CYBERATTACKS BY NON-STATE ACTORS AND CHALLENGES IN STATE ATTRIBUTABILITY

Shreya Menon, ILS Law College, Pune

ABSTRACT

This essay addresses the challenges that arise regarding attributability towards a state for the actions of non-state actor in the cyberspace. With the surge in the cyberattacks both in the national and international levels, it becomes more than necessary for the need of an international legal framework. Existing attribution rules, such as Article 8 of the Articles on Responsibility of States for Internationally Wrongful Acts, the Effective Control test put forward by the Nicaragua case and the Overall Control test put forward by the Tadic case have established an extremely high threshold of proof which is almost impossible to be proven in the cyberspace context. Since these standards were developed for kinetic warfare, it is almost impractical to apply to the cyberspace as the evidentiary requirements and method of action is extremely different for both the scenarios. To establish these aspects, the essay evaluates major cyberattacks that took place against Estonia (2007), Georgia (2008), and Albania (2022). Through this analysis, it can be established that the two tests, especially the Effective Control test, are inadequate tests for attribution in the cyberspace. This paper argues for a revised system for attribution. It suggests for adopting a more relaxed standard, establishing a specialized agency, using multi-factor tests, or applying due diligence principle. Without a strong attribution standard, the state actors responsible will continue to evade responsibility by hiding behind the cloak of legal formalism.

Keywords: Cyberattack, non-state actors, Attributability, Overall Control test, Effective Control test

I. INTRODUCTION

Interstate cyberattack is considered as a new feature of modern-day warfare. Though there is no single internationally accepted definition for what constitutes a cyberattack, one of the narrow and basic definitions of cyberattack would be - any action which "undermines the functions of a computer network for a political or national security purpose".[1] Interstate cyberattack is fairly a new topic of discussion in international law. This is evident from the fact that only recently has the international community woken up to adopt new policies and attempted to create universal legal framework which is inclusive of the cyber space. In a recently published study by the United Nations Institute for Disarmament Research, it was stated that internet is becoming central to business, politics, espionage, and military activities, hence cybersecurity becomes a core question of national and international security. It was also found that 33 states included cyberwarfare in military planning and organization.[2]

The first attempt at bringing interstate cyberattacks under the ambit of legal scrutiny was the Tallin Manual of 2013 by a group of international experts. This was followed up by an expanded version, Tallin Manual 2.0 in 2017[3].

In this current environment of low legal guidelines for ringfencing malevolent cyberattacks by apparently non-state actors, attribution of the same to the respective states becomes a challenge. (In this document, the word 'attribution' shall mean attribution of cyberattacks to the actual perpetrator of such attacks). In recent times, cyberattacks have brought to light several loopholes in international law. It is considered that "attribution of a cyber-attack to a state is a, if not *the,* key element in building a functioning regime"[4] (a functioning regime being governance norms for cyberattacks). Attribution describes the process of assigning an act to its source, but it does not necessarily mean its physical sources, like a computer or the person who operated the computer. Instead, it is to identify the 'mastermind' behind it and then establish

[1] Oona A. Hathaway, Rebecca Crootof, Philip Levitz & Haley Nix, The Law of Cyber-Attack, 100 Calif. L. Rev. 817 (2012), https://openyls.law.yale.edu/server/api/core/bitstreams/a060f74f-2469-4435-bada-cebc181ea9c4/content

[2] Center for Strategic and International Studies, Cybersecurity and Cyberwarfare – Preliminary Assessment of National Doctrine and Organization, UNIDIR Resources Paper (2011), https://unidir.org/files/publication/pdfs/cybersecurity-and-cyberwarfare-preliminary-assessment-of-national-doctrine-and-organization-380.pdf

[3] Michael N. Schmitt (ed.), Tallinn Manual on the International Law Applicable to Cyber Warfare (2013).

[4] Scott J. Shackelford, From Nuclear War to Net War: Analogizing Cyber Attacks in International Law, Berkeley Journal of International Law, Vol. 25, No. 3, 2009, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1396375

his/her link with the state.[5] Various issues like anonymity of the individuals conducting the operations, the fact that a single attack can come from different jurisdictions done from different places, the speed with which a particular operation takes place[6] and many more complicate the attributability in cyberspace. Certainty is, more often than not, elusive. However, these faint digital fingerprints lay the seeds for a certain degree of doubt. Though there cannot be certainty through technology, the law does not require absolute certainty, instead has a threshold only of "reasonable degree of certainty". [7] However, in the absence of an internationally recognized code for the recognition and treatment of such cyberattacks, states will continue not only with disproportionate responses but also with vehement justification of the same on the international stage.

