THE LEGAL JUSTIFICATION OF CYBER CRIME AS A CRIME OF AGGRESSION IN INTERNATIONAL LAW*

Abstract

The international community is largely undermined and endangered by new waves of crimes occasioned by the evolution of modern and sophisticated developments. One new concern is Cybercrime, which is a crime programmed to attack the communication webworks, structure and security systems of countries by other countries, individuals or groups. Surprisingly, international law has not yet designated Cybercrime as a crime against the international community. Undoubtedly, Cybercrime has negatively affected countries' sovereignty and national security. Some of the consequences of the violation of the sovereignty of these countries include physical damage, collapse and disintegration of national communication networks and disruption of internet-based social and public services. This paper seeks to analyze the components of Cybercrime as it affects a country's security network. The paper submits that the horrors and devastation caused by Cybercrime in the international community now makes it necessary for Cybercrime activities to be classified as crimes of aggression and perpetrators be treated in same vein to guarantee peace and harmony in the world.

Keywords: Crime, Aggression, Cyber hostility, international law, undermining Sovereignty

1. Introduction

Undoubtedly, the emergence of technology and its effect on the world system is alarming. Technology has made social interaction and communication very easy. It has also facilitated the procurement and provision of human beings' economic, social and other needs. Unfortunately, apart from the positive impacts, technology also creates a new form of crime known as Cybercrime, which is endangering and compromising the peace and harmony of the international community.[1] Generally speaking, Cybercrime connotes any activity that uses computers or networks as instruments and devices to perpetrate crime.[2] Apart from the complexity of Cybercrime, it is now a catastrophic menace to the security and sovereignty of countries.[3] This is generally described as cyber warfare. Cyber warfare is a situation where a country or group of persons or individuals launches attacks employing cyber technology on another country's vulnerable public facilities related to its national security and sovereignty. For the past three decades, many countries have been accused of getting involved in cyberattacks against other countries. Countries like the US, Iran, Turkey, Russia, and Taiwan have been accused of committing cybercrimes like data linkage, website defacement, data manipulation activities, etc. These activities paralyzed many internet-based public services and social activities. This certainly calls holistic national and international strategies to deal with an international threat to our peaceful coexistence. These cybercrime activities are also crimes of aggression. Because of the vast and changing nature of international law, it is hereby submitted that there is certainly a relationship between Cybercrime and the crime of aggression. It is this kind of relationship that has made it possible for international law to make rules that are meant to regulate Cybercrime. At the moment, there is still no international convention or treaty on Cybercrime that the international community has generally adopted. The highest that has happened is the draft manual from NATO that is utilized as regulation and directions for cyberattacks regarded as crimes of aggression, cyber operations against critical public facilities of a country, and cyberattacks that target commands of enemy territories and control networks and apparatus. This calls for the establishment of generally accepted international legal instruments which should have a binding force to deal with issues that relate to Cybercrime. This could create the needed public awareness, consciousness and understanding, which are the tools required to galvanize and elicit international cooperation in dealing with the challenges of Cybercrime.[4] This paper seeks to develop the needed legal construct as regards the concept of Cybercrime as an evolving phenomenal notion in international law that can be classified and designated as a crime of aggression which is a threat to public services and sovereignty of countries.[5]

***By Richard Suofade OGBE, PhD,** Lecturer, Faculty of Law, Niger Delta University, Amassoma, Yenagoa, Bayelsa State. Email Address: ogberich@yahoo.com. Telephone Number: 08038698054

[1] Michael Glenmon, 'The Blank-Prose of Crime of Aggression, *Constitutional Law Review*, (3) (5) (2015) 187

[2] Noah Weisbord, 'The Mens Rea of the Crime of Aggression Washington University Global Studies Law Review, (12) (3) (2013) 498

[3] Troy Lovers.' The New Crime of Aggression: A Triumph for Powerful States', *Journal of Conflict and Security of Law*, (18) (3) (2013) 512

[4] Jonathan Ophardt, 'Cyber Welfare and the need for individual Accountability on Tomorrow's Battlefield', *Duke Law and Technology Review*, (9) (3) (2009) 53

