INTERNATIONAL JOURNAL OF SPACE LAW AND POLICY
VOLUME 2 AND ISSUE 1 OF 2024
APIS – 3920 - 0014 *(and)* ISSN - 2584-1955 [IF SCORE – 7.58]
Published by
Institute of Legal Education
https://iledu.in

CYBER WARFARE AND THE LAW OF NEUTRALITY

AUTHOR - SNEHA SMRITI, STUDENT AT THE WEST BENGAL NATIONAL UNIVERSITY OF JURIDICAL SCIENCES, KOLKATA

BEST CITATION - SNEHA SMRITI, CYBER WARFARE AND THE LAW OF NEUTRALITY, *INTERNATIONAL JOURNAL OF SPACE LAW AND POLICY (IJSLP),* 2 (1) OF 2024, PG. 52-60, APIS – 3920 - 0014 & ISSN - 2584-1955.

INTRODUCTION

In the popular sense of the term, neutrality can be interpreted as abstaining from the war. As a result of this, the concept of neutrality has existed hand in hand with warfare itself. It is for states who choose to abstain from hostilities while others are fighting[94].The law of neutrality performs a dual protective function by safeguarding both the belligerent interests against intervention from neutral states and the sovereignty of the neutral state from prolonged hostilities[95].When hostilities take place in or through cyberspace, the law of neutrality is frequently questioned, even though it plays a crucial part in the understanding of an international armed conflict which is accompanied by the presence of conventional weapons. Applied to the cyber context, the law would protect the cyber infrastructure present in the territory of the neutral state obligating the belligerents to respect the inviolability and sovereignty of nations that are not involved in the ongoing international conflict.

The paper will start by analysing the nature and functioning of cyberspace and the way in the in which the current idea of sovereignty would get integrated with the same. This would include understanding the ambit of sovereignty in the newest frontier while comparing it with its essence in the land, sea, air and outer space. In the next part we will understand the law of neutrality and the duty it creates. This would be divided into two parts, focusing on the obligations of both the belligerents as well as the neutral states. This would be followed by analysing the probable ways in which the law of neutrality would come into play in probable scenarios like cyber-attack using the servers of a neutral state or by using a CERT network. Then, we would be considering a case study, the cyber attacks which took place in Georgia to understand the probable way in which the law could have been used. We will end the paper by trying to reach a probable way forward.

Keyword: Cyber Warfare, Sovereignty, Belligerents, Neutrality

GRASP - EDUCATE - EVOLVE

[94] Philip C. Jessup, *Neutrality: Its History, Economics and Law,* 4 ECONOMICS AND LAW 3, (1976).
[95] Patrick W. Franzese, Sovereignty in Cyberspace: Can It Exist? , 64 AFLR, 1-42 (2009).

INTERNATIONAL JOURNAL OF SPACE LAW AND POLICY
VOLUME 2 AND ISSUE 1 OF 2024
APIS – 3920 - 0014 *(and)* ISSN - 2584-1955 [IF SCORE – 7.58]
Published by
Institute of Legal Education
https://iledu.in

The Internet is an omnipresent entity, while it cannot be felt anywhere, the impact of its presence can be felt everywhere. Once the person has logged himself in the Internet, he is not just restricted to its physical space, controlled by a territorial sovereign, but also becomes a part of the never-ending cyberspace[96]. This seamless travel from one cyberspace to another poses a variety of problems when juxtaposed with the well-established sovereign territory of a nation state[97]. This makes it necessary to understand how the idea of sovereignty would be understood within the law of cyberspace.

It is not wrong to say that cyberspace serves as the ever-growing fifth-domain of warfare[98]. However, there are certain unique characteristics which make the cyberspace a unique warzone compared to its counterparts. For starters, there are minimal physical manifestations which have a role to play while the transmission of data takes place via various computers, making the domain intangible.[99] The data is scattered within various data providers, part of different jurisdictions, making it next to impossible to place the burden on one particular territory for the data exchange taking place. This is coupled with the fact that the States are not the main stakeholders of the cyber domain and cannot exercise complete control over its functioning[100].

Even if the data is traced back to the servers of a particular state, the State lacks the ability to completely restrict such transmission from taking place. This is due to the presence of three main factors, including but not restricted to the numerous number of technological hurdles.[101] The state may also face various legal limitations due to the extra-judicial territorial reach, due to the fact the servers of these networks would be located in the host country and all the transmission is based out of the same. Lastly, various states may lack the infrastructure required to even locate the private routers which are responsible for the transmission of data.[102] So, often times the management of the transmission of data depends on the working of the private enterprises, which is counter-productive in nature[103]. Due to the development of these factors, the improvement in the cyber space takes place organically with multiple stakeholders getting involved in the decision making regarding the protocol, standards and norms. Due to this, no single body can exercise absolute control over the functioning of the cyberspace. All this makes it necessary to understand how the definition of sovereignty would be applicable with this distributed relationship.

