Jus Corpus Law Journal
Open Access Law Journal – Copyright © 2021 – ISSN 2582-7820
Editor-in-Chief – Prof. (Dr.) Rhishikesh Dave; Publisher – Ayush Pandey

Challenges regarding the Categorization of Cyber Force under International Law

Mudit Burad[a] Vedant Singh[b]

[a]National Law University, Jodhpur, India [b]National Law University, Jodhpur, India

Received 20 May 2021; *Accepted* 02 June 2021; *Published* 09 June 2021

In recent years, the world has obtained such technological advancements that the essential infrastructure like the power grid, stock market, military software, etc. of any nation is not completely unbreachable. Presently, hostile cyber operations which are capable of disrupting these essential infrastructures are of prime concern among the countries. More recently, in the years 2018 and 2019 various countries have agreed to establish an intergovernmental body to look into the aspect of the security of cyberspace in the world. Cyber operation amounting to an attack on a country is a burning topic of debate among scholars that what should be the position of cyber operation under international law.

This paper covers various aspects of the views from both sides. The paper addresses various issues like whether a cyber-attack be considered as a 'Use of Force' under UN Charter, what is the impact of a cyber-attack on the territorial sovereignty of a country, whether a right to self-defense exists against such cyber-attacks or not, and finally and most importantly, the enigma that exists regarding the attributability of such attacks.

Keywords: *international law, cyber attack, self defence, sovereignty, digital.*

INTRODUCTION

In the current scenario of this technologically advancing world, there is no specific international law in place governing the cyber operations done by one country on the other.[1] This may create

[1] Michael N Schmitt, *Tallin Manual 2.0 On International Law Applicable On Cyber Operation* (CUP 2017)

a huge problem in the world community, where the probability of a full-fledged, conventional war is unlikely, and cyberspace is the most preferred mode to damage an enemy country's interests and sovereignty.

CYBER ATTACKS UNDER THE UN CHARTER

The UN Charter under its Art. 2(4) prohibits any use of force by one nation on any other nation, and this has been regarded as *jus cogens*.[2] The article says:

"*All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the purposes of the United Nations.*"[3]

The definition as interpreted by the ICJ as well as various authors has been segregated into three essentials i.e., **Firstly**, the conduct has to be ascribed to a state which shouldn't include any private individual or entity which neither falls within the boundaries of the convention, nor when the harm is similarly done by that of the state. **Secondly**, the conduct must constitute either a 'danger' or a 'utilisation of power'. **Lastly**, in the management of 'foreign policy,' the fear or utilisation of power must be employed.'[4]

Therefore, it can be seen from the Art 2(4) of the Charter does not provide a definition of 'force'.[5] Therefore, for defining the term ICJ has, in various instances applied the ordinary meaning test, which is a mode of interpretation under the VCLT.[6] Dictionary of Law,[7] defines force as any compulsion or threat of violence by a state to another state breaching provisions of public

---

[2] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v US)*, Merits, Judgment, 27 June 1986, ICJ Reports 1986 ('*Nicaragua*'), 187–90

[3] United Nations Charter 1945, art 2(4)

[4] Roberto Ago, 'Addendum to the eighth Report on State Responsibility' (1980) 2(1) Yearbook of the International Law Commission 44; Rein Müllerson, '*Jus ad Bellum*: Plus Ça Change (Le Monde) Plus C'Est la Meme Chose (Le Droit)?' (2002) 7 Journal of Conflict and Security Law 169; Natalino Ronzitti, *Diritto internazionale dei conflitti armati* (4th edn, Torino: Giappichelli 2011) 33

[5] Sir Franklin Berman, 'The UN Charter And The Use Of Force' (2006) 10 SYBIL 9–17

[6] Vienna Convention on Law of Treaties, art 31(1); Stefan Kadelbach, *Interpretation of the Charter, The Charter of the United Nations- A Commentary* (3rd edition, Vol I, OUP 2012) 75

