WHO SHOT THE ARROW IN THE DARK?: DETERMINING THE RIGHTS AND OBLIGATIONS OF CYBERSPACE ACTORS UNDER A VEIL OF ANONYMITY

Utkarsh Srivastava[*]

Abstract

The days of the use of projectiles and bullets in inter-state offensives are nearing an end. So are the days of fraud and extortion where the criminal and the victim stood face to face. The world today is a digital one. Crimes and methods of war are taking a similar form as well. There has been a rampant rise in cybercrimes and the concept of cyber-warfare has also evolved, with the demarcating lines between the two getting increasingly blurred over time.

The emergence of Distributed Denial of Services (DDoS) and its use for both commission of crime and warfare creates a situation where the world experiences difficulty in differentiating between the two. The recent case of the alleged cyber-attack by North Korea on Sony has once again brought the indeterminacy regarding the rights, obligations and liabilities of cyberspace

[*]Utkarsh Srivastava is a 4th year student at National Law University, Delhi. The author may be reached at utkarsh.nlud@gmail.com.

actors out into the limelight. Keeping these observations in mind, the problems associated with the anonymity of the perpetrators that plagues cyberspace shall be analyzed by keeping DDoS as a sample.

The article tries to explore the existing law to solve these riddles and to lay down the possible measures that a victim state could take. It would be argued that the domain of cyber laws is founded upon a system of analogies which is effective to a limited extent. Cyber laws are fraught with definitions of a traditional nature, and the emerging cyber activities do not fall squarely within these definitions in every case. The scattered attempts to codify cyber law and to lay down a conclusive rules are too few and lacking in acceptance. The conclusion is an acknowledgement of the need for a separate body of laws which are specifically designed for the cyberspace and more importantly, the acceptance of such laws.

I. INTRODUCTION

"*The Internet is perfect for plausible deniability*."[1]

When Gadi Evron, a computer security expert from Israel, used the above set of words to describe the ambiguity regarding the nature of the series of digital attacks that were conducted against Estonia in the year 2007, and the identity of the attackers, he was highlighting a major problem that the world has recently come to face.

Throughout the history of mankind, the commission of crimes and indulgence in warfare had involved the use of such mechanisms and weapons which had the notion of identification attached to them. These activities were conducted in the physical world, where visibility and transparency are maintained.[2] Since then, the clock has chimed a countless number of times and with that the *modus operandi* of the perpetrators has undergone a sea change. The world today is a digital one, and the crimes and methods of war are taking a similar form as well. With the emergence of cyberspace as a domain where criminals operate and nations attempt to gain an advantage over each other, the identification of the nature of crime or attack, and the source from which it emanates, has become as daunting a task as there could be. This is because the use of cyberspace for crimes and war allows the perpetrators to defy identification.[3] In such a scenario, the very nature of an attack along with the related rights, obligations and sanctions becomes hard to be put down in black and white.

---

[1]Mark Landler and John Markoff, *Digital Fears emerge after Data Siege in Estonia*, NEW YORK TIMES (May 29, 2007), http://www.nytimes.com/2007/05/29/technology/29estonia.html?pagewanted=print&_r=0.

[2]SUSAN BRENNER, CYBERTHREATS: THE EMERGING FAULT LINES OF THE NATION STATES 7 (Oxford University Press, 1st ed. 2009).

[3]*Id.* at 7-8.

This article seeks to study the complications that arise as a result of the anonymity that exists in cyberspace. The article further attempts to lay down the right, obligations and liabilities of nations and individuals in case the link between the attack or crime and such cyber actor can be established in the first place. For this purpose, the article is divided into seven parts. Part I is a brief introduction where the recent trend of the use of cyberspace for crimes and also inter-state struggles has been highlighted. In Part II, the author would put forth definitions of the concepts of cybercrimes and cyber-warfare in order to differentiate between the two. In Part III, the concept of a Distributed Denial of Services (DDoS), which is rampantly being used for crimes, by individuals as well as for inter-state attacks, shall be explained in relation to the legal questions it poses. This shall be followed by Part IV where the author would look at a few prominent DDoS attacks that have occurred in the recent years and highlight the related issues which are still unresolved. An application of the *lex lata* to DDoS attacks shall be carried out in Part V of the article to determine the retaliatory measures that would be legally available to victim states against cyber attackers and also the situations when the existing domestic criminal laws are unable to cover individual cyber activities. Part VI shall look into the Tallinn Manual and the European Convention on Cybercrimes and mark out the reasons for the need to have other treaties which are more comprehensive and popular. Finally, Part VII shall be a short conclusion.

II. LAYING DOWN THE DEFINITIONAL GROUNDWORK

At this juncture, it is imperative to understand the concept of a cybercrime and to differentiate it from cyber-warfare. One of the primary obstacles in combating cybercrime is the difficulty faced in satisfactorily defining it. In the absence of internationally recognized legal definitions, there are functional definitions that focus on general

offense categories.[4] Cybercrimes are crimes of the digital age and are basically the violations of long standing criminal law, which are perpetrated through the instrumentality of computers or information networks.[5]

Compare it to cyber-attacks, and the major point of difference is that the objective to bring about disruption is essentially in the political sphere or in relation to national security.[6] For these attacks to be characterized as cyber-warfare, the involvement and participation of nation-states is a necessary requirement, as war is a struggle between nations.[7] This has been the traditional understanding of the concept as it was assumed that only nation-states could garner the resources needed to wage war.[8]

The Black's Law Dictionary definition of war requires the involvement of armed forces,[9] which is absent in cases of cyber-warfare. This understanding of the inability of individuals to perpetrate an attack of war-like nature[10] and the strict requirement of armed forces has come to be challenged with the advent of cyberspace as a medium of war, in effect leading to a question mark over these traditional definitions. To add spice, the involvement of non-state actors raises further questions as to the manner in which they may be dealt with. With such haziness existing between the definitions of cybercrimes and cyber-warfare, accurate categorization