[5] David Weissbrodt, 'Cyber-Conflict, Cyber-crime and Cyber-Espionage', *Minnesota Journal of International Law*, (22) (2) (2013) 376

2. The Evolution of Cyber Crime as an International Crime

Undoubtedly, the accelerated development of technology has facilitated communication amongst people, which is certainly advancement in human life.[6] One major improvement in human interaction is the use of information and communication technology strategies which is internet based. One way to guarantee smooth computerized communication is to ensure effective and flawless computerized systems. In other words, Cyberspace, which is a process of human interaction through the use of computers, must be protected.[7] At this time, there are various social networks that facilitate social interactions by the exchange of information through the internet. This space is very critical and important because it is through this means that millions of people in the world interact, communicate, and carry out their daily business transactions. However, despite the huge benefits of the use of Cyberspace, there have been negative manipulations that impede the effective use of Cyberspace. These negative manipulations and their concomitant abuses are generally known as 'cybercrime.' As at April 2022 the estimated number of internet users is put at over four billion people, including the social media users[8]. Cybercrimes generally include[9] offences that bother on privacy, honesty, and probity on the one hand and delivery, distribution and usage of computer data and systems on the other hand. These offences range from hacking/cracking (illegal access) and unlawful acquisition of data, to unlawful interception and unlawful data interference. Furthermore, offences that are computer-related include: fraudulent computer-related acts, copyright-related issues. Finally, offences that are content-related include: hate speech, porn, racism, glorification of violence, religious offence and defamation. The question is, why do people engage in cybercrimes?[10] Generally, the reasons and intentions range from sadism, inordinate ambition, terrorism, military/economic espionage, targeting national information infrastructure, wickedness, revenge, hatred, greed, and ignorance.[11] No doubt, Cybercrime could have a debilitating impact on a country as well as the international community.[12] This may depend on the kind of technology that is being used and the motives of the crime. Some cybercrimes are committed to degrading and destroying a country's military defence.[13] A ready case to be mentioned here was the cyber-attack on Syria by Israel in 2007. A similar method was used by the US against Iran. Cybercrime can also torpefy and incapacitate the economy and social infrastructure base, especially for a country with many internet users. The international community needs to ensure a responsive and responsible use of Cyberspace by its users because of the inimical effect of cybercrimes on countries and their economic and infrastructural development.[14]

There are many ways and strategies to insulate countries against cyberattacks.[15] One key method is to deter by denying the same. A country needs to build and develop a sturdy cyber defence system which is capable of eliminating or at least reducing the chance of attacks. Another way is to deter by retaliating any attack. This method is done by evolving and acquiring the power to punish perpetrators of such attacks. If the adversary anticipates and knows that an attack will elicit a counterattack, the attacker will be circumspect. Most of the time, the second option is generally used because it is seen as less cost-effective and burdensome.[16] The main reason for using this method is the belief that it is not easy to protect the public; therefore, it is better to send a warning signal to any would-be perpetrator to know the consequences of any attack.

It is generally argued that cybercrime activities are thriving because of the dearth of international legal instruments.[17] At best, some international legal instruments and treaties only exist at the regional and multilateral levels. This means such treaties only bind countries and organizations within such regions. Therefore, they only

[6] Matthew Gillet, 'The Anatomy of an International Crime: Aggression at the International Criminal Court' *International Criminal Law Review,* (13) (4) (2013) 845

[7] Jennifer Trahan, 'A Meaningful Definition of the Crime of Aggression: A Response to Michael Glennon', *University of Pennsylvania Journal of International Law,* (4) (3) (2012) 932

[8] https://www.statista.com/statistics/617136/digital-population-worldwide/

[9] Marco Benatar, 'The Use of Cyber Force: Need for Legal Justification', *Groettingen Journal of International Law,* (1) (3) (2009) 382

[10] Kevin Miller, 'Cyberattacks, the Laws of War and the Crime of Aggression, *ILSA Quarterly,* (22) (1) (2013) 24

[11] Tom Ruys, 'Criminalizing Aggression: How the future of Law on the use of force rests in the Hands of the ICC', *European Journal of International Law,* (29) (3) (2018) 912

[12] Susan Brenner, 'Fantasy Crime: The Role of Criminal Law in Virtual Worlds', *Vanderbilt Journal of Entertainment and Technology Law,* (11) (7) (2018) 76