[7] Jonathan Law and Elizabeth A Martin, *Dictionary of Law-Oxford Reference* (7th ed, OUP 2014)

international law, further, according to Law Lexicon,[8] force is exercised when by an act of one, another country is compelled or pressurized to give up its sovereignty in decision making. Therefore, after looking at the meaning in these three widely used law dictionaries, we can safely say that 'force' is broad enough to include not only **armed force**[9] but even intangible force such as a **cyber-attack**.[10]

Tallinn Manual[11] is currently the most appropriate source to understand the law regarding cyber-attacks.[12] Going with what's written in rule 32, peacetime cyber espionage is not in violation of international law *per se* but the method of doing so maybe.[13] Cyber espionage, according to the manual isn't fixed to the limited use of cyber capacities, but extends to any act that puts any other nation in a position of confusion and threat.[14] Therefore, any act of cyber espionage or attack that comes under the plain meaning of force then, that can be considered as 'Use of Force' under Article 2(4).[15]

CUSTOMARY INTERNATIONAL LAW (CIL) REGARDING CYBER-ATTACKS

The customs acc. to Art. 38 of VCLT,[16] rule that *it should constitute evidence of a general practice accepted as law*.[17] There are the **material facts** i.e., the actual practice of states, and the **psychological** or subjective belief that the practice is 'law'.[18] Something similar happened earlier in the ICJ in the *Libya/Malta* case,[19] that the content of present worldwide legal standards must be sought mainly in the governments' existing practise and their opinions.[20] The CIL that is

[8] JJS Wharton , *Law Lexicon or Dictionary of Jurisprudence* (OUP 1987)
[9] B Simma, *The Charter of the United Nations (Commentary)* (3rd edn, Vol I, OUP)
[10] Daniel B Silver, 'Computer Network Attack as a Use of Force under Article 2 (4) of UN Charter' (2002) 76 International law Studies 92,93
[11] *Tallinn Manual* was written at the invitation of the Tallinn-based NATO Cooperative Cyber Defence Centre of Excellence by an international group of approximately twenty experts
[12] *Supra* Note 1
[13] *Ibid* 168
[14] *Ibid*
[15] Vienna Convention on Law of Treaties, art 31(3)(b)
[16] Vienna Convention on Law of Treaties, Vol 1155, 1-18232
[17] Malcolm N Shaw, *International Law* (5th edn) 70
[18] *Ibid*
[19] [1985] ICJ Rep 13; ICGJ 118 (ICJ 1985) (OUP reference)
[20] ICJ Reports, 1985, 13, 29; 81 ILR, 239; Also, the Advisory Opinion on the *Legality of the Threat or Use of Nuclear Weapons,* ICJ Reports, 1996, 226, 253; 110 ILR 163

prevailing conditions related to the use of power defines that any attack may be qualified as a 'use of force' when they produce **effects** that damage civilian property,[21] harm the health of individuals,[22] or jeopardize the security of a state.[23]

This **effect-based approach** has been followed by ICJ in *Nicaragua,*[24] where it held that any aggression would constitute a use of force if *its scale and effect are similar to that of regular use of force.*[25] Under this approach, for example, a A cyber-attack conducted vs a government's stock market that disrupted the nation's essential industries can be titled as a consideration of utilising force.[26] The cases of the Court in *Nicaragua*,[27] *Armed Activities,*[28] and *Oil Platforms*[29] are read as those with laying down the doctrine of "accumulation of events." Tom Ruys (a famous scholar cited by ICJ at numerous stances),[30] presents a concrete explanation to the doctrine stating that the doctrine comes into effect when consecutive attacks occur.

