, but sometimes neglected to do so, revealing, the FBI believes, the true location (Ibid).

However experts remained unconvinced that the US has proved its case. They maintained that The FBI has not revealed anything new. As various IP addresses have been associated with this attack, some in Taiwan and some in Japan. They also said IP address connected to the internet can be compromised and used by attackers. (Ibid)

With all this issues at stake, Sony Pictures chief executive said his firm always intended to release The Interview, despite threats, he insisted that his firm was "adequately prepared" (Ibid).

and finally on Christmas day 25 December, 2014 this controversial comedy about a fictional plot to kill North Korean leader, Kim Jong-un, has been released in some cinemas and online in the United States although larger theatres decided not to show the film (Ibid).

This incidence of hack therefore escalated into a diplomatic crisis between these two nations. As North Korea has condemned US President Barack Obama over the release of the film. The National Defence Commission (NDC) also accused the US of shutting down North Korea's internet - and described Mr Obama as "reckless" and "a monkey". This bring another internet shut-down hours later.

North Korea's also denounced the US for screening the "dishonest and reactionary movie hurting the dignity of the supreme leadership of the DPRK [North Korea] and agitating terrorism". They accused president Obama as the chief culprit who forced the Sony Pictures Entertainment to indiscriminately distribute the movie. They also added that "Obama always goes reckless in words and deeds like a monkey in a tropical forest." (BBC News, 2014).

Washington was also accused of "groundlessly linking the unheard of hacking at the Sony Pictures Entertainment to the DPRK". All this happened because it is a political satire. The movie depicts Kim Jong-un as a vain, buffoonish despot, alternating between threats and weeping that he's been misunderstood. The people around him have all the signs of fear you might expect with a despot - they second-guess his likes and dislikes. There is a view in the south that these are a particularly powerful means of undermining the regime in Pyongyang. If that's so, The Interview might be a good candidate for inclusion (Ibid).

That fear may explain the North Korean leadership's intemperate, deeply racist language.

In view of the above the US in retaliation, has imposed new sanctions on North Korea, The sanctions affected three North Korean organisations and 10 individuals. The sanctions are believed to be the first time the US has moved to punish any country for cyber-attacks on a US company (Sallius, 2012).

7. US Sanctions on North Korea

The following were among those mentioned in the sanction

- The Reconnaissance General Bureau, North Korea's primary intelligence organisation.
- North Korea's primary arms dealer, the Korea Mining Development Trading Corporation (Komid).
- Korea Tangun Trading Corporation, which supports North Korea's defence research.
- Jang Song Chol: Named by the US Treasury as a Komid representative in Russia and a government official.
- Kim Yong Chol: An official of the North Korean government, according to the US, and a Komid representative in Iran.
- Ryu Jin and Kang Ryong: Komid officials and members of the North Korean government who are operating in Syria, according to the US.
- The White House said

"We take seriously North Korea's attack that aimed to create destructive financial effects on a US company and to threaten artists and other individuals with the goal of restricting their right to free expression," "Today's actions are the first aspect of our response." (BBC News, 2014).

Conclusion and Recommendations

Critically analyzing this incidence, one will come to the conclusion that the US has a hidden motive behind the sanction, this is partly because, while the white House officials told reporters the sanction was in response to the Sony hack, the targets of the sanctions however were not directly involved in the attack. In addition The FBI has previously said it believed North Korea was behind the cyber-attack but the sanctions show the US is not backing off its assertion that the country is responsible, this was despite North Korea denying involvement in the hack, and lingering questions from some cyber-security experts. However it can generally be concluded that the issues of cyber attacks can affects nation's relations at the international system and can metamorphosed and culminated into sanctions imposition on one country or the other. It can also be predicted that the third world war might be fought on the computers considering the different attacks that are being launched though the internet. The paper recommends more partnership between government and private sectors and more international collaboration to mitigate the menace.

References

- "15th Annual Computer Crime and Security Survey 2010/2011" Computer Security Institute "About UNODC" United Nations Office on Drugs and Crimes; URL: http://www.unodc.org/unodc/en/about-unodc/index.html?ref=menutop (Accessed: Jan 20th, 2015)
- Archick, K. "Cybercrime: The Council of Europe Convention" Report for Congress, Congressional Research Service, September 28th, 2006;
- BBC News (2011) http://www.bbc.com/news/30601512 (Accessed 28 March, 2015).

- BBC News (2014) http://www.bbc.com/news/entertainment-arts-30512032 (Accessed 31 March, 2015).
- Ibid
- BBC News (2014) http://www.bbc.com/news/world-us-canada-30661973 (Accessed 31 March, 2015).
- BBC News (2014) http://www.bbc.com/news/technology-30744834 (Accessed 29 March, 2015).
- Beñat Bilbao-Osorio (2014) World economic forum the global information Technology report 2014.
- Ganuza, N., Hernandez, A. and Benavente, D. (June 2011) "An Introductory Study to Cyber Security in NEC" NATO Cooperative Cyber Defense Center of Excellence - Tallinn, Estonia
- Glenny, M. "The Cyber Arms Race Has Begun". Nation, October 31, 2011; 293 (18): 18
- http://en.wikipedia.org/wiki/Stuxnet (Accessed 29 March, 2015).
- Kravets, D. "Citi Credit Card Data Breached for 200,000 Customers" Wired Magazine, June 9th, 2011; URL: (http://www.wired.com/threatlevel/tag/citibank/), last accessed: Nov, 12th, 2014
- Sallius, P. (2012**).**What factors explain why there is not a common and comprehensive global response to cyber threats? Leiden University. Retrieved from https://openaccess.leidenuniv.nl/handle/1887/19509 (pg 3-14)
- Report from UNODC Executive Director Yury Fedetov retrieves from **http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf** (Accessed 21 March, 2015).
- The Front Lines (2014). http://blog.crowdstrike.com/cybercrime-cybersecurity-affects-nations-geopolitics/ (Accessed 23 March, 2015).