[13] Kenneth Kraszewski, 'Classification of Cyber Operations under International Law', *Finnish Yearbook of International Law,* (25) (6) 164

[14] Anne -Laure Chaumatte, 'International Criminal Responsibility of Individuals in Case of Cyberattacks', *International Criminal Law Review,* (18) (1) (2018) 24

[15] Titiriga Remus, 'Cyber-Attacks and International Law of Armed Conflicts; a jus ad Bellum Perspectives', *Journal of International Commercial Law and Technology* (18) (3) (2013) 182

[16] Reuven Young, 'Defining Terrorism: The Evolution of Terrorism as a legal concept in International Law and its influence on Definition in domestic legislation', *Boston College of International and Comparative Law Review,* (29) (1) (2006) 87

[17] Noah Weisbord, 'Judging Aggression', *Columbia Journal of Transitional Law,* (50) (1) (2011) 134

bind the countries included in that specific regional organization. The effort by the United Nations to set up and adopt an international convention on Cybercrime has not seen the light of the day. The best that has happened at the international level is the attempt by the EU to move for the ratification of the European Cybercrime Convention in a bid to tackle the endemic problem of Cybercrime.[18]

3. Concept and Complexity of the Crime of Aggression as an International Crime

The crime of aggression only shows how aggressive human beings can become.[19] This state of affairs has really caused untold destruction and retrogression to the international community. To curb the debilitating effect, the *jus ad Bellum* principle was established to legally and morally constrain countries from the draconian and tyrannical use of power against other countries.[20] The first attempt at bringing perpetrators to account for their actions was in line with The Treaty of Versailles 1919, particularly Article 227, even though the trial did not happen. The second attempt was the London Agreement for the creation of Military Tribunal (IMT) at Nuremberg in 1945. The crime of aggression was expressly forbidden in line with Article 6 of the London Agreement, which was meant to hold individuals accountable for their actions.[21] One significant development was the definition of the crime of aggression by the UN General Assembly Resolution 3314 (XXIX), in 1974. The resolution defined the crime of aggression as 'the use of armed forces by any State against the territorial integrity or sovereignty or political independence of another State, or in any other manner that is not consistent with the UN Charter.[22] The UN International Law Commission (ILC) in 1996 midwife a Draft Code of Crime against Peace and Security of Mankind, which states that an individual, whether a leader or organizer, who actively participates in or orders the designing, arranging, planning of aggression committed by a State shall be held liable for a crime of aggression.

The definition of crime of aggression is crucial and complex because countries and legal experts give it different interpretations.[23] Unfortunately, the Rome Statue of 1998 has not lucidly provided the definition of crime of aggression. This is paradoxical because one of the key functions of the International Criminal Court (ICC) is to adjudicate on the crime of aggression.[24] Perhaps this was the reason why the Review Conference of the Rome Statute in 2010 gave the Special Working Group on the Crime of Aggression (SWGCA) the mandate to design a proposal about crime of aggression, generally known as the Kampala amendments on the crime of aggression. Article 8, Paragraph 1 of the Rome statute, which was the Kampala Agreement defines the crime of aggression as the designing, arranging, preparing or implementing by a person in a position who has general control over or is capable of directing the political or military formation of a State, which has any act of aggression by its nature, magnitude and scale, and constitutes an obvious violation of the Charter of the United Nations. The point is that whether or not an act is a crime of aggression will depend on objective and subjective elements. The objective element is based on how it is described both in the Kampala amendments on the crime of aggression and in the United Nations Resolution 3314 (XXIX) of December 14, 1974. These can be divided into six points:

(1) The incursion or infiltration by the armed forces of any State of the territorial integrity and sovereignty of another State, or by way of military occupation, no matter how temporary which results from such incursion or onslaught, or any move to annex by the use of force of the territory of another State or part thereof.
(2) Cannonade or shelling by the armed forces of any State against the territorial integrity or sovereignty of another State or the use of any weapons by a State against the territorial integrity or sovereignty of another State.
(3) The obstruction of the ports or coasts of any State by the armed forces of another State.
(4) An onslaught by the armed forces of any State on the land, sea or air forces, or marine and air fleets of another State.
(5) The utilization of armed forces of any State which are within the territorial integrity or sovereignty of another State with the consent of the receiving State, in violation or breach of the conditions provided