[4]Nicholas Cade, *An Adaptive Approach For An Evolving Crime: The Case For An International Cyber Court And Penal Code*, 37 BROOK. J. INT'L L. 1139 (2011).
[5]Mrinalini Singh and Shivam Singh, *Cyber Crime Convention and Trans Border Criminality*, 1 MASARYK U. J. L. & TECH. 53 (2007).
[6]Reese Nguyen, *Navigating Jus Ad Bellum in the Age of Cyber Warfare*, 101 CAL. L. REV. 1079 (2013).
[7]YORAM DINSTEIN, WAR, AGGRESSION AND SELF-DEFENSE 5 (Cambridge University Press, 1st ed. 2005).
[8]BRENNER, *supra* note 2.
[9]BLACK'S LAW DICTIONARY 1720 (9th ed. 2009).
[10]BRENNER, *supra* note 2 at 14.

of a particular attack into any of these definitions becomes an almost impossible task.[11]

III. DISTRIBUTED DENIAL OF SERVICES: THE NEW PLAYER IN THE FIELD

A recent trend in the province of cybercrimes has been the emergence of Distributed Denial of Services (hereinafter "DDoS"), a new form of cybercrime which flexibly traverses the distance between cybercrime and warfare. A DDoS attack is a coordinated effort that sends out massive bursts of data at the targets of the attack, and attempts to overwhelm websites and their servers or consume their bandwidth.[12] While DDoS attacks have been used for traditional crimes such as extortion,[13] the case of the 'Mafiaboy' in Canada served as an indicator of the potential of this crime to wreck large scale havoc by shutting down a number of widely used websites.[14] Mafiaboy, a teenager used a DDoS attack to deny legitimate access to users of prominent websites such as CNN.com, Yahoo.com, eBay.com and Amazon.com by barraging them with huge amounts of

[11]Joshua Kastenberg, *Non-Intervention and Neutrality in Cyberspace: An Emerging Principle in the National Practice of International Law*, 64 A.F. L. REV. 43 (2009).
[12]BRENNER, *supra* note 2, at 1.
[13]Jose Nazario, *Cyber Extortion, A Very Real Threat*, IT-OBSERVER (June 7, 2006), http://www.it-observer.com/articles/1153/cyber_extortion_very_real_threat/.
[14]Pierre Thomas and D. Ian Hopper, *Canadian Juvenile Charged in Connection with February "Denial of Service" Attacks*, CNN.COM (Apr. 18, 2000), edition.cnn.com/2000/TECH/computing/04/18/hacker.arrest.01/.

data.[15] The potential of cybercrimes to cause far greater impact than the conventional forms of crime is evident.[16]

The flexible nature of the DDoS mechanism which allows it to be used at larger scales than private commission of crimes has encouraged nation-states to tap this potential as a means for carrying out cyber-attacks. This trend of the usage of DDoS at the level of nation-states raises certain conundrums. The issue that needs to be addressed is with regard to the category into which a particular instance of DDoS, or for that matter any form of cyber-attack, would fall. Factors such as the identity of the perpetrators, the scale of commission and the nature of the targets of the attack end up as the relevant ones for such a determination. In light of the recent spurt in the use of DDoS as the preferred form of cyber-attacks across the globe,[17] the author would attempt to explore these cyberspace related issues in general by understanding them in context of DDoS in particular.

IV. THE COMPLEXITY INVOLVED IN DETERMINING THE NATURE OF THE ATTACK

The identification of the nature of the attack is paramount for the subsequent determination of the rights, obligations and suitable sanctions in every particular case of DDoS attacks. While a DDoS attack by a private entity, motivated by self-profit would be covered

[15]DR. TALAT FATIMA, CYBERCRIMES 157-158 (Eastern Book Company, 1st ed. 2011).
[16]Shalini Kesar, *Is Cybercrime one of the weakest links in Electronic Government?*, 6 J. INT'L COM. L. & TECH. 243 (2011).
[17]Rick Rumbarger, *Viewpoint: DDoS attacks are evolving to take advantage of mobile*, BBC NEWS (July 10, 2012), http://www.bbc.com/news/technology-18786815.

by the domestic laws of a nation, it is the presence of nation-states in the fray which raises issues of whether or not a DDoS attack would amount to the illegal use of force on part of the attacking nation, or could the victim nation claim the right to self-defense under the United Nations Charter[18] by contending that the DDoS attack had satisfied the essentials of an armed attack being carried out by the attacking nation. It all boils down to the categorization of the attack, which is an extremely tricky task considering that the nature of the attacker is very often unknown and the smoking gun is not traceable. This is best understood by delving into the kind of DDoS attacks that have taken place and the ambiguity regarding their nature that still persists.

A. Estonia, 2007

The DDoS attack on Estonia in the year 2007 provides the best depiction of the complex issues involved. Towards the dying days of the month of April 2007, a series of sustained digital attacks were targeted at various components of Estonia's infrastructure.[19] Both civilian and government agencies such as banks, ministries and even the Estonian Parliament's email server were targeted by this anonymous attack,[20] leaving the country at the brink of helplessness. The absence of a visible army firing bullets and launching missiles at Estonia brought forth the problem of identification at its best. While initially, the Estonian authorities blamed the country of Russia for being involved in cyber-warfare against them,[21] very soon the

[18]Charter of the United Nations, Art. 51, June 26, 1945, 1 U.N.T.S. XVI [hereinafter UN Charter].
[19]BRENNER, *supra* note 2 at 1.
[20]Jeffrey T.G. Kelsey, *Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare*, 106 MICH. L. REV. 1427 (2007).
[21]Ian Traynor, Russia *Accused of unleashing cyber war to disable Estonia*, THE GUARDIAN, (May 17, 2007), http://www.theguardian.com/world/2007/may/17/topstories3.russia.

realization that the series of attacks was within the capabilities of mere civilians dawned upon the Estonians. The idea that the attacks were an instance of cyber-warfare on part of Russia was abandoned and the Estonian Prime Minister ended up describing the entire scenario as a "criminal activity".[22] The notion that only nation-states can assemble the manpower, equipment and other resources to wage attacks of this proportion was dispensed with and the capacity of private individuals to use cyberspace in this manner was recognized. To put it ironically, the confusion, ambiguity and lack of clarity were crystal clear in this case, all by virtue of the malleable nature of the DDoS attacks.