First, this essay will analyse the existing legal framework for attribution under the international law and its application to the cyber operations. Second, it will examine case studies of major NSA cyberattacks and compare similarities and differences in terms of attribution. And third, it will discuss possible reforms.

II. AVAILABLE LEGAL FRAMEWORK FOR ATTRIBUTION

A. Article 8 of Articles on Responsibility of States for Internationally Wrongful Acts (ARSIWA) of the International Law Commission (ILC), United Nations

In ARSIWA, articles 4-11 talk about various ways in which an action can be attributed to the state. The article that is relevant for this document and the one that deals with actions of non-state actors is Article 8. It states that the conduct of a person or group of persons will be attributable to the state if such an act is done on the instructions, directions or control of the state.[8] The commentary of this article begins by saying that the conduct of private persons or entities are generally considered not attributable to the state, under the international law. But it can be attributable if "there exists a specific factual relationship between the private person or entity engaging in the conduct of the state."[9] The commentary also explains how Article 8

[5]British Institute of International and Comparative Law, State Responsibility for Cyber Operations: International Law Issues Event Report (2014), https://www.biicl.org/documents/380_biicl_report_-_state_responsibility_for_cyber_operations_-_9_october_2014.pdf

[6] *Id.*

[7] Delbert Tran, The Law of Attribution: Rules for Attributing the Source of a Cyber-Attack, 20 YALE J. L. & TECH. 376 (2018), https://yjolt.org/law-attribution-rules-attributing-source-cyber-attack

[8] International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, Supplement No. 10 (A/56/10), chp.IV.E.1, November 2001.

[9] International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts,

works in practice. A state can be held responsible for the actions of a private group/ individual if it gives specific instructions *and* directs their activities, *and* exercises control over them. These three conditions are disjunctive, which means that it does require all the three aforementioned actions for state attribution. It is also clarified that the link must be specific in nature. The state's involvement must be related to the particular wrongful act, example, an attack, detention, or killing and it cannot be vague and have some general influence. [10] But it has also been mentioned that case by case analysis must be done in order to determine control of the state of the non-state actor and hence attributability[11]. This provides flexibility in the determination of attribution.

One of the strongest criticisms that has arisen towards article 8 is the requirement of the state *instructing, directing and controlling the specific conduct* in order for attribution is extremely vague and restrictive in nature. In practice, states are held responsible even if they have a general or overall control over a group. The "specific conduct" requirement does not reflect the state practice.[12]

B. Nicaragua Effective Control Test

In the case of *Military and Paramilitary Activities in and against Nicaragua[13] (Nicaragua vs United States of America),* which dealt with the support provided by the USA to the Contras (the faction that was fighting against the Government of Nicaragua), the primary question was whether the conduct of the Contras was attributable to the United States. The judgement of the International Court of Justice (ICJ) regarding this issue is two layered.

Firstly, it found U.S. to definitely be responsible for its own role in planning, directing, and supporting operations, which violated the international law[14], which means the USA Violated the rule against intervening in another state's internal affairs and the rule against the use of force under customary law

But secondly, the court denied the claim that all contra acts can be attributed to the US merely

with Commentaries, November 2001
[10] *Id*. 7
[11] *Id*. 5
[12] Antonio Cassese, The Nicaragua and Tadić Tests Revisited in Light of the ICJ Judgment on Genocide in Bosnia *(2007),* https://www.ejil.org/pdfs/18/4/233.pdf
[13] Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), I.C.J. 14 (1986)
[14] *supra* note 9, at Art. 8 para. 4

because of its strong support and influence. [15]

The ratio decidendi of the court regarding this decision is that though there is proof of strong support and influence, there is not enough proof to show that the USA legally controlled 'every act' of the Contras, i.e. the USA did not have *effective control* over the actions of the contras.

This effective control test has been criticized for not citing state practice, or opinio juris and didn't refer to case law or general principles of international law.[16] This gives the effect that the ICJ simply created the test without having a clear legal foundation.