[18] Mark Drumbl, 'The Push to Criminalize Aggression: Something lost Amid the Gains', *Case Western Reserve Journal of International Law*, (41) (2) (2009) 311
[19] Ananyo Mitra', Cyber Warfare: A Bane of the Modern Era', *International Journal of Law Management and Humanities*, (4) (5) (2007) 65
[20] Aris Culapa, Cyberattacks, Cyberterrorism and Cyber-use of Force: Countering the unconventional under International Law', *Ateneo Law Journal*, (48) (4) (2004) 1163
[21] Yaroslav Shiryaev, 'Cyberterrorism in the Content of Contemporary International Law', *San Diego International Law Journal*, (14) (4) (2011) 987
[22] See generally, UN General Assembly Resolution 3314 (XXIX)
[23] Priyanka Der, 'Use of Force and Armed Attack, Thresholds in Cyberconflict: The looming Definitional Gaps and the Growing Need for formal UN response', *Texas International Law Journal*, (50) (1) (2018) 398
[24] Mary-Ellen O'Connell, 'Cyber Security without Cyber War', *Journal of Conflict and Security Law*, (17) (4) (2012) 195

for in the mutually signed treaty or any extension of their presence in such territory beyond the end of the treaty.

(6) Any action of any country which allows the use of its territory, which it has decided to keep at the discretion of another country, to be utilized by that other State for committing an act of aggression against a third country.

The subjective element is on the basis of the establishment of the criminal intent by way of taking part in the preparation of the crime. The intention, in this case, should include the fact that the person had knowledge of the crime and the resulting effect of the act of aggression. This kind of responsibility will also include the chief of military or the officials of a country apart from the country itself so long as they have knowledge of the plan of the crime of aggression. The ICC clearly accepts and concedes to the subjective element as the mental element in Article 30 of the Rome Statute. The mental element refers to the liability that a person has for the crimes within the jurisdiction of the court if the physical element is carried out with intent and knowledge. 'Intent' is taken to mean the conduct and consequences. That is a situation where the actor knows the consequences of his action. Knowledge in this paper is seen as knowing the fact that the crime exists or the results that will arise from it. Both elements must concomitantly exist for a crime to be classified as a crime of aggression under the jurisdiction of the ICC. Despite the fact that the act of aggression is forbidden in line with the provision of General Assembly Resolution 2625 (1970), it does not preclude the exercise of the right of self-defence.

4. The changing nature of Cyberwarfare towards lethal warfare

Cyberwarfare is described as ‘transnational cyber offences’ which does not have a name it operates with and no designated borders. The point is that people can successfully use the internet without proper names and identities. This group of people can use false names or simply use their nicknames or sometimes unlawfully use the identities of others for the purposes of perpetrating crimes. The real reason or motive for this illegal action is to escape justice or escape from being caught. Internet technology has evolved so fast that it has affected the way human beings now carry out their daily lives and changed almost every aspect of human life. Hitherto, one can access the internet only through desktop computers that were permanently positioned and identifiable; wireless devices are now all over the place.

Attempts will be made briefly discuss six classes of people who manipulate Cyberspace unlawfully. One first-class relates to people who do not have the technical know-how and prowess. This class of people, without much understanding, distorts the software without realizing the adverse impact. The second class push harmful substances into Cyberspace. This class of people does not have regard for laid down rules and constituted powers. The third class of people consists of criminals who commit cybercrimes and hide behind epithets so as not to be caught. The fourth class is made up of professional people with high form of intelligence and capacity who engage themselves in advanced deception and sharp practices. The class of people are the Cyber-Terrorists who sometimes are called freedom fighters. Cyberspace is full of patriotic users, hackers and cyber fraudsters.

.