B. Georgia, 2008

Shortly before the armed offensive by Russia in Georgia in 2008, the Georgian President's official website, along with the website of the central government and the Ministry of Defense came under a DDoS attack.[23] This affected the government's ability to connect to its people and its sympathizers around the world.[24] While Georgia claimed that Russia was behind the attacks, the Russians washed their hands off the entire episode. The exact identity of the ones behind the attack remained an unsolved mystery,[25] and so did the question of whether or not Georgia was involved in a cyber-war with Russia.

---

[22]BRENNER, *supra* note 2 at 5-6.
[23]Jon Swaine, *Georgia: Russia 'conducting cyber war'*, THE TELEGRAPH (Aug. 11, 2008), http://www.telegraph.co.uk/news/worldnews/europe/georgia/2539157/Georgia-Russia-conducting-cyber-war.html.
[24]John Markoff, *Before the Gunfire, Cyberattacks*, THE NEW YORK TIMES (Aug. 12, 2008), http://www.nytimes.com/2008/08/13/technology/13cyber.html?_r=0.
[25]*Id.*

C. South Korea And USA, 2009

The DDoS attack that targeted the United States government websites, the Pentagon and the White House in 2009[26] was in addition to a similar attack that affected the South Korean defense ministry, Presidential Blue House and the National Assembly in the same year.[27] These attacks were alleged to have been the handiwork of the North Korean government.[28] It is relevant to note that North Korea was merely suspected to be behind these attacks. Even after the attacks were traced back to North Korea, there was no conclusive evidence to suggest that the government in Pyongyang was behind the attacks.[29] It is only when the government can be conclusively linked to the attacks, that questions regarding North Korea's breach of its international law obligations can be resolved.

D. Japan, 2010

Japan had its own share of cyber-attack related problems when its Defense came under a DDoS attack. Japan suspects it to be the Chinese response to a row between the two nations over the collision between a Chinese fishing trawler and a couple of Japanese Coast Guard vessels.[30]

---

[26]*U.S. eyes North Korea for 'massive' cyber-attack*, NBC NEWS (July 9, 2009), http://www.nbcnews.com/id/31789294/ns/technology_and_science-security/t/us-eyes-n-korea-massive-cyber attacks/#.VJqGR14BWA.

[27]*Governments hit by cyber-attack*, BBC NEWS (July 8, 2009), http://news.bbc.co.uk/2/hi/technology/8139821.stm.

[28]Id.

[29]*South Korea hit by cyber-attacks*, BBC NEWS (Mar. 4, 2011), http://www.bbc.com/news/technology-12646052; Supra note 26.

[30]Pauline C. Reich et al., *Cyber Warfare: A Review of Theories, Law, Policies, Actual Incidents - and the Dilemma of Anonymity*, 1 EUROPEAN J. L. & TECH. (2010).

E. South Korea, 2011

A couple of years later, South Korea once again became the target of DDoS attacks on government ministries, banks and the military headquarters, suspected to have been orchestrated by North Korea.[31] Once again the problem of identification of the attacker in cyberspace continued to pose major obstacles in dealing with the menace.

F. Attack On Sony And The Alleged Retaliatory DDoS Attack By USA, 2014

These DDoS attack cases are not the only instances of the use of cyberspace for widespread disruption and damage,[32] with the most recent skirmish in cyberspace being the one related to the attacks on Sony. While the FBI attributed them to North Korea, there has been widespread questioning of the evidence that the FBI has been relying upon to mark out North Korea as the perpetrator by experts.[33] Proof of who is and who is not behind a cyber-attack is extremely difficult to garner.[34] Thus the situation as it stands currently is that by no stretch of imagination can North Korea's role in these attacks be proven beyond reasonable doubt which is essential for FBI's attribution to hold ground.[35]

The DDoS attack on North Korea's limited internet facilities was suspected to be a retaliatory measure against the attack on Sony, by

[31]*Supra* note 29.
[32]*Burma hit by massive net attack ahead of election*, BBC NEWS (Nov. 4, 2010), http://www.bbc.com/news/technology-11693214.
[33]Dave Lee, *What is FBI evidence for North Korea hack attack?,* BBC NEWS (Dec. 19, 2014), http://www.bbc.com/news/technology-30554444.
[34]*Id*.
[35]Brian Todd and Benn *Brumfield, Experts doubt North Korea was behind the big Sony hack*, CNN.COM (Dec. 27, 2014), http://edition.cnn.com/2014/12/27/tech/north-korea-expert-doubts-about-hack/index.html.

USA.[36] This may be defended as being a countermeasure by USA, along with the sanctions that it has recently imposed on North Korea.[37] The legality of such measures, if indeed these were the handiwork of USA, can be determined after an analysis in Part V (A) and (B) of this article.

As of now, with nothing to conclusively pin point the source of the cyber- attack due to spoofing or the creation of intermediaries which hides the location of the attacker,[38] the nature of the attack remains an unsolved mystery. This in turn seriously impacts the manner in which the nations respond to and regulate such activities.