According to the said philosophy, occurrences such as this one would otherwise be considered "less serious" applications of force & these would become "uses of force" when they are part of a "continuing, overarching plan of action."[31] Therefore, in the context of cyber-attack, the overall effect is to be taken into consideration. **The attacks which exclusively target computer systems and result merely in the elimination of data of private organizations, private individuals and**

[21] Russell Buchan, 'Cyber-attacks: Unlawful Uses of Force or prohibited interventions?' (2012) 17 Journal of Conflict and Security Law 212; Heather Harrison Dennis, *Cyber Warfare and the Laws of War* (CUP 2012) 74
[22] "Basic rules of the Geneva Conventions and their Additional Protocols", Additional Protocol I, Part IV, Geneva Convention relative to the protection of civilian persons in time of war (Convention IV of 12 August 1949)
[23] *Ibid*
[24] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America),* Judgment, I C J Reports 1986 at paras 188–190 and Report of the International Law Commission on the Work of Its Eighteenth Session, UN Doc A/6309/Rev1 (1966), ⁋ 195
[25] *Ibid*
[26] Michael N Schmitt, 'Wired Warfare: Computer Network Attack and Jus in Bello' (2002) 84 INT'L COMM OF THE RED CROSS 365, 377
[27] *Military and Paramilitary Activities in and Against Nicaragua (Nicar v US)* 1986 ICJ 14
[28] *Armed Activities on the Territory of the Congo (Dem Rep Congo v Uganda)* 2005 ICJ 116, ¶ 24
[29] *US v Iran* 1980 ICJ 3, 36 ¶76
[30] Tom Ruys, 'Use Of Force' And Article 51 Of The Un Charter: Evolutions In Customary Law And Practice' (2010) 134 GRILI
[31] *Ibid*

merely disrupt the economic activities, then, the force should not be regarded as use of force under Article 2(4).[32]

Further, the concept of **Instant Custom** can be applied by the people supporting the view that cyber operation doesn't constitute such an utitlisation of power. Instant Custom, as explained by *Bin Cheng*,[33] arises when the first incident concerning an act occurs, and a lot of reaction of the international community is experienced.[34] He, in such a situation, advocates that repetition of an act is not at all necessary for the formation of *opinio juris*.[35]

Following this, the first incident regarding a cyber-attack occurred in 2007, when a cyber-attack originating from institutions in Russia launched on Estonia and the international community never condemned this as a use of force.[36] Therefore, an Instant Customary International Law can be said to arise from this incident clearing the stance *that cyber-attacks don't come under such use.*

Today, in this technologically changing world the level of threat to each country is not just limited to conventional attacks, but also to intangible means like that of software attacks, which can create damage comparable to a conventional attack. Also, now every countries' economic, social as well as political aspect is connected to technology or its software, and an attack on a country's software would mean an attack on all three aspects of that nation. Therefore, we would endorse the latter view, which is a modern view that a cyber-attack would and should be considered under 'Use of Force' under Article 2(4) of the UN Charter.

CYBER ATTACKS AND THEIR IMPACT ON TERRITORIAL SOVEREIGNTY OF A COUNTRY

[32] Tom Farer, 'Political and Economic Coercion in Contemporary International Law' (1985) 79 AM J INT'L L 405, 411
[33] 'UCL Laws pays tribute to Professor Bin Cheng' (*UCL*, 24 October 2019) <https://www.ucl.ac.uk/laws/news/2019/oct/ucl-laws-pays-tribute-professor-bin-cheng> accessed 16 May 2021
[34] Cheng, United Nations Resolutions
[35] Malcolm N Shaw, *International Law* (6th edn, 1947) 78
[36] Scott Shackelford, 'From Nuclear War to Net War' (2009) 27 Berkeley J Int'l L 192, 209-10

This is the most important issue regarding the effects of a cyber-attack because the international community is still divided on this as to whether to adopt the conventional approach towards territorial sovereignty or to change it with changing times.

