ORIGINAL RESEARCH PAPER

Law

OPENING PANDORA'S BOX: CYBER ATTACKS, NON STATE ACTORS AND ATTRIBUTION UNDER INTERNATIONAL LAW

KEY WORDS: Attribution, State responsibility, virtual attacks, non-state actor

Professor Sunil Deshta Department of Laws, Himachal Pradesh University, Shimla-171005 India.

Aastha Agnihotri Aastha Agnihotri, Ph.D. Research Scholar, Himachal Pradesh University, Shimla-171005 India.

ABSTRACT

The development of cyber-space has diminished international boundaries and consequent emergence of cyber warfare has caused complex problems. Conventionally, international wars are fought between two nation-states. Penetration of non-state actors in international cyber space has allowed non- state actors to launch cyber attacks against state actors, thereby altering the way traditional wars are fought. In the recent years, it has been witnessed that physical and/or economic harm can be caused to a state through virtual attacks. Many of such attacks have been attributed to non-state actors. This has raised complex challenges for the international legal system. Under the international legal system, state responsibility is a fundamental principle that ensures that states make reparations for any breach of international law attributable to them. However, this obligation does not extend to non- state actors and henceforth, states have easily eluded responsibility for cyber attacks stimulated by non-state actors present in their territory. State responsibility is quintessential to deter violations of international law. In presence of an implicit immunity to non-state actors stimulating virtual attacks, there is an ever- increasing danger of virtual attacks that gravely impacts civilians along with state functionaries. In this backdrop, the authors seek to examine whether the virtual attacks of non-state actors can be attributed to states under whose territory they are present.

INTRODUCTION

"You can't say civilization don't advance,
In every war they kill you in a new way."
-Will Rogers

Wars have been fought on land and sea throughout history. However, within the last 100 years, the face of warfare has evolved dramatically, and rapidly due to technological advancements. In the First World War, soldiers were dragging themselves through muddy trenches and dodging mortars. The technological advancements in air and space made it possible to fight the Second World War with V-2 rockets and atom bombs. Development of autonomous weapons made us witness use of drones and long- rage missiles during the Gulf Wars. In the 21st century the nations are facing an entirely different kind of battlefield and a different brand of weaponry. After land, sea, air and space warfare has entered a fifth domain –

Cyberspace.

Cyberspace has fundamentally changed the nature of warfare as it transcends geographical borders. Cyber weapons and cyber warfare have become one of the most dangerous innovations of recent years, and a significant threat to national security. Humans across the world are completely hooked to new technologies so much so that everyday life has categorically become dependent on the virtual world. As the societies become more reliant on these technologies, they also expose themselves to the dangers lurking around in the cyberspace. From ransom ware to data breaches, election security to unemployment fraud, organizations around the world, public and private, have found themselves faced by major cyber security challenges, both new and accelerated. Cyberspace gives a chance to approach opponent targets that would otherwise be utterly unassailable, such as national defence systems and air traffic control systems. The more technologically developed a country is, the more vulnerable it becomes to virtual attacks against its infrastructure. The very nature of cyberspace makes this domain a potent force that will play a pivotal and decisive role in any future war. Thus, all the nations are worried about cyber security of their Government organisations along with cyber safety of private citizens.

Traditionally, International wars are fought between two nation-states and non- state actors wielded little or no influence on conflicts fought on land, sea and air. However, non- state actors have deeply penetrated cyberspace and wield great influence and pose greater national security risks in the cyber domain. Cyber space has allowed non- state actors to launch cyber attacks against state actors, thereby altering the way traditional wars are fought. Easy accessibility to technology, low barriers to entry in the virtual world and low economic cost of obtaining cyber weapons are key factors that have made cyberspace fertile space for non-state actors. Malicious groups including terrorist organisations have manufactured and obtained lethal cyber weapons. Considering the fact that Cyber weapons can imperil economic, political, and military systems by a single act, or by multifaceted orders of effect, with wide-ranging potential consequences; all nations are concerned about cyber threats from non- state actors. Indeed, the virtual world has thrown the spotlight on non- state actors and brought them to the center stage of the international system.