V. DETERMINATION OF RIGHTS AND OBLIGATIONS IN THE BACKGROUND OF THE BLURRING LINE BETWEEN CYBERCRIMES AND CYBER-WARFARE

It is imperative for each nation to note that actors in cyberspace are evolving and mechanisms such as DDoS are being used by both individuals and nation-states as is evident from the Russian DDoS attack on Georgia.[39] With the same mechanism being employed by both, and the problems regarding identification of the perpetrators in cyberspace looming over as a perpetual complexity, the victims, whether individuals or states, would continue to be in a state of dilemma. Whether or not a nation is at war would remain an unanswerable question. Whether or not an individual would have

[36]*North Korea loses its link to the internet*, THE NEW YORK TIMES (Dec. 22, 2014), http://www.nytimes.com/2014/12/23/world/asia/attack-is-suspected-as-north-korean-internet-collapses.html?_r=0.
[37]*Sony cyber-attack: North Korea faces new US sanctions*, BBC NEWS (Jan. 3, 2015), http://www.bbc.com/news/world-us-canada-30661973.
[38]Nyugen, *supra* note 6, at 1105.
[39]Markoff, *supra* note 24.

recourse to law in case a pure DDoS does not satisfy the elements of the traditional crimes would again remain a grey area in the present situation. Also, assuming that the involvement of North Korea or Russia had been established, what recourse would the injured state have had against the perpetrators of cyber-warfare? In the absence of judicial precedents or state practice related to an armed conflict having started due to a cyber-attack, answering these questions would require a foray into unexplored territory.

A. When It Amounts To Cyber-Warfare

"*We will respond proportionately and in a space, time and manner that we choose*."[40]

These were the words of US President Barack Obama in response to North Korea for allegedly conducting the cyber-attack on Sony. First and foremost, the question that arises is can USA respond in any manner that it chooses? The answer which would be in the negative does not imply that President Obama would be without any recourse whatsoever. A determination of the manner in which cyber-attacks would be dealt with under international law can only be made after analyzing such attacks in the backdrop of the existing treaty law and customary international law.

Once it has been established that nation-states are involved, the attacks may be categorized in accordance with international law itself. Art. 2(4) of the UN Charter prohibits the threat or use of force by Member States. In the absence of any definition of the phrase "threat or use of force" in the Charter, reliance may be laid on the *travaux preparatoires* which shows that a proposal to include economic

[40]*Sony Hack: Obama vows response as FBI blames North Korea*, BBC NEWS (Dec. 19, 2014), http://www.bbc.com/news/world-us-canada-30555997.

coercion under Art. 2(4) of the UN Charter was specifically rejected.[41] Thus, political, psychological or economic coercion such as trade sanctions are not covered under Art. 2(4)[42] and is confined to the use of military force.[43]

In contrast, Art. 51 being an exception to Art. 2(4), allows a nation to exercise its right to self-defense against an armed attack. A preliminary but crucial doubt may be pertaining to the possibility of the use of computer networks amounting to an armed attack as opposed to guns and bombs. The ICJ's *Nuclear Weapons* advisory opinion provides the answer when it lays down that armed attacks are not to be restrictively associated with specific weapons.[44] The relevant requirement is the use of force, irrespective of the kind of weapons used.[45] Thus, cyber-attacks can amount to an armed attack subject to the fulfilment of the armed attack threshold.

Once again definitional ambiguity persists in relation to the term "armed attack".[46] Armed attack is narrower and more restrictive than the term "use of force"[47] and calls for the satisfaction of a gravity threshold.[48] The International Court of Justice in the *Nicaragua* case determined that the "scale and effects" test needs to be fulfilled for an

[41]See Doc. 2, G/7 (e)(4), 3 U.N.C.I.O. Docs. 251. 252-53 (May 6, 1945) (Brazilian amendment proposal to include economic coercion under Art. 2(4) of the Charter). For rejection of this proposal see Summary Report of Eleventh Meeting of Committee 1/1, Doc. 784, /1/27, 6 U.N.C.I.O. Docs. 331, 334, 559 (June 4, 1945).
[42]Sheng Li, *When does Internet Denial Trigger the Right of Armed Self-Defence?*, 38 YALE J. INT'L L. 179 (2013).
[43]Michael Gervais, *Cyber-attacks and the Law of Wa*r, 1 J. L. & CYBER WARFARE 8 (2012).
[44]The Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, ¶ 39 (July 8, 1999).
[45]*Id.*
[46]Christine Gray, *The Use of Force and the International Legal Order*, INTERNATIONAL LAW 589 (Malcolm D. Evans ed., 2003).
[47]Sheng Li, *supra* note 42, at 184.
[48]Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, ¶ 35 (June 27) [hereinafter Nicaragua].

armed attack to be constituted.[49] The Court further highlighted this distinction between "use of force" and "armed attack" in the *Oil Platforms* case, and ruled an "armed attack" to be the "gravest" form of "use of force".[50]

The pertinent question is whether a cyber-attack such as DDoS, carried out by a nation, taking Russia as an example, would amount to an armed attack and allow a nation like Estonia to exercise the right to self-defense under Art. 51. An effects based approach would require that the DDoS attack proximately cause some kind of release of kinetic energy and resultant physical damage in order to satisfy the armed attack threshold.[51] The requirement is physical damage arising as a direct and foreseeable consequence in a manner similar to a conventional attack.[52] A major flaw in this approach is that it fails to consider the non-physical effects of cyber-attacks that may turn out to be equally, if not more, damaging as physical attacks.[53] Adopting such an approach would mean that only an attack such as the Stuxnet virus attack carried out in 2010, which resulted in physical damage being caused to the Iranian nuclear facility at a level comparable to the air strikes that were conducted by Israel on nuclear reactors in Baghdad and Syria, would be regarded as an armed attack.[54]

Assuming that the DDoS attack on Estonia was the work of the country of Russia and not a group of individuals, could it be argued that it amounts to an armed attack against Estonia, giving it the right to self-defense under Art. 51. It seems that the effects based approach

[49]*Id.* at ¶195.
[50]Case concerning Oil Platforms (Iran v. U.S.), 2003 I.C.J. 161, ¶ 64 (November 6) [hereinafter Oil Platforms].
[51]Sheng Li, *supra* note 42, at 188.
[52]Michael Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUM. J. TRANSNAT'L L. 885 (1998).
[53]Sheng Li, *supra* note 42, at 188-189.
[54]Nyugen, *supra* note 6, at 1082-1083.

would yield an answer in the negative as a DDoS attack always has non-physical effects. Thus, it can never be considered to be an armed attack. This is an illogical conclusion as the severity of the consequences is rendered to be an irrelevant consideration. The absurdity of this conclusion flows from the possibility that an aggressor nation would resort to a DDoS attack to bring down critical infrastructure of its victim nation and thereby cause damage of a comparable proportion to a physical armed attack, but would still not be legally subject to retaliation under Art. 51 of the UN Charter.