C. TADIC Overall Control Test

This was a test put in place by the International Criminal Tribunal for the former Yugoslavia Appeals Chamber - to evaluate the relationship between the Bosnian Serb Army and the Government of Yugoslavia (Federal Republic of Yugoslavia). Here again, the question was how and why the actions of the Bosnian Serb Army could be attributed to the Federal Republic of Yugoslavia (FRY). In order to decide this, the Tribunal had to see if Bosnian Serb units were acting on behalf of the FRY. If so, the groups' act would count as Serbia's, turning the conflict into an international one. [17] The Tribunal held that in order to treat the conflict as international, Yugoslavia needed to have "overall control" over the Bosnian Serb forces. This was a departure to a certain extent from the Nicaragua Effective Control Test because the Tadic Overall Control Test stipulated only an overall control by the state player on the insurgent group and not specific action-by-action control.

The ICTY clarified that, although Nicaragua test deals with State responsibility and not individual criminal liability, the issue is when acts of individuals can be legally attributed to the state. The court further distinguished two situations: First, when private individuals act for state and second, when an organized group acts for a state. In the first case, specific instructions are required to be provided for each act and thus the test of effective control must be applied. In the second case, involving organized armed group or military units, overall control of the state is sufficient to show attributability, and there is no requirement of specific instructions to be provided. Overall control includes equipping, financing, or training the group, as well as,

[15] *Id.*
[16] Cassese, *supra* note 12.
[17] Prosecutor v. Tadić, IT-94-1-A, (ICTY App. Ch., July 15, 1999).

providing operational support, coordinating or assisting in the general planning of the group activities. The Appeals Chamber argued that a flexible approach must be taken.[18]

In both these tests (Effective and Overall Control), the act of attribution of involvement on state actors is at best cloudy. However, given the obscurant nature of international politics with myriad interest, both individual and collective, the clear establishment of state involvement still remains, to a large extent, minimally protected by transnational law. While the presence of laws, for attribution in the case of even physical insurgency, is thus at best ghostly, it is not difficult to imagine the plight of attributing state involvement to cyberspace interventions.

III. APPLICATION TO CYBERSPACE

A. Application of International Humanitarian Law to the Cyberspace

The debate regarding the applicability of international law to the cyberspace is an ongoing one. But it has been established by many reliable sources that just like the application of international law to traditional means of warfare, it can also be applicable to cyberattacks as well. Tallinn Manual on the international law Applicable to Cyber Warfare[19] and the Tallinn Manual 2.0 on the international Law Applicable to Cyber Operations[20] are highly authoritative works in the field of cyberspace. Rule 20[21] of the manual mentions that in situations where the express rules of the law of armed conflict do not explicitly address cyber operations, the Martens Clause applies (which is also found in the 1949 Geneva Conventions[22] and its Additional Protocol I[23]). It has been opined by the International Court of Justice (1996) in an opinion concerning the legality of threat or use of nuclear force, as well as reiterated by the International Committee of the Red Cross (ICRC) that the international humanitarian law applies to *all* forms of warfare and to *all* kind of weapons and which automatically includes cyber operations[24] (emphasis added). It was also agreed by the states at the UN Group of

[18] *Supra* note 12.
[19] Michael N. Schmitt (ed.), Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge University Press, 2013.
[20] Michael N. Schmitt, Tallinn Manual 2.0 On the International Law Applicable to Cyber Operations, Cambridge University Press
[21] *Id.* Rule 20
[22] Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (First Geneva Convention), Aug. 12, 1949, 75 U.N.T.S. 31.
[23] Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), June 8, 1977.
[24] Yola Verbruggen, Cyberattacks as War Crimes, International Bar Association (IBA) (10 January 2024), https://www.ibanet.org/Cyberattacks-as-war-crimes.

Governmental Experts in 2013[25] and 2015[26] that international law, including sovereignty and non-intervention principles, applies to state activities in cyberspace as it does in the physical context. Thus, it can be concluded that International Humanitarian Law (IHL) is applicable to the cyberspace as well.