Unlike other domains of war, the laws of war are ambiguous as regards cyberspace. The development of law is said to be reactive i.e. the desire for regulation drives the law. This is especially true in case of law of wars, which is based on consensus between states. However, due to its reactive nature, law lags behind the advancements in technologies. Currently, we find ourselves, applying the twentieth century law to rapid advancements of the twenty-first century. This is not to say that the law is not applicable to the new technological advancements. In fact the development and use of the new technologies must comply with the law. However, the tensions between the international law and technology raise questions on adequacy and applicability of the law to the digital world. In the borderless virtual world traditional ideas of state sovereignty don't work very well and this new domain remains rather lawless. Under the international legal system, state responsibility is a fundamental principle that ensures that states make reparations for any breach of international law attributable to them. Attribution describes the process of assigning a particular act to its source not necessarily in the sense of its physical perpetrator but more importantly in the sense of its mastermind. To simply put forth, attribution means putting a name and a face to the perpetrator. Attribution is important because it forms the basis of appropriate and effective technical, political and legal determinations and underpins technical, political and

legal action and responsibility. However, attribution of cyber attacks remains one of the most difficult tasks because the virtual world affords and encourages anonymity. The possibility of spoofing, the multi-stage nature of cyber attacks, and the indiscriminate nature of cyber tools also hinder the assessment of risk and identification of perpetrator.

Moreover, traditionally the law of state obligation does not extend to non- state actors and henceforth; states have easily eluded responsibility for cyber attacks stimulated by non-state actors present in their territory. As a matter of fact, anonymity has enabled many states to covertly achieve nefarious goals in the cyber domain through proxy non-state actors. It has been seen that states evade responsibility by taking advantage of ambiguities in the law. Russia, for example, evaded responsibility for cyber attacks on Estonia and Georgia. While effectively responding to state-launched cyber-attacks is already a complicated task, this becomes even more difficult when states hide behind non-state actors. The state responsibility under international law is quintessential to deter breaches of international law. Attribution problem in the virtual world and ambiguity in international law on the issue have resulted in a veiled protection to states for cyber attacks launched through their territories. Arguably, immunity harbouring the cyberspace encourages state and non-state actors to kill the opponent virtually.

In this backdrop, the authors seek to examine whether the virtual attacks of non-state actors can be attributed to states under whose territory they are present.

A. What are cyber attacks?

The term attack is of primary significance in International Humanitarian Law, which governs and regulates the conduct of states during an armed conflict. The rules and standards of armed conflict are housed in the four Geneva Conventions and their two Additional Protocols. Though the original Geneva Conventions did not provide a definition for attacks, in 1977 a definition of attack was laid down in the 'Protocol I'. Article 49 states that an attack' ***is an '[act] of violence against the adversary, whether in offence or defence.***

Naturally, in 1977 the scope of violence was limited to reality of that time. Cyber attacks were beyond imagination at that time and thus, do not find inclusion in this definition. In fact, even in 1984, when William Gibson webbed the term cyberspace together, the term was used to describe a fictional space where billions of legitimate users experienced a consensual hallucination. It is however, pertinent to mention that while cyber space is a de novo arena, the term cyber is not novel. It is borrowed from the ancient Greek adjective "KUBRNETIKOS" which is synonymous in the English language with piloting, governing or skilled in steering. The term cyber is used in short for cybernetics. Nobert Weiner popularised the term cyber in 1940 to describe the then futuristic idea of a self-regulating computing system, solely running on information feedback.

In a short span of time, cyberspace and the virtual world has dominated the daily affairs of humans. For the last two decades, cyber attacks are the biggest security threats facing states. However, no international legal document has defined cyber attack or dwelled on the issue. The closest to a globally accepted definition of cyber attack is the definition housed in the Tallinn Manual, a non- binding document released by NATO Cooperative Cyber Defence Centre of Excellence. *Rule 30* of the Manual defines 'cyber attack' as '***a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects.***' It is, in other words, a cyber operation whose consequences are expected to exceed a certain threshold. This definition highlights that to qualify as a cyber attack the conduct must be active and it is irrelevant whether it is offensive or defensive in nature. Generally attackers deploy both active and passive operations. If active and passive conduct is working in tandem, together, the authors opine that they will fall within the understanding of cyber attack. However, a passive conduct in isolation should not be termed as a cyber attack to safeguard world peace.