Conventional Approach

State is a central discussion point when it comes to talking about the internationally set legal standards across the world.[37] It becomes necessary to understand the legal position regarding the term '*territory*' *as the fundamental concept of territorial sovereignty* relates to the **territory of a state**. The territory has been defined as a physical, geographical part of a country that can be located on the map.[38] Territorial sovereignty in general means controls over a specific territory by a nation-state.[39] The exercise of its territorial sovereignty by a state can be done within its boundary only.[40] And, the boundary of a state can be defined as a fictional line that demarcates the territorial expansion of some particular region and the nation as a whole.[41]

From the ICJ judgments as well as the opinions prevailing regarding the idea of territory and territorial sovereignty, it can be said that cyber-attacks cannot violate the Territorial Sovereignty of a State because **it does not destroy or affect the geographical location held by a particular country rather, it just hampers the functioning of the state through affecting its cyberspace** i.e., telecommunications, destruction of sensitive data, infecting the cyberspace with a malware.

Modern Approach

In the continuously developing, evolving and technologically advancing world, there's a widespread consensus over the principle of territorial sovereignty that a state must possess power over the territories it controls.[42] "*Sovereignty in relation to states signifies* ***independence****. Independence in regard to the portion of the globe is the right exercise therein, to the exclusivity of any other States, the function of a State*."[43] Further, sovereignty ordinarily is been defined as having

[37] Malcolm N Shaw, 1947-International Law (6th edn, 1947) 487
[38] Bryan A Garner (ed), *Black's Law Dictionary* (9th edn, St Paul MN: Thomson West, 2009) 717
[39] Oppenheim, 1 *International Law* (R J Jennings and A D Watts eds, 9th edn, London 1992) 563
[40] *Ibid*
[41] Robert Bledsoe and Boleslaw Boczek, *International Law Dictionery* (Santa Barbara Califf 1987) 143
[42] *The Lotus*, PCIJ Ser A, No 10, at 18 *et seq* (1927); *Free Zones of Upper Savoy and Gex Case,* PCIJ Ser A/B, No 46, 166 *et seq* (1932)
[43] 2 RIAA 829, 838

sole authority without anyone's interference.[44] The territorial sovereignty principle protects a State from being interfered in any form by any other State.[45]

It may be argued that territorial sovereignty is applicable only on the physical geographical territory which can be located on the globe. But what they fail to acknowledge is the fact that cyberspace can be considered in the category of telecommunications, and the legal framework for the telecommunications industry is been given by a lot of INTELSATs which are namely the International Telecommunication Satellite agreements which enable each country to establish their control over their telecommunication systems.[46] A state who is willing to set up a new or control over an existing satellite television broadcasting can do so by notifying the International Telecommunications Union.[47] Therefore, if we apply the concept of sovereignty discussed prior, then it can be fairly concluded that a particular country does have control over its telecommunications or cyberspace, it must be considered as a part of the territorial sovereignty of a country.

Including the internet, telecommunication, computer systems, etc., cyberspace is considered to be an area within the world of information.[48] Although, legally cyberspace is considered to be *res communis omnium*.[49] Notwithstanding the accurate designation of 'virtual worlds as being such' as just a res communis omnium, Government experience demonstrates that digital world, but furthermore: elements thereon, isn't really exempt to sovereignty and jurisdictional challenges and their use.[50] Governments have uptil now and even from hereon and will strive to wield their penal authority over cyberattacks.[51]

---

[44] Bryan A Garner (ed), *Black's Law Dictionary* (9th edn, St Paul MN: Thomson West, 2009)
[45] *Ibid*
[46] JM Smiths, *Legal Aspects of Implementing International Telecommunications Link* (Dordrecht 1992)
[47] 'Resolutions adopted by the General Assembly at its 37th session' (*Dag Hamrraskjold Library*) <https://research.un.org/en/docs/ga/quick/regular/37> accessed 17 May 2021
[48] Arie J Schaap, 'Cyberwarfare Operations: Development and Use under International law' (2009) 64 AFLR 121, 126
[49] 'Strategy for Operating in Cyberspace' (*US Department of Defense*) <http://www.defense.gov/news/d20110714cyber.pdf> accessed 17 May 2021
[50] Buchan (n 22) 10
[51] Council of Europe Convention on Cybercrime of 23 November 2001, ETS No185

Further, various kinds of attacks or other violent actions in the genre of cyberattacks in the cyberspace region of the U.S. is considered to be a cyber-attack according to the U.S. International Strategy of Cyberspace.[52] This may act as an instance to prove the *opinio juris* or the intent of the international community to treat cyberspace as a matter of territorial sovereignty and any act violating it, as an act violating the sovereignty and territorial integrity of a state.