If this were true, then each state would use DDoS attacks instead of physical attacks to cripple its adversaries to the same extent that an armed attack would have done, and still manage to walk away without any sanctions or liabilities. This illogicality can be revealed by equating a DDoS attack to some kind of action that takes place in the physical world, and by then understanding its nature in an analogous manner. The Estonian Defense Minister had highlighted the similarities between the 2007 cyber blockade on Estonia and naval blockades on ports.[55] Can an analogy be drawn between the two?

Way back in 1956, the then Israeli foreign minister Golda Meir had declared to the UN General Assembly that blockades by Egypt against the ships carrying the Israeli flag in the Gulf of Aqaba and the Strait of Tiran would be considered to be an armed attack by Israel.[56] Israel's stance that this would trigger its inherent right to self-defense

[55]NATO Parliamentary Assembly, NATO and Cyber Defence, 173 DSCFC 09 E bis., 2009, ¶ 59.
[56]U.N. GAOR, 11th Sess., 666th plen. mtg. at 1275-1276, U.N. Doc. A/PV.666 (Mar. 1, 1957).

was accepted by the international community.[57] The possibility of naval blockades amounting to an armed attack is therefore a real one.

Drawing an analogy between naval blockades and DDoS attacks, it may be argued that since naval blockades have been recognized as armed attacks[58] and involve the restriction on the flow of trade imposed through such a blockade, DDoS attacks may also be recognized as armed attacks if they satisfy the requirements of scale and effect,[59] as these affect the flow of information.[60] Naval blockades, in a manner similar to DDoS attacks, may not satisfy the kinetic energy requirement as discussed above,[61] which further highlights the feasibility of this analogical extension. The basis of this categorization would be the subjective blurring of the distinction between physical and non-physical goods.[62]

Cyber-attacks that result in fatalities by affecting critical life support systems that shut down computers that control dams and waterworks resulting in large scale floods or severely incapacitate state security by denial of access to the designated persons, are equivalent to armed attacks. [63] A DDoS attack is capable of bringing about these effects, all of it without a single bomb explosion or a bullet shot. In a scenario where a cyber-attack such as a DDoS fulfils the requirement of severity and foreseeability,[64] it would be extremely absurd to deny the inherent right of self-defense to a victim nation where the identity of the attacker nation has been established, merely due to the fixation

[57]Jonathan E. Fink, *The Gulf of Aqaba and the Strait of Tiran: The Practice of "Freedom of Navigation" After the Egyptian-Israeli Peace Treaty*, 42 NAV. L. REV. 121 (1995).
[58]Sheng Li, *supra* note 42, at 194-196.
[59]Nicaragua, *supra* note 48.
[60]Sheng Li, *supra* note 42, at 196.
[61]*Id.* at 193.
[62]*Id.* at 196.
[63] MACRO ROSCINI, CYBER OPERATIONS AND THE USE OF FORCE IN INTERNATIONAL LAW 73-74 (Oxford- University Press, 1st Ed. 2014).
[64]Oona Hathaway et. al., *The Law of Cyber-Attack*, 100 CAL. L. REV. 817 (2012).

with kinetic energy which has come about due to the traditional form of warfare.

In cases where a cyber-attack violates Art. 2(4) of the UN Charter without crossing the scale and effects threshold, the victim state cannot resort to retaliation under Art. 51. It is to be noted that the customary international law obligation of non-intervention in the internal affairs of another nation[65] complements Art. 2(4) and has come to be recognized as coterminous with Art. 2(4).[66] Therefore, a use of force would be in violation of the obligation of non-intervention as well. In the absence of the right under Art. 51, the victim state can fall back upon the option of non-forceful countermeasures or retorsions in case of low-intensity attacks.[67]

Retorsions and countermeasures, which are commensurate to the injury suffered,[68] are lawful retaliations to international law violations by other states.[69] As such, even if the kinetic energy fixation is allowed to have the limelight and is not ignored, a victim of a DDoS attack such as Estonia or even South Korea and US may resort to countermeasures against the violation of the customary international law obligation of non-intervention by the states of Russia and North Korea respectively. As a last step, retorsions such as limiting diplomatic relations[70] or economic coercion such as withdrawal of voluntary aid are lawful but unfriendly steps that the victim states

[65]Declaration of Principles of International Law Concerning Friendly Relations and Cooperation Among States in accordance with the Charter of the United Nations, G.A. Res. 2625 (XXV), U.N. Doc. A/RES/2625(XXV) (Oct. 24, 1970).
[66]Nicaragua, *supra* note 48.
[67]U.N. Int'l Law Comm'n Draft Articles on Responsibility of States for Internationally Wrongful Acts, Rep. of the Int'l Law Comm'n, U.N. GAOR, 53d Sess., Supp. No. 10, U.N. Doc. A/56/10 (2001), at 31, 75; Michael Reisman & James E. Baker, REGULATING COVERT ACTION 90 (Yale University Press, 1st ed. 1992).
[68]Gabcikovo-Nagymaros Project (Hung. v. Slovk.), 1997 I.C.J. 7 (Sept. 25, 1999).
[69]Oona Hathaway, *supra* note 64, at 845.
[70]*Id.*

may take against the cyber attacker state instead of military action.[71] The weight that a nation like North Korea may attach to a retorsion of this kind, taken by South Korea or USA might not be much, in effect leading to doubts regarding the effectiveness of such measures as a response to cyber-attacks by foreign nations.

B. When Non-State Actors Are Involved

The complex nature of the process of link establishment between the attack and the suspected nation gives it ample opportunity to deny culpability, and instead put the blame on individuals or private hacker groups.[72] As has been already discussed, cyberspace blurs the traditional demarcating line that exists between the strike potential of individuals on one hand and states on the other. As such, the possibility of non-state actors such as individuals or private groups carrying out terrorist activities through cyber-attacks would not be too distant. In a scenario where a cyber-attack such as a DDoS attack, resulting in a threat to national security, is carried out from the territory of North Korea on USA, it would be interesting to see if an argument can be made on behalf of USA which triggers Art. 51 of the UN Charter in its favour. Or would USA have to be satisfied with the option of countermeasures?