B. Stakeholders In Cyber Space

Generally, the primary actor in the international sphere is the state. States are the principle makers and primary subjects of international law. The UN membership and the right to appear before the International Court of Justice are also reserved for states alone. State is generally understood to possess four attributes: a permanent population, a defined territory, Government and capacity to enter into relations with other states. The Montevideo Convention on Rights and Duties of States has laid down these four qualifications in Article 1. To be deemed a state the actor must possess all four qualifications. Even though the Montevideo Convention is not widely ratified, the definition of state laid therein is widely accepted and has become a customary understanding of the concept of state.

Cyberspace involves key stakeholders that include, but are by no means limited to, states. In the virtual domain Non-State Actors are dominant figures that can significantly impact global affairs as much as states do. Non-state actors in cyberspace include civilians, big Private corporates, Non Governmental Organisations, media houses, private military organisations, academic institutions, labour unions, political groups, small businesses along with criminal organisations, terrorist organizations, hackers etc. The dominance of non-state actors in cyber space is primarily because unlike the other domains of international system, cyberspace did not originate with states but with academic institutions and private actors who innovated the Internet (albeit with government support). Even today, private corporates and individuals dominate cyberspace and this domination is only bound to increase with time as any individual with access to Internet and phone/ computer can enter this global domain. In- fact cyberspace has become a commercialised domain; where private corporates like Microsoft are serving as platforms for majority of cyber conduct. Even in cyberspace norm making, non- state actors are taking the initiative. For instance, in 2019, Microsoft published a report "Protecting People in Cyberspace: The Vital Role of the United Nations".Likewise, Microsoft alongside governments of Netherlands and France funded the Global Commission on the Stability of Cyberspace to examine and analyze the stability of Cyberspace.

Factually, states are lagging behind the non- state actors in supporting governance of cyberspace in the international framework. This is primarily because states are not willing to sacrifice the freedom that cyberspace presently offers them. Also, in absence of international framework on cyber attacks, states are easily escaping responsibility for executed attacks. To safeguard their freedom and escape accountability, nations have remained mute spectators to the demand for internationally legally binding law on cyberspace.

C. Non-state Actors, Cyber Attacks And International Law
A) Non State Actors And Cyber Attacks

Traditionally, wars were only fought between states and states alone possessed the power, funds, weaponry and armies that could cause large-scale harm to another country. Inter-state conflict between a state and a non-state actor was beyond imagination for mankind. **The term 'non-state actor' (NSA) covers a wide range of diversified entities** with one particular trait in common – **while often playing a significant role in international relations, they are independent of states.** This broad term covers, *inter alia*, individuals, corporations, non-governmental organizations,

armed non-state actors, de facto regimes, trade associations, and many more. The advance of technology has turned the unimaginable into reality and capabilities that once only states possessed have become available to non-state actors in the dark virtual space. In- fact, the US secret Service has observed that currently many non-state actors have capabilities that far exceed that of nation-states. Many of the recent conflicts have been characterised by cyber attacks from non-state actors. The most recent war between Russia and Ukraine witnessed cyber offensives launched by non-state actors. In 2007, Cyber attacks on Estonia and in 2008 cyber attacks on Georgia involved participation of non-state actors. However, even in peacetime, states are continuously facing cyber attacks from non-state actors that are either economically or politically motivated. Cyber attacks ranging from denying access to the basic services to cyber espionage operations resulting to data thefts are being launched on regular basis. Most of these attacks are aimed at stealing sensitive information or to cripple critical infrastructure. For instance, All India Institute of Medical Sciences was attacked causing disruption in online services and 1.3 tetra-bytes of data was stolen. Likewise, the servers of National Health System of United Kingdom were brought down by cyber attacks. Literally, everyday there is a cyber offensive from a non-state actor and with each passing day these cyber attacks are becoming more sophisticated. In 2022, attacks on state agencies were up by 95% globally and 45% of these attacks were on India, US, Indonesia and China. According to IBM's **'Cost of Data Breach Report 2022'**, the average cost of data breaches in the government sector has increased from $1.93 million in 2021 to $2.07 million this year. The asymmetric nature of cyber attacks coupled with problem of attribution and low economic cost of cyber weapons are the primary reasons for this increase.