B. Issue Regarding Attribution

Now that it has been established that IHL is applicable to the cyberspace, we will now analyse the practical issues that arise in its applicability. Judge Al-Khasewneh in his dissenting opinion[27] mentioned that "the inherent danger in such an approach is that it gives States the opportunity to carry out criminal policies through non-state surrogates without incurring direct responsibility." This opinion was regarding the applicability of the attribution test to the traditional armed attack by non-state actors to the state. It is considered almost "impossible" to apply this test to the cyberspace.[28]

By close examination of past practices, it can be found out that loosely the actions of organized military groups are attributed to state players through the overall control test, while the actions of individual or non-military organizations are attributed to states through the effective control test. This can be seen in cases such *as Kenneth P. Yeager*[29]*, Loizidou*[30]*,* and *Cyprus v Turkey*[31] and is supported by UN bodies.[32]

The Permanent Court of International Justice in the Lotus Case emphasized that a precedent must have "close analogy" to the case under consideration.[33] The effective control test requires proof that the state directed and enforced specific operations of a non-state group. But applying this to the context of cyberattacks will be similar to comparing "Lemons" and "Tangerines"

[25] UNGA, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc A/68/98, para 20 (2013).
[26] UNGA, Report of the Group of Government Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/70/174, ¶ 27 (2015).
[27]Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro), Judgment, I.C.J. Reports 2007, Dissenting Opinion of Vice-President Al-Khasawneh.
[28] Jakub Vostoupal, Stuxnet vs WannaCry and Albania: Cyber-Attribution on Trial (2024), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4729496
[29] Kenneth P. Yeager v. The Islamic Republic of Iran, IUSCT Case No. 10199.
[30] Loizidou v. Turkey, App. No. 15318/89, 1995 Eur. Ct. H.R. (1995).
[31] Cyprus v. Turkey, App. No. 25781/94, ¶ 77 (Eur. Ct. H.R. 2001).
[32] Report of the Working Group on Arbitrary Detention 2000, A/CN.4/2000/4, at para. 15 https://www.un.org/unispal/document/auto-insert-188635/, Situation of Human Rights in East Timor, Report of the UN Secretary- General, 10 Dec. 1999, UN doc A/54/660, at para. 59.
[33] S.S. Lotus (Fr. v. Turk.) 18 (1927).

into a single category.[34]

Application of effective control becomes impossible as it is extremely hard to prove evidence and control. Attribution in cyberspace mainly includes three steps[35]. Firstly, linking the attack to a machine, secondly, linking machine to a perpetrator and thirdly, linking perpetrator to a state. Each step is extremely complex and uncertain and very different from the traditional armed attack. However, what emerges from these discussions is that the Overall Control Test is the best available refuge in the case of cyberattacks.

IV. CASE STUDIES ON CYBERATTACKS BY NON-STATE ACTORS

A. Estonia v. Russia (2007)

The issue arose when Estonia relocated the Bronze Soldier, a soviet era war monument from the central Tallin to a military cemetery in April 2007. This relocation sparked outrage among Russian-language speakers and it resulted in a protest because, for ethnic Estonians this action reminded the soviet occupation and oppression but for Russian-speaking minority, it symbolized red Army's victory over Nazism.[36] This sparked unrest among the two groups which led to street riots which quickly escalated beyond physical demonstrations into cyberspace. On 26 April 2007 Tallin witnessed two nights of rioting and looting which resulted in the injury of 156 people and the death of one. On 27th April, Estonia was hit by major cyberattacks. Many of the initial attacks were traced to nationalist groups which encouraged civilians to join, and later on, more advanced DDoS attacks came from international botnets, which was found to have originated from thousands of computers worldwide.[37] This is considered the first instance where security of a state and its political independence was undermined primarily through cyber operations of one state by another.[38]

Estonia's vital digital infrastructures were targeted including government, financial, media and

[34] Judge Chile Eboe-Osuji, The Influence of the Permanent Court of International Justice in the Work of the International Criminal Court (International Criminal Court), https://www.icc-cpi.int/sites/default/files/itemsDocuments/201210-statement-President-Eboe-Osuji.pdf
[35] Vostoupal, *supra* note 27.
[36] Damien McGuinness, How a Cyber Attack Transformed Estonia, BBC News, Apr. 27, 2017, https://www.bbc.com/news/39655415
[37] Michael N. Schmitt, Cyber Operations and the Jus Ad Bellum Revisited (2011), https://digitalcommons.law.villanova.edu/cgi/viewcontent.cgi?httpsredir=1&article=1019&context=vlr
[38] Council on Foreign Relations, Estonian Denial of Service Incident ,May 2007, https://www.cfr.org/cyber-operations/estonian-denial-service-incident

internet service provider.[39] In Estonia, everything from tax returns to parking depended on online networks.[40] Because of its largescale digitization, the attack was extremely devastating in nature.