It is to be noted that Art. 51 allows a state to act in self-defence against an "armed attack". It may be put forth on behalf of USA that the inherent right to self-defence has nowhere been restricted to an armed attack which has been conducted by a nation-state.[73] The Security Council Resolution[74] after the 9/11 terrorist attacks on USA

[71]Gervais *supra* note 43, at 19; Hathaway, *supra* note 64, at 857.
[72]Nyugen, *supra* note 6, at 1105.
[73]Thomas Franck, *Terrorism and the Right of Self-Defence*, 95 AM. J. INT. L. 839 (2001).
[74]Security Council Resolution. 1368, U.N. Doc. S/RES/1368 (Sept. 12, 2001) on the "Threats to International Peace and Security caused by terrorist acts.

recognizes international terrorism as a threat to international peace and security. A threat to international peace and security can be dealt with by the Security Council under Chapter VII of the UN Charter. The Security Council can resort to use of armed force to deal with such a situation.[75] This implies that the Security Council could take actions against the terrorist group Al-Qaeda under Chapter VII of the UN Charter. By logical extension, so can a state take action against an armed attack under Art. 51, irrespective of the nature of the attacker.[76] The Resolution allows "individual or collective self-defence".[77]

According to international law as stated above, cyber-attacks amounting to armed attacks, carried out by terrorist or hacker, would give the victim state to act in self-defence against that particular group. But this debate has not yet been settled in light of the ICJ's advisory opinion in the *Legality of the Israeli Wall*[78] and the *Armed Activities*[79] case which have held the exercise of the inherent right under Art. 51 to be exercisable solely against nation-states.

Another path to Art. 51 in case of non-state actors may be traced by the attribution of the conduct of these actors to the state in question. The test of "effective control"[80] for attribution was laid down by the ICJ in the *Nicaragua* case, which has been diluted to the level of the "overall control" test in the recent years.[81] The high levels of

[75]UN Charter, Art. 42.
[76]Franck, *supra* note 73, at 840.
[77]*Id.*
[78]Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, 2004 I.C.J. 136, ¶ 139 (July 9, 2004).
[79]Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda), 2005 I.C.J. 168, ¶ 147 (Dec. 19, 2005).

[80]Nicaragua, *supra* note 48.
[81]Prosecutor v. Tadic, Case No. IT-94-1-A, Appeals Judgment, ¶ 120 (Int'l Crim. Trib. for the former Yugoslavia, July 15, 1999); Prosecutor v. Lubanga Dyilo, Case No. ICC-01/04-01/06, Pre-Trial Chamber I's Decision on the Confirmation of Charges, ¶ 211, International Criminal Court (Jan. 29 2007).

evidentiary proof required for the satisfaction of these tests makes these methods of attribution of conduct as not the most suitable courses of action in context of the conduct of various actors in cyberspace.[82]

Where the cyber-attack originates from the territory of a particular nation, a victim state may invoke the *sic utere tuo* principle, which obligates states to prevent the use of their territory in a manner which harms the interests of another nation. The landmark *Corfu Channel*[83] decision recognized this principle, which has now come to be regarded as a customary international law norm as it has found recognition in a number of cases[84] as well as General Assembly Resolutions.[85] So in case North Korea knowingly allows Lizard Squad or any other hacker group to carry out attacks on any other nation such as USA or South Korea, from its own territory, the victim state can claim responsibility of the state harbouring the cyber-attackers as there has been a violation of an international law obligation. The entire law dealing with countermeasures would be applicable in response to a breach of an international law obligation.

Additionally, in case Estonia or South Korea and USA can garner proof against Russia or North Korea to show that it was organizing or

[82]Vijay Padmanabhan, *Cyber Warriors and the Jus in bello*, 89 INT'L L. STUD. SER. US NAVAL WAR COL. 288, (2013); Sheng Li, *supra* note 42, at 209 (highlighting the near impossibility of gathering evidence in cyberspace to satisfy the high threshold of the 'effective control' test); *Supra* note 43, at 45 (explaining that the overall control test was applicable to participants in a structured and hierarchically organized group, which is difficult to establish in case of cyberspace actors).

[83]Corfu Channel Case (U.K. v. Albania), 1949 I.C.J. 4, at 22 (Apr. 9, 1949).

[84]Trail Smelter Arbitration (U.S. v. Canada) 1938/1941, R.I.A.A. 1905; Lake Lanoux Arbitration (Fr. V. Spain), 24 I.L.R. 101 (1957); Settlement of the Gut Dam Claims (U.S. v. Can.), 8 I.L.M 118 (1969). (These arbitral decisions concretize the Corfu Channel principle which states that a state cannot knowingly use its territory in a way which is harmful to the interests of another nation).

[85]Cooperation between States in the field of the Environment, G.A. Res. 2995 (XXVII), Dec. 15, 1972; International Responsibility of States in regard to the Environment, G.A. Res. 2996 (XXVII), Dec. 15, 1972.

funding a non-state actor involved in the attack, it may be able to successfully make a claim of the violation of the customary international law obligation of non-intervention.[86] Furthermore, in *Nicaragua* case, the arming or training provided to the rebel forces by USA was considered to be graver than mere supply of funds and was held to be in breach of Art. 2(4).[87] Thus, attacks by non-state actors can be regulated in this manner.

C. When It Amounts To A Cybercrime

Cybercrimes are unconnected to national security and political issues and do not raise legal issues of international law.[88] The identification of these activities as a crime attracts the application of domestic rules and laws,[89] after which an attempt is made at this juncture to bring the DDoS within the ambit of one of the traditional crimes by aligning the features of the DDoS with one of the traditional crimes and drawing analogies. Cybercrimes are personal in nature[90] and do not involve the furtherance of political ideologies or raise issues of national security. A DDoS attack on Feedly, a news aggregator, and Evernote, an online notes service, involved the demand for money in return for putting an end to the attack.[91] This attack can be conveniently labelled as a cybercrime as it fits into the scope of the traditional crime of extortion.