In 2007 there was a terrible cyberattack on Estonia, which heralded the international community to the menace of cybercrime activities as one of the contemporary developments and its effect on the crime of aggression. It was in response to this horrific cyberattack that took place in Estonia, that galvanized the NATO member countries in 2011 to adopt NATO Policy on Cyber protection perspective. It was during the NATO summit in Wales in 2014 that approval was made for the Cyber plan by NATO. It was this kind of understanding that made the then NATO secretary-general Fogh Rasmussen to suggest that cyber protection is part of a collective security at the international level. No doubt, cybercrimes have monumental aftermath and repercussions on the international society. For instance, there could be nuclear eruptions and other dangerous impacts if there is an attack on a nuclear facility. Again, a cyber-attack can result in a kinetic warfare. Article 2, Paragraph 4 of the UN Charter prohibits any form of Cyberattack. One landmark example of a cyberattack was the one against Iran by the US in 2010. The catastrophic and devastating effect of this attack can be likened to a crime of aggression. This cyberattack, known as Stuxnet, targeted a factory facility known for enriching uranium in Iran. To enrich uranium, a centrifugal motion was applied to control the pressure and temperature exactly. Stuxnet was planned to change the direction of the centrifugal motion. The Stuxnet virus was known to cause unrestrained vibration until it was enough to disfigure the centrifugal motion. Suffice it to say that the losses occasioned by this cyberattack were monumental.

The foregoing scenario is a clear example of an action to be classified as a crime of aggression. The cyberattack orchestrated against Iran by the US was a war planned and executed to incapacitate and diminish the power and prowess of Iran, not to be able to carry out any embargo policy against the US. This was the kind of action referred to in the Kampala Amendments as the definition of the crime of aggression in line with the UN Charter. It seems clear that persons who are in a position to exercise control over or direct the political or military action of a State

are not covered by the jurisdiction of the ICC, and this calls for an amendment. A cybercrime, most cases do not occur in the context of a tight chain of command. Generally speaking, it is perpetrated by persons who have a weak affiliation with a concerted and collaboratively may or may not be associated with or supported by such a State.

5. Attempts to minimize the divide between Cybercrime and Cyber aggression

Through the UN Charter

One key debate over the years is whether or not States have a right to defend themselves against cyber acts, which are armed attacks. This is in line with the convergence between cybercrimes and crimes of aggression. Article 2, Paragraph 4 and Article 51 of the UN Charter clearly stipulate the provision of self-defence carried out by a country in response to cyberattacks. There is no doubt that international law, through Articles 39, 41, and 42 of the UN Charter, approves acts of self-defence by a country. Under Article 51, the innate right of an individual or collective self-defence in response to an armed attack is a different systematic material when it relates to cyberattacks. The reason is partly that Article 51 only lays emphasis on armed attacks, which do not include cyber-weapons. The foregoing interpretation contradicts the view that harm caused by cyberattacks remains outside the scope of an armed attack under international law. The thinking is that cyberattacks are perilous and therefore are very likely to decimate the infrastructural development of a country. This kind of debate is contentious under international law because the issue of countermeasures may not be the right action to take based on the fact that cyber-attacks are relatively of recent development in the international legal discourse. The point is that, under international law, there are restrictions placed on self-defence. It must be noted that the primary reason for a country to embark on countermeasures is simply to motivate the country being offended to make peace by fulfilling its obligations regarding its acts that have occasioned losses to another country. This is like compensating an aggrieved country without necessarily applying force. When the government of a nation wants to carry out retaliation, such a country needs to bear the issues of necessity and proportionality in mind.

Circumstances that will amount to countermeasures:

1. A State that is offended and desires to take countermeasures should note the following:
   (a) encourage the State responsible for fulfilling its agreed duties in line with Article 43;

   (b) Inform the State responsible of its desire to take countermeasures even if it is still ready to pally with that State.
2. Despite paragraph 1 (b), the offended State is free to take such urgent countermeasures as it deems fit in the circumstances.
3. Any countermeasures taken can still be lifted if the following happens:
   (a) That the unlawful international act has abated. Also,
   (b) that, the dispute is now before a court or tribunal with the jurisdiction to make decisions meant to bind the parties automatically.

Article 52 clearly describes the circumstances that will warrant a country taking vengeance because of what another country did. One major thing that arises is how the sovereignty of a country is affected because of cyberattacks carried out by another country. A country so affected by cyberattacks can quickly take action to address such an attack.