Factually, majority of the attacks from non-state actors have been carried out at the behest of state actors. States have found allies in Cyber proxies or cyber mercenaries. Some CNSA are therefore unofficial emanation of the States where most of their components are located and act as 'corsairs' for their country, often conducting activities aimed at: a) extorting and stealing money; b) attacking enemy countries institutions and infrastructures; c) cyber- espionage. In fact, several states tolerate or even protect CSNA in order to: a) create the conditions for development and prosperity of as many cyber- operators with hacking capabilities as possible and to be able to get access to information and intelligence of different kind. Hiring cyber proxies or mercenaries clothes the states behind cyber attack with an invisible cloak i.e. if a cyber attack is traced to their territory, states effectively deny knowledge of it and hide behind nameless agents. This makes it extremely difficult for the victim state to take countermeasures. For instance, it is a widely known fact that Russia was behind cyber attacks on Ukraine, Estonia and Georgia but Russia claimed that private actors who merely happen to reside in its territory made these attacks. The ever increasing cyber attacks from non state actors raise a critical question that whether states should be held responsible for attacks of non-state actors launching attacks or should non state actors be treated as subjects of laws of war and be held liable for unlawful conduct?

B) International Law, Non State Actors And Attribution

The conventional paradigms of International Law and International relations take a state- centric view. Traditionally, states alone are considered to be the subjects of international law. It was believed that it is only possible for international law to govern the states. As subjects of international law, states are bound to obey the law and bear responsibility in case of violations. States includes the government, its organs as well as those acting on behalf of the Government. If a state violates law, certain consequences follow; the responsible state shall be under a duty to cease the harmful conduct and also make reparations for any damage or injury caused by its conduct. However, to hold a state responsible for violation of international law it must be shown that the breach is attributable to the state. International law has, however, ignored the presence of Non- state actors. International law does not recognise the legal personality of non-state actors; it is difficult underline whether this is purposive or inadvertent. Since non-state actors are not subjects of international law, they can commit no wrong under it and as such cannot be held responsible for breaches of international law. This gives rise to the question whether breach of international law by non-state actors can be imputable to states?

c) Non State actors and International law on Attribution

International law stands clear that violations by non-state actors can be imputed to a state provided that the conduct is attributable to the state. So attribution is quintessential to hold a state accountable for breaches committed by non-state actors. In this context, attribution is the key to determine whether the act of a private actor constitutes the act of a state. The rules of attribution are essential to determine state responsibility. Attribution process that distinguishes conduct of private actors from state actors has long been a concern for international courts and tribunals. The international courts, jurists and scholars have diverse opinions on the issue.

In the Nicaragua case, the International Court of Justice laid down the effective control test. It held that as a general rule states cannot be held liable for acts of non-state actors, except for when the effective control test is satisfied i.e. when it can shown that a state has effective control over the non-state group breaching international law, the state can be held liable for the violation of international law. In this case the ICJ held that conduct of Nicaraguan rebels could not be imputed to the United States as the military and Para military operations of the rebels were neither controlled nor directed by the US. This judgment is criticised because the Court refused to hold US responsible even though the rebels had received finances, supplies and training from the US. The facts of the case reveal that 'Effective control test' is rigid and water tight in nature, which easily allows states and malicious non-state actors to evade responsibility.

In the Tadic case the Tribunal held that in order to attribute conduct of a non-state actor to a state, it is essential for a state to have direct control over the non-state actor but it is not essential that the conduct in question was directed or controlled by the state. So the ICTY drifted from the Nicaragua case mandate that a state must have directed the harmful conduct of non-state actor. The test devised by ICTY is called 'overall control test'. The threshold of overall control is reached even if a state merely exerts general influence on non-state group. The ICTY deduced the test based on detailed study of state practice and jurisprudence.

The ICJ in the Bosnia Genocide case rejected the overall control test laid down by ICTY on grounds that it was neither persuasive nor needed to determine criminal responsibility. In this case the Court used the 'effective control test' to determine if acts of genocide of the Bosnian Serb armed groups could be attributable to Yugoslavia. The Court held that acts of genocide could not be attributable to Yugoslavia as neither were the armed groups dependent on it nor were they acting on its instructions.