Therefore, from the changing State Practice as well as the *Opinio Juris* a fresh Customary International Law can be established that cyberspace does come under the area of territorial sovereignty of a state.

CYBER ATTACKS AND THE RIGHT TO SELF-DEFENCE

The Right of Self Defence is enshrined under Art. 51 of the UN Charter, which says: "*Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations until the Security Council has taken the measures necessary to maintain international peace and security*…."[53] Sel-defense is a condition which can only happen when there seems to be a happening of a armed & violent acion against the said individual(s).[54] But the international community, as well as the scholars, are divided on the issue of inclusion of the said defense should be a part of the clause 51 & the most prominent reason for the same is that the term 'armed attack' is left undefined, therefore, it is open to a lot of interpretation.[55] The two differing opinions are as follows-

CYBER-ATTACK DOES NOT COME UNDER AN ARMED ATTACK

[52] David P Stewart, 'The UN Convention on Jurisdictional Immunities of States and Their Property' (2005) 99 AJIL 194,195

[53] UN Charter 1945, art 51

[54]CASSESE Antonio, 'Under What Conditions Belligerents May Be Acquitted of the Crime of Attacking an Ambulance?' (2008) 6(2) Journal of International Criminal Justice 385-397;
Dinstein Yoram, *War, Aggression and Self-defence* (3rd edn, CUP 2001) 318;
Galand Renaud & Delooz François, 'Larticle 31, par. 1 c) du Statut de la Cour pénale internationale : une remise en cause des acquis du droit international humanitaire?' (2001) 842 IRRC, 533-538

[55] ÖykülIrmakkesen, 'The Notion of Armed Attack under the UN Charter and the Notion of International Armed Conflict – Interrelated or Distinct?' Geneva Academy of International Humanitarian Law and Human Rights, 4

Geneva Convention of 1949,[56] a customary norm, is applicable wherever this is the slightest chance of a war or any such action of the said level.[57] Further, Article 49(1) defines 'attacks' as 'acts of violence against the adversary, be it in offense or be it in defense.[58] It should be seen that 'acts of violence' mean acts of warfare involving the use of violence means an immediate loss of life.[59] And, stealing important military or personal data by penetrating illegally into the ministry of defense's website, does not bring any immediate loss of lives, therefore it can't be an armed attack.[60]

An attack that results in large-scale adverse consequences alone does not qualify as an attack,[61] according to the International Group of Experts.[62] The ICJ in the *Nicaragua* case has explicitly mentioned that "mere frontier incidents" do not constitute armed attacks and are instead "fewer grave forms of use of force."[63] Further, the ICJ in the *Nicaragua*, *Oil Platforms*,[64] and *Armed Activities* cases,[65] interprets armed attack as "the gravest form of the use of force".[66] And most importantly, the conventional view on armed attack involves, an act of mobilizing arms violating a country's sovereignty and borders.[67]

Following the principle above, it can be said that a cyber-attack which unlike a traditional armed attack does not violate the territorial borders of a country, plus they are not capable of damaging the lives of people directly, therefore, it cannot be regarded as of that level which goes over the top of the present situation. So, a cyber-attack isn't an equivalent to a situation of an attack