1. Attribution

The source of the attack has been mainly traced to Russia. Technical evidences such as some of the attacks came from private IP addresses, but some were also traced to a number of Russian government institutions.[41] Estonian leaders directly accused Russia based on the evidence pointing to IP addresses that originated from Kremlin offices in Moscow.[42] There were also various circumstantial evidences that were obtained. Such as, Nashi youth group was involved. This is a Russian pro-Kremlin group which was considered responsible for conducting regular cyberattacks on behalf of the Russian Government.[43] There was also evidence of Russian botnet expertise, the scale and sophistication with which the attack was conducted also pointed it to the Russian organized effort.[44] Non-cooperation of Russian law-enforcement was also a determining factor. As only one local attacker was convicted, making "silent support"[45]. It has also been claimed that Estonia was chosen because it's a former Soviet republic that had joined NATO.[46]

With the available evidence, effective control test fails to meet the extremely high threshold that has been established. In this case, it can be proven that overall control exists between the Nashi group and Kremlin. Nashi received millions in rubles from the state institutions like Public Chamber, presidential funds etc, Nashi was set up to propagate Russian internal and external policy, this shows that Russia has been involved with setting Nashi Youth Group and its goals and purposes. The group's strong ties with the government of Russia and its leaders supported them directly by conducting summer camps.[47] Thus it can be proven that the state

[39] Iradhati Zahra, Irawati Handayani & Diajeng Wulan Christianti, Cyber-Attack in Estonia: A New Challenge in The Applicability of International Humanitarian Law (2021).
[40] *Id.*
[41] *Id.*
[42] Schmidt, Andreas, The Estonian Cyberattacks, Atlantic Council (January 2013)
[43] Ashmore, William C. Impact of Alleged Russian Cyber Attacks. School of Advanced Military Studies Monograph (2009), https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-027.pdf
[44] *Id.*
[45] Ottis, Rain. Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective. Cooperative Cyber Defence Centre of Excellence (2008), https://ccdcoe.org/library/publications/analysis-of-the-2007-cyber-attacks-against-estonia-from-the-information-warfare-perspective/
[46] Eric Lipton, David E. Sanger & Michael Schwirtz. The Perfect Weapon: How Russian Cyberpower Invaded the U.S. N.Y. Times, Dec. 13, 2016.
[47] Zahra, Handayani, Christianti *supra* note 38.

had a role in organizing, coordinating, financing, and providing operational support hence the actions of Nashi group being attributable to Russia.

B. The Georgia–Russia war (2008)

On August 7, 2008, Russia and Georgia entered into armed conflict. The war originated after Georgia attempted to recapture South Ossetia. And as a response to this, the Russian army entered the country and seized back the territory of South Ossetia and Abkhazia.[48] Alongside tanks and airstrikes, cyberattacks were launched in a two-pronged manner on Georgia[49]. First prong consisted of conventional warfare tactics such as tanks, planes and missiles. And the second prong constituted cyber warfare, which coincided with the military attack. As a direct consequence of these attacks Georgian Banks got cut off from the international financial systems, cell phone services were disabled which resulted in Georgia being isolated from the rest of the world. It is commented that the Russian armed forces didn't need to hit communication facilities as they were already destroyed by the cyberattacks[50]

1. *Attribution*

Due to the intense technological advancements and complications, it is not clear who exactly initiated the cyberattack. Georgia openly blames the Russian government which has continuously been denied by the Russian Government. But the US researchers have purportedly unearthed strong evidences that link the attack to the Russian Business Network (RBN), which is a St. Petersburg-based organized crime gang. It also indicates that hacktivists/volunteers were also involved as they obtained simple tools to attack Georgian networks. Example: some sites had a simple button labelled "FLOOD", which unleashed attacks with a single click. [51]

The vagueness in pin-pointing who the actors make the already hard attribution extremely hard. Though, it is unclear, the timing of the cyberattacks strongly coincides with Russian military strikes, but Moscow denied official responsibility.[52] In a statement made by Colonel Anatoly Tsyganok, belonging to the Russian Military Forecasting Center, though did not blame the

[48] Gordon Corera, "UK Says Russia's GRU Behind Massive Georgia Cyber-Attack," BBC News, Feb. 20, 2020. https://www.bbc.com/news/technology-51576445
[49] Collin S. Allan, Attribution Issues in Cyberspace (2013). https://scholarship.kentlaw.iit.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1094&context=ckjicl
[50] *Id*.
[51] John Markoff, "Before the Gunfire, Cyberattacks," N.Y. Times, Aug. 12, 2008.
[52] *Id.*

government, called the cyberattack part of a broader "information battle"[53]

Cyberattacks were traced to U.S. Based servers, Russian telecom firms, and RBN- Controlled botnets which shows how "murky" attribution is in cyberspace.[54] According to Collin S. Allan[55], with the available evidences, Russia's conduct does not satisfy either of the tests.