In 2012, the International Criminal Court affirmed that the overall control test was the correct test to determine whether an act of non-state actors can be attributable to a state.

d) Problem Of Attribution In Cyber Attacks

Attribution, in context of cyber attacks signifies allocation of responsibility to an attacker and unveiling their true identity. Cyber attribution entails two aspects - technical and legal. Technical attribution of a cyber-attack requires engagements with forensic evidence of the attack. This concerns the study of

the software used for cyber attack, investigation of the type of targets and means of intrusion used alongside identification of the system used. Cyberspace is a borderless domain unlike other domains of war. This makes technical attribution particularly challenging. Additionally, Cyberspace was designed to promote anonymity, which makes identification of the source of attack complex. Perpetrators use various techniques like spoofing to obscure their true location, and isolating the origin of a cyber attack is extraordinarily difficult when attacks are routed through multiple machines in multiple locations across the world. These techniques make the task of retrospectively establishing a forensic link between an attacker and an incident extremely difficult. The more elaborate the attack, the harder it is to attribute. Even perfect technical attribution, however, will only go as far as identifying the individual or group behind the attack. While constant advancements are being made to enhance technical attribution, the spoofing techniques used by attackers to weaken attribution are advancing at an equal pace if not faster.

In context of international law, cyber attribution determines who is responsible for the attack. In order to establish legal attribution, it becomes essential to investigate the resources invested in the attack alongside testing whether the attacks were made under the influence, control or backing of another state? The legal tests of attribution, as discussed in detail in the previous part, focus on the level of control a state exerts over the non-state actor. Rule 17 of the Tallinn Manual headed 'Attribution of cyber operations by non-State actors' also emphasises on control. It reads as-'Cyber operations conducted by a non-State actor are attributable to a State when:(a) engaged in pursuant to its instructions or under its direction or control; or (b) the State acknowledges and adopts the operations as its own.' In context of cyber attacks, the traveux-repositories of the Tallinn Manual reveal that there was a consensus amongst the experts that the **'overall control'** test is the key to determine whether a cyber-attack by a private actor can be attributable to a state actor. The researchers argue that in case of cyber attacks it becomes irrelevant as to which test is applied, primarily because attribution is a complex and establishing degree of control of a state over the non state actor becomes nearly impossible. Additionally, the overall control test was laid down in context of military and paramilitary units. In case of cyber attacks, the attackers are rarely organized entities. In most cases, attackers are individuals who possess cyber expertise and are motivated to carry out attacks for thrill or under control of other states. Even when attackers are acting under control of a state, it is challenging to give persuasive evidence and establish the link between the attacker and the state.

Considering the challenges thrown by cyber attribution, some scholars recommend the application of due diligence principle to hold states responsible for malicious cyber activities originating in their jurisdictions. The principle of due diligence is not de novo. Its incorporation in international law can be traced to the *Island of Palmas* arbitral award. It evolved as a primary rule of international law in the *Corfu Channel* case. Due diligence is enlisted as a substantive duty by The Tallinn Manual 2.0 on the International Law Applicable to Cyber Warfare. Rule 6 reads as "State must exercise due diligence in not allowing its territory, or territory or cyber infrastructure under its governmental control, to be used for cyber operations that affect the rights of, and produce serious adverse consequences for, other States." Once the due diligence obligation is used to establish responsibility, it must be proven that the cyber attack and the adverse effects of it were in the knowledge, actual or constructive, of the territorial state from whose jurisdiction it originates. Additionally, it needs to be proven that the territorial state could but did not take possible measures to prevent it. The obligation of due diligence is largely based on expectation of best conduct from states and there are no explicit standards of adherence. Due to this, it is a crippled obligation and arguably, applying it in cyber context would lead to immunity instead of accountability.

In this situation, the authors insist on the need of a global policy on attribution and state accountability for cyber attacks.

There is an urgent need for states to step up and draft an international legal instrument to deal with challenges posed to international security by non-state actors. There is an urgent need for an international legal instrument to specifically lay down the rights and obligations of non-state actors along with a detailed convention on cyber attacks. The United Nations must achieve the same degree of normative strength concerning non-State use of force as it has concerning State use of force. The failure to do so will surely undermine the relevance of international law as a means for both facilitating and regulating the exercise of international power in the 21st century.