6. Law and Armed Conflict

It is trite that armed conflict is regulated by the Geneva Conventions, The Hague Conventions, and a collection of relevant treaties and laws. All countries that have signed, ratified, or acceded to the rules are automatically bound by them. Customary international law expects all countries who have acceded or signed these treaties and conventions to obey and keep the sanctity of these rules. As regards to war crimes that happen in the convergence of Cybercrime and aggression, there is a need to extend the magnitude of the crime of aggression to add cyber warfare that has all the characteristics of war into the realm of international conventions in reality. The method that should be adopted is to incorporate legal incidents that happened and integrate them into existing legal rules that bother on armed conflict.

7. *Ius in Bello*

There has been concern about the means and weapons of warfare. This is what *lus in bello* lays emphasis on. The focus is that war should be fought according to rules and regulations laid down by international humanitarian law, like the Geneva and Hague conventions. Two main principles regulate how war is fought. They include the

principle of 'distinction' and the principle of 'proportionality.' The principle of 'distinction' lays emphasis on the fact that war should avoid civilians and neutral parties. Even in conventional warfare, combatants find it difficult to obey and observe this principle. It is a herculean task to apply this principle to cyberattacks. This is because of the amalgam of networks and systems of military and civil populations, which make it onerous to place the identity of the war targets. There is also the complexity of the technological systems and networks on which cyberattacks are based. The point is that a person targeted may be affected even though he is not in the country being attacked because of the nature of Cyberspace. This is one of the reasons why this principle cannot be applied to cyberattacks. The second principle of 'proportionality' lays emphasis on the effect of the attack and the correlating target being attacked. For example, if the target is the military and military facilities, the intended attack should avoid other targets, such as the civil population, noncombatants, and neutral parties. In cyberattacks, one major challenge is the problem of identifying and evaluating the impact of a cyberattack. This is principally as a result of the peculiar nature of cyberattacks.

8. *Ius Post Bellum*: Ensuring Justice after War

There is a need to discuss what happens after a war is fought and lost. This is what *Ius post bellum* does. This is premised on three main principles. The first is about how to seek lasting peace. The second is how to hold those culpable to account for their actions. The third is how to galvanize redress and possible compensation. The issue of how to seek lasting peace is taken to mean activities that will bring about healing and restore enduring peace amongst the affected people and environment. Unfortunately, this principle is difficult to be achieved because of cyber warfare's fluid nature and scope. The second principle is equally difficult to be achieved because of cyber warfare's anonymous nature. The third principle of restitution and compensation for persons and state actors affected by physical and nonmaterial losses caused by the perpetrators is usually confronted with the inability to effectively assess and determine the quantum of damage and persons involved.

9. Conclusion

No doubt, Cybercrime has come to stay as a nefarious international crime which poses itself as a threat to the peaceful coexistence and harmony of the international community. There is an urgent need to consolidate the existing checks and create new measures to combat its spread and debilitating effect. For many decades now, cyberattacks have developed using ICT innovations to commit cybercrimes of different kinds. The international community needs to keep an eye on internet-based crimes across the length and breadth of the world. The recent ugly cases of cyberattacks against Estonia allegedly carried out by Russia in 2007 and the US against Iran in 2010 must be avoided in the future. Indeed, these crimes have also caused monumental damage and loss to the affected countries. As mentioned earlier, a cyberattack is seen as a form of warfare fought in order to defeat the opponent and demolish their prowess to counterattack. There is a need to strengthen the Kampala Agreement as well as Article 2, Paragraph 4 of the UN Charter to pointedly classify Cybercrime as a crime of aggression. There is, therefore, a need for every country to fortify and bolster its defence against cyberattacks. One way to get around this is to evolve strategic domestic defence mechanisms and international conventions to deal with Cybercrime. States need to equally embolden and stimulate research efforts and advancement in cyber technology and encourage all domestic attempts meant to galvanize domestic cyber defence against Cybercrime. Unfortunately, there are no internationally adopted treaties aimed at monitoring Cybercrime at the moment. This paper calls on the international community to holistically develop a sophisticated treaty to combat and handle issues arising from our technological advancement. There is a need to punish the antics and perpetrators of Cybercrime severely.