This was the first known instance of cyberattacks which had consequences similar to that of kinetic warfare[56]. And an example of how cyberwarfare requires different evidences and is harder to attribute as compared to kinetic warfare.

C. Iran v. Albania (2022)

On July 15, 2022, Albania was hit by a massive cyberattack aimed at destroying government digital infrastructure which completely crippled services and hijacked data. The attack was claimed by "Homeland Justice" which pretended to be Albanian but in all likelihood was connected to Iran, which targeted the Iranian opposition group Mujahedeen-e-Khalq (MEK) living in Albania. According to FBI and Cybersecurity and Infrastructure Security Agency (CISA), the hackers got into Albania's networks 14 months before the actual attack and secretly stole large amounts of government data.[57] On July 2022, they used ransomwares to destroy data and left anti-MEK propaganda messages. In September 2022, a second wave of attacks were used employing the same methods and malware.[58]

1. *Attribution*

According to Microsoft, the attacks were carried out by a hacking group called "EUROPIUM", which is linked to Iran's Ministry of intelligence. Amongst many evidences, there were evidences of hackers operated from inside Iran. The tools used were same as the ones used by well-known Iranian actors, the targets matched Iran's political as well as strategic interests, and the wiper code was previously used by Iranian groups[59]

[53] Allan**,** *supra* note 48.
[54] Markoff, *supra* note 50.
[55] *Id.*
[56] *Id.*
[57] Vostoupal, *supra* note 27.
[58] Federal Bureau of Investigation & Cybersecurity and Infrastructure Security Agency, Iranian State Actors Conduct Cyber Operations Against the Government of Albania (2022). https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-264a
[59] Vostoupal, *supra* note 27.

Albania's Prime Minister publicly accused Iran which was supported by UK[60] and US. NATO[61] also attributed the attack to Iran and condemned the attack.[62] On September 6, 2022, the Albanian government cut off all diplomatic ties with the Islamic Republic of Iran and issued Iranian embassy staffs 24 hours to leave the Albanian capital.

V. POSSIBLE REFORMS

The intentions and motives of the different state and non-state players mentioned in this document are not the subjects of this discussion. Each may have their own reasons as it is the perspective that draws the thin line of separation between right and wrong. The purpose of this paper is not to take sides but to clinically and dispassionately evaluate the legal environment that would help determine whether there is State involvement in the actions of a third party in another state, especially so when the action is not kinetic but in digital form.

1) Existing attribution criteria are extremely strict in nature and hence it is difficult to fulfil such extremely strict standards. The existing laws of attribution were developed in a time when non-state actors acting to pursue the interest of the state were dependent on the state for material resources. But today many non-state actors are independent and self-sufficient. Therefore, a more practical standard for attribution is necessary, especially in cyber attribution, perhaps a revamped form of the overall control test proposed by the ICTY. Though the ICJ has rejected the overall control test, it was unable to put forward an exact reason why[63].

   In the case of cyberattacks, it is not necessary to financially support, or train or provide resources to non-state actors at the scale of kinetic warfare. States can support non-state actors even with minimal hand-holding, making it less traceable and linkable. Even the low threshold of Overall Control Test becomes insufficient for legal attribution to happen.

2) The establishment of an international agency[64] which is responsible for analysing, investigating and providing an assessment of responsibility in cases related to cyberattacks or cyberspace in general, would go a long way in attribution with respect to Cyber War. Establishment of such

[60] National Cyber Security Centre, UK Condemns Iranian State-Linked Actors for Cyber Attack Against Albania, Sept. 21, 2022. https://www.ncsc.gov.uk/news/uk-condemns-cyber-attack.
[61] North Atlantic Treaty Organization, Statement by the North Atlantic Council Concerning the Malicious Cyber Activities Against Albania. https://www.nato.int/cps/en/natohq/official_texts_207156.htm
[62] Vostoupal, *supra* note 27.
[63] Cassese, *supra* note 12.
[64] Nicholas Tsagourias & Michael Farrell, Cyber Attribution: Technical and Legal Approaches and Challenges, European Journal of International Law (2020), https://doi.org/10.1093/ejil/chaa057

agency will ensure that there will be required expertise to deal with the cyberspace and the intricacies related to it.