Unfortunately, cyber-attacks do not take up such simplistic shapes on most occasions. There exists a possibility that a DDoS attack in its "pure" form, may not fit into the boundaries of any of the traditional crimes such as extortion, theft, fraud and the like. DDoS attacks, such

[86]Nicaragua, *supra* note 48.
[87]*Id.* at ¶ 292(4).
[88]Hathaway,*supra* note 64, at 831.
[89]Nyugen, *supra* note 6, at 1090.
[90]*Supra* note 8, at 10.
[91]Leo Kelion, *Feedly and Evernote struck by denial of services cyber-attacks*, BBC NEWS (June 11, 2014), http://www.bbc.com/news/technology-27790068.

as the one carried out by the Mafiaboy, may be carried out for no consequential reason with the sole objective of creating widespread disruption and inconvenience to people.[92] Similarly, the hacker group Lizard Squad used DDoS to topple the online gaming networks of Xbox and Sony Playstation, with the intention to simply cause mayhem.[93] The kind of harm that such a pure cybercrime inflicts cannot be replicated by any of the traditional crimes of the physical world.[94] In such scenarios, the system of analogies to regulate cyberspace conduct is rendered ineffective.

What then is the nature of such an attack? It falls outside the scope of cybercrimes and also fails to satisfy the elements of warfare. Is it cyber-terrorism? Cyber-terrorism requires that the attack be aimed at some political or social objective.[95] In those cases where the purpose is simply to create a ruckus without the advancement of any political ideology, the elements of cyber-terrorism also stand unfulfilled. The exact categorization of such activities thus remains unknown.

VI. SEARCHING FOR THE LIGHT IN THE MIST

A few general observations made over the course of the last few pages are that cyberspace is plagued with issues of identification of the nature of attack and the perpetrator. The demarcating line between cybercrimes and cyber-warfare is getting hazy. While *de jure* warfare would remain in the hands of nation-states due to the definitional requirements of warfare which calls for the involvement of nation-states, the fact that civilians are capable of launching cyber-attacks of

[92]*Supra* note 2, at 33-34.
[93]Tony Dokoupil, *Hacked? Xbox and Playstation Networks both go down for Christmas*, NBC News (Dec 26, 2014).
[94]*Supra* note 2, at 34.
[95]*Supra* note 8, at 15-17.

humongous proportions, and satisfying the scale and effects threshold of wars between nation-states, would mean that *de facto* warfare would not remain in the exclusive domain of nation-states.[96]

In light of the evolving trends and crimes in this realm, it is of paramount importance that the system of analogies to determine rights and obligations in the cyberworld be dispensed with. This approach is similar to the pigeon-hole theory of torts propounded by Salmond.[97] If the action fits the definition of one of the crimes or traditional understanding of war i.e. falls within one of the pigeon holes, it is regarded as a cybercrime or warfare as the case may be. Else there is no recourse. Such an understanding of and approach towards cybercrime and cyber-warfare cannot withstand the test of time. It is imperative to accept the fact that the ambiguity that haunts cyberspace erodes the efficacy of the traditional law enforcement mechanisms.[98] Similar is the case with the international law governing inter-state relations. The conclusion being that the tactics we use to control chaos in the real, physical world would be ineffective when it comes to the cyberworld.[99]

The issue of identification of the perpetrators presents a major obstacle in policy formation and implementation in this field. Nations such as the Netherlands believe in the practical feasibility of analogous application of existing international law on a case by case basis.[100] The Netherlands is of the stance that a global cyber treaty is not a necessity,[101] but that is possibly one of the most practical solutions to all these quandaries. Multilateral treaties can go a long

[96]*Supra* note 2, at 107.
[97]RK BANGIA, LAW OF TORTS 16 (Allahabad Law Agency, 22nd ed. 2010).
[98]*Supra* note 8, at 17.
[99]*Supra* note 2, at 8.
[100]Jody M. Prescott, *The Law of Armed Conflict and the Responsible Cyber Commander*, 38 VT. L. REV. 103 (2013).
[101]*Id.*

way in establishing the boundaries of the crimes and defining the customary international law associated to such crimes.[102]

Moving onto the domain of cybercrimes, it is observed that the Council of Europe's Convention on Cybercrimes is the sole international agreement which attempts to define cyber-attacks.[103] While it attempts to combat cyber fraud, copyright infringement and pornography, unfortunately, it does not enjoy widespread acceptance. Therefore, it has been unable to crystallize into a norm of customary international law.[104] The global treaty discussed above would also act as the foundation upon which domestic legislations can be structured and international co-operation fostered in relation to cybercrimes as well.[105]

Specific laws at the domestic level such as the United Kingdom legislation[106] outlawing DDoS attacks and envisaging the possibilities in the cyberworld are required. Such grass root action would be imperative to internalize the structure that a global cyber treaty related to cybercrimes would create, and allow the movement towards a system of regulation which brings about transparency in the domain of cybercrimes.[107]

The Tallinn Manual[108] is a prime example of attempted codification of the UN Charter and the laws of armed conflict as applicable in a

[102]*Supra* note 4, at 1169.
[103]*Supra* note 43, at 19.
[104]*Id.* at 20.
[105]*Id.*
[106]UK Police and Justice Act, 2006.
[107]*Supra* note 4, at 1169.
[108]MICHAEL SCHMITT (ED.), TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (Cambridge University Press, 2013) [hereinafter Tallinn Manual].

cyber context.[109] It is a result of the NATO's invitation to an international team of experts to put together the laws governing cyber-warfare and to bring about some semblance of clarity.[110] The Manual, more or less, follows the same line of reasoning and analogies as has been discussed in Part V(A) of this article and therefore lends authority to such analogical extensions being made. One of the striking and appreciable features of the Tallinn Manual is that it sheds the kinetic energy fixation by recognizing that cyber-attacks without physical destruction may qualify as armed conflicts.[111]