---

[56] Michael N Schmitt, Tallinn Manual on the International Law Applicable to Cyber Operations, in *Tallinn Manual On The International Law Applicable To Cyber Operations* 9, 27 (2 edn, 2017)
[57] International Committee of the Red Cross (commentary), Geneva Convention, art 2, ¶1, 20
[58] Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the protection of victims of International Armed Conflicts (Protocol I), art 49(1), June 8, 1977, 1125 UNTS [hereinafter Additional Protocol I]
[59] ICRC, 'Constraints on the Waging of War' (*Introduction to International Humanitarian Law*¸ March 2001) <https://www.loc.gov/rr/frd/Military_Law/pdf/Constraints-waging-war.pdf> accessed 18 May 2021
[60] Joyner and Lotrionte, 'Information Warfare' 855
[61] Schmitt (n 1) 91
[62] *Ibid*
[63] *US v Nicaragua*, ICJ Reports 1986, ¶ 91
[64] *Nicaragua* (n 26)
[65] Schimdt (n 27)
[66] *ibid* ¶ 191
[67] *DRC v Congo* [2005] ICJ REP 168

containing large amounts of armour. Hence, no Right of Self Defense arises in cases of a Cyber Attack.

CYBER ATTACK DOES CONSTITUTE AN ARMED ATTACK

Contrary to the above, 'so called' obsolete criterion of an armed attack, the trans-border element is given most importance. This criterion, unlike the traditional view, is always fulfilled when a country performs a cyber-attack on another one.[68] Also, there's no particular, exact or right definition of an Armed Attack given in the UN Charter.[69] But at the same time, ICJ made it clear that Article 51 applies to any 'Use of Force irrespective of the weapon used.[70] Karl Zemanek an emeritus professor of law in his works clearly and persuasively notes that, 'it is not the device or devices used which matters, it's the intent is what matters the first and foremost and then the effect matters', any utilisation of a device that ends with the extensive damage to private lives,[71] and destruction to property can be considered as Armed Attack.[72] According to the ICJ, "trifling border instances" lack the required intensity to be classified as one to be called an attempted attack(s).[73]

Nevertheless, the Law doesn't define the boundaries of what constitutes an attempted assault in a particularly precise way; rather, the Oil Platforms decision suggests that the level of severity is a fluid one which is contingent on the individual particular instances.[74]

It is to be noted that,[75] it is the scale and effect of any act that qualifies it as an Armed Attack.[76] Therefore, any cyber-attack which raises to the level of conventional attack i.e., destroying lives of common people of the target country, or violating the sovereignty of any state, then that attack

---

[68] Michael N Schmitt, Tallinn Manual on the International Law Applicable to Cyber Operations, In *Tallinn Manual On The International Law Applicable To Cyber Operations* 340 (2 edn, 2017)
[69] *Nicaragua* (n 64) ¶ 176
[70] *Nuclear Weapons* (n 21) ¶ 39
[71] Karl Zemanek, 'Armed Attack', *Max Planck Encyclopedia of Public International Law,* (2012) Vol 1, pp. 599
[72] The UN high level panel on Threat, Challenges and Changes, SC Res 1368 and SC Res 1373, UN Doc/AA/59/565, 2 Dec 2004, ¶ 14
[73] *Nicaragua* (n 64) ¶ 195
[74] Ruys (n 28) 143
[75] Marco Roscini, *Cyber Operations and the use of Force in International Law* (OUP 2016) 73
[76] Yoram Dinstein, 'Computer Network Attacks' 105

can be qualified as an armed attack and would give rise to a right of self-defense under Article 51.

ENIGMA OF ATTRIBUTABILITY

Chapter two of the draft articles of state responsibilities[77] enshrines that if the conduct is done by a state authority or a person controlled or directed by the state or done due to default of state officials then the conduct is attributable to the state.[78] This essentially means that, if a state directly attacks another state through its functionaries or lets the non-state actors attack, willingly or negligently by not taking reasonable care, then only the state can be made liable for the attack.

Now, the question as to what the threshold of reasonable care should be. If we impose very high standards of reasonable care, then the states would have to breach the privacy of the individuals and convert into a surveillance state and if we put the threshold too low then the instances of cyber-attacks will keep on happening and there will be no one to hold responsible. Also, the extent of cyber technological advancements in the area of information technology would be a relevant factor while determining the standard of reasonable care for a country. For example, the standard of reasonable care should be much higher in Israel as compared to South Sudan. Therefore, there is no scope for making a universally applicable standard of reasonability.