e) Self Defense, Non State Actors And Cyber Attacks

Despite the fact that non-state actors do not have obligations and liabilities under international law, the 9/11 attacks have stirred a debate on whether the states can exercise the right to self-defence in case of attacks by non-state actors. Article 51 of the UN Charter acknowledges the inherent right of self-defence in case of an armed attack against a member of the UN. Technically, non-State actors cannot carry out an armed attack within the meaning of article 51, unless their actions are attributable to a State. The language of the Article is, however, not explicit in this regard as it does not specify that the attacker must be a state. The war against terror has prompted states to exercise the right against non-state actors, even though the attack was not attributable to the state in whose territory such a non- state actor is situated. The ICJ in diverse judgments has, however, elucidated that the right of self-defense is limited against non-state actors and can only be exercised if acts are attributable to the state. Judge Kooijmanas in his separate opinion on the Armed Activities in the Territory of Congo case rightly supported the right of states to self-defense against attacks by non-state actors. To quote, "It would be unreasonable to deny the attacked state the right to self defense merely because there is no state attacker, and the Charter does not require so." Some states like U.S. and Israel, have gone too far ahead and claimed a pre-emptive right to self-defense against non-state actors. The ICJ has escaped specifically dealing with the issue of anticipatory right to self-defense on two occasions. In the Nicaragua case and the Congo case the ICJ refused to dwell on the issue. Arguably, a pre-emptory right against non-state actors it would set a dangerous precedent and should be opposed to safeguard mankind.

Even though the law is not explicit as regards right to self defense against non-state actors, the authors opine that the state practice in the aftermath of terrorist attacks of 9/11 point that in the near future right to self defense even in case of armed attack by non state actors will certainly acquire the status of customary law. Nonetheless, it is critical to ask, 'How should the right be interpreted in the age of over-the-horizon weaponry, computer network attack and asymmetric threats when warning times are reduced virtually to zero and enemies can strike almost anywhere?' While the right to self-defence against non-state actors is available, do cyber attacks qualify the threshold of armed attacks remains unanswered. Since cyber attacks are non-kinetic nature and do not necessarily cause physical harm it is difficult to fit them in the traditional compartment of armed attack. Moreover in case of cyber attacks, attribution is particularly challenging as cyberspace is borderless in nature and harbours anonymity. As a result of vacuum in international law malicious non-state actors in cyber space easily evade responsibility for cyber attacks. It is particularly problematic, when states use proxies

and mercenaries to attack another state, and the excuse of non-state actors to evade accountability.

D. Summary

It is only in the 21st century that non-state actors have emerged as mighty forces that can trigger international conflicts, endanger international peace and security. In spite of the penetration of non-state actors as global players, international law continues to turn a blind eye to them. There is a vacuum in the law of attribution as it neglects the violations of international law by non-state actors. An unwritten regime of immunity dominates the world affairs due to this ignorance. The states are taking advantage of this and forging alliances with non-state actors. Hiding behind the veil of non-state actors states are making breaches of the law to serve their own interests. Attribution is essential to usher in a regime of accountability in international law. The authors, therefore, strongly recommends that a detailed law of attribution should be drafted, that takes into account non-state actors as violators of international law. There is an urgent need for states to step up and draft an international legal instrument to deal with challenges posed to international security by non-state actors. Even though the future of attributing cyber acts appears uncertain, there is hope that someday, somehow the real identity of the online villains will be uncovered and they will be brought to justice.