However, the problem still persists. The Manual itself lays down that it is a non-binding document, which merely reflects the opinion of the group of experts, acting in their private capacities.[112] It can be said that the Manual is no more than an iteration of the *lex lata,* and Michael Schmitt, the Project Director of the drafting of the Tallinn Manual, has himself accepted that *lex ferenda* was strictly off limits for the expert body.[113] A major criticism is that the work is a mere restatement of existing treaty provisions with the addition of the word 'cyber',[114] a fact accepted by the Manual itself.[115] On the other hand, it may be argued that it can be accepted to be the "teachings of the most highly qualified publicists", which is a subsidiary means for the determination of the rules of law.[116] Such teachings assume greater significance in the absence of state practice or *opinio juris,* as is the

[109]Brett Esptein, *The Rules of Cyber-Warfare: What are the Issues with these Rules, How Can the United States Respond to an Attack when Applying these Rules, and Should New Rules be Enacted?*, 18 HOLY CROSS J.L. & PUB. POL'Y 247 (2014).
[110]*Id*. at 269.
[111]TALLINN MANUAL, *supra* note 108, Rule 13.
[112]TALLINN MANUA, *supra* note 108, at 23.
[113]Michael Schmitt, *The Law of Cyber Warfare: Qua Vadis?*, 25 STAN. L. & POL'Y REV. 269 (2014).
[114]*Supra* note 63, at 31.
[115]*Supra* note 108, at 6.
[116]Statute of the International Court of Justice, Art. 38(1)(d).

case in the cyber context.[117] In any case, if it cannot be considered to be a source of law, it can serve in a manner similar to the Lieber Code,[118] which was an aspirational attempt at regulation of warfare during civil wars, which finally became a core text in the modern laws of war[119] and gave a fair indication of the legal thinking of that time.[120]

With due respect to all the arguments in favour of and against the Tallinn Manual, it is submitted that it is overly dependent on analogical references to international law as it stands, which is further diluted due to its non-binding nature. The indeterminacy plaguing Art. 2(4) would anyway seep into any such application of the existing law to cyber activities. The Manual, if at all of any relevance, should only be considered to be so at an ad-hoc level, and should in no way block the formulation of a global cyber treaty.

The need for a treaty that lays down clear cut definitions of cybercrimes and cyber-warfare by shedding the skin of being defined in terms of conventional crimes and acts of use of force, is the need of the hour.[121] For such a treaty would allow a distinction to be made between the two and will provide nations with the much needed support to identify the avenue through which these problems can be combated. Such a treaty needs to go beyond analogies and also come up with international guidelines on evidence collection and prosecutions related to illegal conduct in cyberspace.[122] It needs to be a product of the combined efforts of the nations from across the

[117]Lianne Boer, *Restating the Law "As It Is": On the Tallinn Manual and the Use of Force in Cyberspace*, 5 AMSTERDAM L. F. 4 (2013).
[118]Instructions for the Government of Armies of the United States in the Field (Lieber Code), Apr. 24, 1863.
[119]*Supra* note 109, at 270.
[120]William Boothby, *Cyber Deception and Autonomous Attack – Is there a Legal Problem?, in the 5th International Conference on Cyber Conflict, Tallinn*, 2013.
[121]*Supra* note 64, at 881.
[122]*Id.*

globe. The global treaty may very well be founded upon the Tallinn Manual and take the well-suited parts from the Manual itself, but it is imperative that it be structured and designed exclusively for cyberspace.

The legal regime governing the outer space consists of specific treaties which were formulated with the belief that they would further the purposes and principles of the UN Charter.[123] The Outer Space Treaty does not completely exclude the application of international law and the UN Charter,[124] despite being a treaty designed especially for the regulation of activities in outer space. Judge Manfred Lachs has highlighted the dangers related to analogies in his work on outer space law, but it has also been accepted by him that the system of analogies cannot be utterly discarded.[125] The author at this stage submits that cyberspace needs something similar - a legal regime governing cybercrimes and warfare, where analogical references are not the only means of regulation of conduct. Instead, it should be a regime where analogies are restricted to a supportive role.

Above all, acceptance of such a treaty or treaties by various States, as and when it comes into force, is of paramount importance.

VII. CONCLUSION

With inspiration from the words of Justice Bhagwati of the Supreme Court of India who was speaking in relation to the concept of

[123]Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, Jan. 27, 1967, 610 U.N.T.S. 205, Preamble [hereinafter Outer Space Treaty].
[124]Outer Space Treaty, Art. III.
[125]MANFRED LACHS, THE LAW OF OUTER SPACE: AN EXPERIENCE IN CONTEMPORARY LAW MAKING 20-21 (Martinus Nijhoff Publishers, 1972).

equality,[126] I would argue that cyberspace activities are dynamic in nature with various facets and dimensions and these cannot be "cribbed, cabined and confined within traditional limits". At the slightest change in the facts and circumstances, attacks such as DDoS are seen to diffuse from the sphere of crimes to the province of warfare and vice versa, thus highlighting the need for a comprehensive body of law to deal with the situations that take birth in cyberspace, but end up affecting the physical world at large. The emerging field of cybercrimes and warfare needs its own set of laws. The need is further magnified in light of the increase in the use of cyberspace for crimes and inter-state skirmishes.

This would be a set of laws that does not attempt to compress these actions taking place in cyberspace within the confines of the already existent laws, leading to debates over what is applicable and what is not. Such a compression should be practised to prevent cyber activities from being left completely unregulated, but only until a global and comprehensive treaty does not come into force. In this way, the recognition of cybercrimes, cyber-warfare and cyber-attacks as a separate body of laws would serve as the panacea to all the maladies hindering the regulation or prohibition of the existent and emerging cyber activities.

[126]E.P. Royappa v. State of Tamil Nadu, (1974) AIR SC 555.