To attribute an attack to a country we need to trace back the attack's origin, but with the technological advancements, tracing down and attributing the cyber-attack has become very problematic. There are two main questions related to attributability first is whether the attacks are initiated by a state or non-state actor and the second is whether the state from where the attack originated, is responsible or not. These questions are of immense importance because of the technological constraints. For instance, when the Chinese military hackers breached the firewalls of US department of defense servers to steal the blueprints of US Airforce jets, the US could not do anything at all because they could not prove that the Chinese government is behind

[77] Draft Articles on Responsibility of States for Internationally Wrongful Acts 2001
[78] *Ibid*

the attacks, or these attacks were just routed through Chinese servers.[79] In another similar case, when there was a cyber-attack on Winter Olympic games of 2018 held in PyeongChang, South Korea, where according to US reports, the attackers were Russian military agency that routed the attack through a North Korean IP address to make it look like their belligerent neighbour launched the attack.[80]

The attackers use techniques such as virtual private networks, proxies, and onion routing which is sending data with numerous encryption layers which get redirected to different servers all over the world with the decryption of each layer. In this way, it becomes practically impossible to trace the attacks to their origin with certainty but sometimes these attackers make mistakes because of which they get caught, for example, one of the hackers of the infamous Lazarus group hacker Park Jin Hyok who got identified and charged by the US Department of Justice for the "WannaCry" malware outbreak and attempt to hack US defence contractor Lockheed Martin among other charges because he opened his mail on the Lazarus group's IP address.[81] The US alleged that the Lazarus group including Park Jin Hyok is sponsored by the North Korean government under Article 4 of ARSIWA because Park Jin Hyok was the employee of a Government-owned company in North Korea[82] but the same enigma of attributability would make it almost impossible to prove beyond reasonable doubt that the group is run by or supported by the North Korean government in any way. The threshold of proving beyond a reasonable doubt is the most important thing in attributing criminal liability to a state because a small misunderstanding can lead to a war with the wrong country. Therefore, we can conclude that there cannot be a universal law that defines the attributability, rather, we should create an international task force to investigate the matter for each case and will report directly to the UNSC.

---

[79] Richard Norton Taylor, 'Titan Rain - how Chinese hackers targeted Whitehall" (*The Guardian*, 5 September 2007) <https://www.theguardian.com/technology/2007/sep/04/news.internet> accessed 19 May 2021

[80] Editorial, 'Winter Olympics hit by cyber-attack' (*BBC News*, 12 February 2018) <https://www.bbc.com/news/technology-43030673> accessed 20 May 2021

[81] *US v Park Jin Hyok* MJ18-1479

[82] Catalin Cimpanu, 'How US authorities tracked down the North Korean hacker behind WannaCry' (*Zero Day*, 6 September 2018) <zdnet.com/article/how-us-authorities-tracked-down-the-north-korean-hacker-behind-wannacry/> accessed 20 May 2021

CONCLUSION

It is apparent from the analysis of various aspects of the international community that can get affected by the illegal use of cyber force, it can be said with utmost certainty that this topic needs to be answered with clarity as soon as possible by the nations. The technology today knows no bounds and can breach any level of security, so, it becomes very pertinent for the nation-states to come together can formally enact a law that governs the use of cyber operations.

After extensive research in this area, we found various reasons as to why the use of cyber force be regarded as a Use of Force under the UN charter, should be held to be violative of territorial sovereignty of a country, and right to self-defence must be present against cyber-force as this does amount to an armed attack. Reasons being the capability of today's technology to cause harm to another nation much more than a conventional attack. Because stealing or destroying an enemy country's data does not only causes harm at that point in time but also puts that victim country into a vulnerable state of uncertain future. Such cyber operations also have the ability to breach an individual's right to privacy very easily, therefore, the threshold of caution while dealing with such cases must be higher. And to solve the enigma of attributability, objectivity in law would not work because of the numerous variables involved which might get overlooked, therefore we have to make laws that allow subjective assessment and investigation of the matter at hand.