REFERENCES

1. Brian Mazanec, "The Evolution of Cyber War: International Norms for Emerging Technology Weapons" 141 (Potomac Books, University of Nebraska Press,2015)
2. The Week Staff, "Why World War III will be fought on the Internet" The Week. 8 june 2015, available at https://theweek.com/articles/441194/why-world-war-iii-fought-internet
3. Ignatius Demetris, "Will deterrence have a role in the cyberspace 'forever war'?" Washington Post. 16 Septemeber 2022, available at https://www.washingtonpost.com/opinions/2022/09/15/deterrence-cyberspace-conflict-new-strategy/
4. Cybergymexperts, "Cyberspace – the battle ground for world war 3?" available at https://www.cybergym.com/cyberspace/
5. Weismann, G (2004). Cyber Non -State Actors : The Cyber Taliban. Special Report of United
6. States Institute of Peace. 2-4. Retrieved from https://usiofindia.org/publication/usi-journal/cyber-
7. non-state-actors-the-cyber-taliban/
8. James Shires , "The Word Cyber Now Means Everything—and Nothing At All." Slate Magazine, 1 December 2017, available at https://slate.com/technology/2017/12/the-word-cyber-has-lost-all-meaning.html
9. Eric Talbot Jensen, "The Future of the Law of Armed Conflict: Ostriches, Butterflies, and Nanobots" 31(2). Michigan Journal of International Law 253 2014.
10. Colarik and Janczewski, "Establishing Cyber Warfare Doctrine" 5(1) Journal of Strategic Security 31-48 2012.
11. Supra note 3.
12. Nicolo Bussolati, "Cyberwar Law and Ethics for Virtual Conflicts" 102-105 (Oxford University Press, Oxford, 2015)
13. David Clark and Susan Landau, "Untangling Attribution." 2 Harvard National Security Journal. 324-344
14. William Banks, "Cyber Attribution and State Responsibility"9 International Studies 1040-1045 2021.
15. Emrah Tanyildizi, " State responsibility in cyberspace: the problem of attribution of cyberattacks conducted by non-state actors" 8(14). Law & Justice Review 119-176 2017.
16. Matthew C.Waxman, "Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)" 36YALE JOURNAL OF INTERNATIONAL LAW 421 (2011).
17. supra
18. Paul Szoldra, "The next world war is going to be fuellled by state-sponsored hacking" Business Insider. (16 August 2016) available at https://www.businessinsider.in/tech/the-next-world-war-is-going-to-be-fueled-by-state-sponsored-hacking/articleshow/53715799.cms
19. Additional Protocol I to the Geneva Convention of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, 1125 UNTS 3, June 8, 1977, Art 49.
20. Michael Schmitt, "Tallinn manual 2.0 on the International law applicable to cyber operations" (Cambridge University Press, New York, 2017) 564.
21. Jeffrey L Dunoff, Steven R Ratner and David Wippman, "International Law: Norms, Actors, Process: A Problem-Oriented Approach" (Aspen, 2002) 105.
22. Montevideo Convention on Rights and Duties of States, opened for signature 26 December 1933, 165 LNTS 19 (entered into force 26 December 1934).
23. '[t]he State ... should possess the following qualifications: (a) a permanent population; (b) a defined territory; (c) government; and (d) capacity to enter into relations with the other States'.
24. Microsoft, "Protecting People in Cyberspace: The Vital Role of the United Nations in 2020" 2019 Available at: https://www.un.org/disarmament/wp-content/uploads/2019/12/protecting-people-in-cyberspace-december-2019.pdf.
25. Global Commission on the Stability of Cyberspace, "Advancing Cyberstability: Final Report" 2019 Available at: https://cyberstability.org/wp-content/uploads/2019/11/Digital- GCSC-Final-Report-Nov-2019_LowRes.pdf.
26. Anahit Parzyan, "Cyberspace- A man made domain of wars" 21st CENTURY, No 1 (20), 2017. 48. < https://www.academia.edu/35526590/CYBERSPACE_A_MANMADE_DOMAIN_FOR_WARS>
27. Todd Lopez, ' DOD: Its not just state actors who pose cyber threat to US' DOD News, May 2022. < https://www.defense.gov/News/News-Stories/Article/Article/3039462/dod-its-not-just-state-actors-who-pose-cyber-threat-to-us/>
28. Tim Maurer, "Cyber Mercenaries: The State, Hackers, and Power" (Cambridge: Cambridge University Press: 2018), x.
29. Kevin Townsend, "Cybersecurity Geopolitical Insights" Security Week, 1 Feb 2023. Available at < https://www.securityweek.com/cyber-insights-2023-the-geopolitical-effect/>
30. Ahaskar Abhijit, " India saw the highest rise in cyber attacks on Government Agencies" The Mint , 30 December 2022 available at < https://www.livemint.com/technology/tech-news/india-saw-the-highest-number-of-cyberattacks-on-govt-agencies-in-2022-report-11672389099189.html>
31. Scott Shacklford, "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law". 27 Berkeley Journal of International Law 193-195 (2009)