3) The application of the principle of "duty to prevent harm"[65] in international law can be one more step in eliminating 'reasonable doubt' while determining cyberattack attributability. This originated from the principle of due diligence which has been mentioned in Trail Smelter (1941)[66] and the Corfu Channel (1949)[67] cases. These cases put forward that the state is responsible if it fails to take the necessary and reasonable measures to prevent harm, even though it was not directly involved in causing harm.

   In the context of cyberspace, often cyber groups have similar motto or political ideology as that of the state. If, despite the group's wrongful act, the state does not take appropriate measures, to prevent the group's wrongful conduct, then it can be said, with reasonable fairness, that the state violated the principle of due diligence and hence is responsible for the conduct of the group. Questions like what preventive measures did the state take once they were aware of the threat? Were the measures taken by the state, reasonable enough, as compared to the technical resources that they have? If not, where they facilitating the actions of the cybergroup? Did the state gain any benefits from the group's action? etc. This method is only a part of the broader concept of attributability. Due diligence does not replace attribution tests, but in the cyberspace, this principle helps analyse the situation better and ~~provides~~ adduces evidences which might help in the attribution

4) The usage of multiple factors when attributing cyberattacks by non-state actors is propounded by the "control and capabilities" test.[68] This test looks at various factors like geographical location of attackers, method used, motivations that align with that of the state interest and technical capabilities that match with the state. Attribution in the case of cyberattacks can be made with reasonable surety only in cases where there are meaningful technical, social and other evidences. In the cyber-attacks faced by Estonia in 2007, the attack was attributed to Russia based on Russian-language coordination, IP address and timing etc. Similarly, the 2008 cyberattack on Georgia was linked to Russia because of the simultaneous armed attack that

[65] Peter Z. Stockburger, "Control and Capabilities Test: Toward a New Lex Specialis Governing State Responsibility for Third Party Cyber Incidents,"2018, https://ccdcoe.org/uploads/2018/10/Art-10-Toward-a-New-Lex-Specialis-Governing-State-Responsibility-for-Third-Party-Cyber-Incidents.pdf
[66] Trail Smelter (U.S. v. Can.), 3 R.I.A.A. 1905, 1965 (1941).
[67] Corfu Channel Case (U.K. v. Alb.), 1949 I.C.J. 4, 35 (Apr. 3).
[68] Stockburger, *supra* note 63.

was occurring from Russia and the evidences obtained about the linkage of the attack with Russian forums and actors. And hence, an approach towards attribution using circumstantial evidences is progressively increasing with respect to identifying state backing for cyberattacks.

VI. CONCLUSION

To form a legal framework, ideas from current practices must be taken into consideration even though the current practices are merely political attributions. Concrete evidences like circumstantial indicators, pattern of conduct, technical evidences etc. form the basis for state attribution in the case of cyberattacks. It is to be made clear that, it is not being established that the attribution is to be as flexible or fluid as done as in political arena but instead, to use the evidence used in political attribution as admissible and standard legal evidence.

Cyberattack attribution is an extremely complex area in international law and in order to address these complexities in a procrustean approach[69] which is a rigid, one-size-fits-all solution, will not be an appropriate solution. From the analysis of various cyberattack cases, it is clear that the practical application of attribution is markedly different from the currently prevalent attribution standards. Hence, in the interest of justice for those who bear the brunt of state-backed attacks, it is a crying need to establish an international legal framework for cyber warfare attribution in order to ensure uniformity, fairness and clarity in attributability standards. Such a framework can benefit from the lessons learnt from the attempts made by lawmakers who walked earlier and also from the practice of states in guarding their own interests. The framework shall also necessarily imbibe the technological advancements in locating cyber transgressions through the setting up of a separate international body for cyber warfare attribution through modern techniques and of course the tell-tale signs!

[69] Thomas C. Wingfield & Eneken Tikk, "Frameworks for International Cyber Security: The Cube, the Pyramid, and the Screen."
https://ccdcoe.org/uploads/2010/01/1.Wingfield_Tikk_FrameworksforInternationalCyberSecurity.pdf