32. Pierluigi Panini, 'Non state actors in cyberspace: an attempt to a taxonomic classification, role, impact and relations with a state's socio- economic structure' Center for Cyber Security and International Relations, June 2022, 28. Accessed online at < https://www.cssii.unifi.it/upload/sub/Pubblicazioni/2022_Paganini_Pierluigi.pdf>
33. supra at 12
34. Fokus Demetrius, "Cyberspace Warfare Attacks & Non State Actors" 28 Available at < https://www.academia.edu/27561649/Cyberspace_Warfare_Attacks_and_Non_State_Actors>
35. Jenny Maddocks, "Ukranian Symposium: State responsibility for Non State actors conduct" Articles of war Available at < https://lieber.westpoint.edu/state-responsibility-non-state-actors-conduct/>
36. Cedric Ryngaert, "Non-State Actors: Carving Out a Space in a State-Centred International Legal System" 63 Netherlands International Law Review 183-195 (2016).
37. Milan Plucken and Joern Griebel, "New Developments Regarding the Rules of Attribution? The International Court of Justice's Decision in Bosnia v. Serbia" 21 Leiden Journal of International Law, 601-622 (2008).
38. James Crawford, "First report on state responsibility" 2(1) Yearbook of international law, 154 1998.
39. Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Merits, Judgment, I. C. J. reports 1986, 14, para 54 – 55.
40. Supra para 109-115.
41. Supra Para 131.
42. ICJ Case concerning application of the convention on the prevention and punishment of the crime of genocide (Bosnia and Herzegovina v. Serbia and Montenegro) 402-406 26 Feb. 2007
43. Supra para 393, 394, 413.
44. Prosecutor v. Lubanga, Trial Chamber Judgment, 2012, para 541
45. Lorraine Finlay & Christian Payne, " The attribution problem and cyber armed attacks" American Journal of International Law 113,204 2019 available online at https://researchonline.nd.edu.au/cgi/viewcontent.cgi?article=1089&context=law_article
46. Clara Asumcao, "The problem of cyber attribution between states" E International relations 6 May 2020. Available at https://www.e-ir.info/2020/05/06/the-problem-of-cyber-attribution-between-states/
47. supra
48. supra note at 18.
49. Note2, Commentary to Rule 22 Tallinn Manual 79 Available at https://doi.org/10.1017/9781316822524.010.
50. Florian Egloff, "Public Attribution of Cyber Intrusions" 6(1) Journal of Cybersecurity 2020 available at https://academic.oup.com/cybersecurity/article/6/1/tyaa012/5905454.
51. UN Group of Governmental Experts, "Report on Advancing Responsible State Behavior in Cyberspace in the Context of International Security" UNGA A/76/50.71(g) Available at https://dig.watch/wp-content/uploads/2022/08/UN-GGE-Report-2021.pdf
52. Antonio Coco and Talita de Souza Dias, "Cyber Due Diligence: A Patchwork of Protective Obligations in International Law" 32(3) European Journal of International Law, Pages 771–806, 2021. Available at https://doi.org/10.1093/ejil/chab056
53. The Corfu Channel Case (United Kingdom v. Albania), 1949 ICJ Merits, ICJ Report.
54. McDonald, 'The Role of Due Diligence in International Law', 68 International and Comparative Quarterly 1043–1044 2019.
55. Okwori Enenu, "The Obligation of Due Diligence and Cyber-Attacks: Bridging the Gap Between Universal and Differential Approaches for States" 2019.
56. Thomas Franck, "Preemption, prevention and anticipatory self-defense: New law regarding recourse to force?" 27 Hastings International and Comparative Law Review 425 2004.
57. Fergus Green, "Fragmentation in Two Dimensions: The ICJ's Flawed Approach to Non-State Actors and International Legal Personality" 9 Melbourne Journal of International Law 47-54 2008.
58. Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, ICJ 2004 para39
59. Judge Koojimans, Separate Opinion, Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda), Judgment, (2005)ICJ, para 29 &30.
60. U.S. Department of State, 'The National Security Strategy of United State of America' 2002, 15. Accessed online at <http;//www.state.gov/documents/organisation/63562.pdf>; The United States of America had been a overt advocate of the preventive right under the Bush Doctrine. In 2016, even US superficially made amends and affirmed the requirement of armed attack before exercising the right.
61. Supra 37, (merits) para 194.
62. Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda), Judgment, (2005) ICJ, para 143.
63. Abdul Ghafur Hamid, "the legality of anticipatory self-defence in the 21st

century world order: a re-appraisal", 54 Netherlands International Law Review 441–490 (2007).
64. Donald Rotthwell, "Anticipatory Self-Defence in the Age of International Terrorism Special Edition:The United Nations and International Legal Order" 24(2) University of Queensland Law Journal (2005) 337 available at http://classic.austlii.edu.au/au/journals/UQLawJl/2005/23.html
65. Dimitar Kostidanov, "The attribution problem in cyber attacks" Infosec 1 February 2013. Available at https://resources.infosecinstitute.com/topic/attribution-problem-in-cyber-attacks/