Sovereignty can be understood as the supreme political authority which is responsible for the functioning of an independent state. As can be understood from Article 2(4) of the UN Charter, the importance of the sovereignty is to ensure that the State's ability to maintain its territorial integrity is protected. This is one of the vital goals of both the state-based international organizations as well as the individual state concerned[104]. This idea of sovereignty is much easier to apply in the physical domains and have been in existence for a long period of time. These often get determined with the culmination of the state interests combined with their technological capabilities.

Even though references can be taken from the procedure available for outer space, it lacks in the prospect that there is no common goal attached with this avenue for the welfare of all mankind[105], which serves as a hindrance for

[96] MITCHELL WILLIAM, CITY OF BITS 8 (The MIT Press 1995).
[97] *Id.* at 60
[98] Ronald R. Fogleman, *Information Operations: The Fifth Dimension of Warfare*, 10 DEFENCE ISSUES 1, (1995).
[99] TALLIN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 105 (Cambridge University Press 2017).
[100] Cybercrime Convention Committee (T-CY), CRIMINAL JUSTICE ACCESS TO ELECTRONIC EVIDENCE IN THE CLOUD: RECOMMENDATIONS FOR CONSIDERATION BY THE T-CY , (2016)
[101] Eric Talbot Jensen, *Sovereignty and Neutrality in Cyber Conflict*, 35 FORDHAM INTERNATIONAL LAW JOURNAL, 824 (2012).
[102] *Id*
[103] Kristen E. Eichensehr, *The Cyber-Law of Nations*, 103 GEORGETOWN LAW JOURNAL, 317 (2014).
[104] PATRICK, *supra* note 1, at 90.
[105] CARL E. BUCHMANN, SPACE LAW: STATE RESPONSIBILITY FOR SPACECRAFT DAMAGES AND FOR THE RETURN OF PERSONNEL AND EQUIPMENT 1-40 (1965).

state sovereignty. With the number of entities involved, it is necessary that a sovereign exercises its control and makes the rule. This necessitates the introduction of a well-established procedure like the Law of the Sea which is a balance between the needs for international freedom as well as national security.[106] It needs to recognize that the international telecommunication system is beneficial for all the States while ensuring that these systems are following certain basic protocols.

Understanding this principle of sovereignty and the role it plays in cyber space becomes necessary due to the interplay between sovereignty and the law of neutrality. Both the obligations of the belligerents as well as the neutral state is linked to their sovereignty[107]. One example of the same is the requirement of not intervening in the cyber infrastructure of another neutral county, as the same would be considered violative of their sovereignty[108]. This would be better understand when we look at the application of the law of neutrality in the upcoming section.

THE LAW OF NEUTRALITY

The term "law of neutrality" can be regarded in its most common usage as the legal relationship that exists between countries involved in hostilities (belligerents) and those who are not part of the same (neutrals)[109]. It is responsible for protecting the sovereignty of the neutral states and their citizens against attacks by belligerent states while protecting the interests of the belligerent state from the interference of the neutral states[110]. It plays a significant part in limiting hostilities to the belligerent states, controlling the behaviour of the parties engaged, and reducing the negative impact of the hostilities on the global environment[111]. In the cyber context, it can be understood that the law is responsible for protecting the infrastructure present in the neutral state or any other infrastructure used by the neutral state for any non-commercial purpose[112]. Simultaneously, the neutral states need to remain impartial and not support any of the belligerent states in their cyber activities and take active steps for the protection of their cyber infrastructure from any probable abuse from the belligerent states.

These findings have been supported by majority of authors who have written on the implementation of law of neutrality for the cyber domain along with its implementation in the State practices. One illustration of the same can be seen in the U.S. Department of Defence (DoD). Among the various definitions which exist about cyberspace, they see it as an international domain with interconnected networks of information technology cells that enable the transfer of data[113]. They have emphasized that the same needs to be followed for armed conflicts in cyberspace as well and the application of the same is critical for the welfare of both the neutral and belligerent state[114]. The Report also outlines the activities that take place through computers and telecommunication networks which are present in the neutral state.

There have instances where this complex regulation and the application of the report have come into question in real life. The New York Times reported in October 2011 that the United States was considering using cyberwarfare against Libya, but that decision was ultimately made to deploy kinetic force instead, owing to the "potential legal complications" associated with that strategy[115].

[106] Steven M. Barney, *Innocent Packets? Applying Navigational Regimes from the Law of the Sea Convention by Analogy to the Realm of Cyberspace*, 48 NAVAL L. REV. 58, 63 (2001).
[107] T.K. Shahani, *Neutrality and the Law of Neutrality in Recent Times,* 3 THE INDIAN JOURNAL OF POLITICAL SCIENCE 3, 277-312 (1942).
[108] *Id*
[109] The Commander's Handbook on the Law of Naval Operations, A.R. Thomas & James C Duncan
[110] Stephen D Rynerson, *The Law of Information Conflict: National Security Law in Cyberspace*, 31 DENVER JOURNAL OF INTERNATIONAL LAW 1, 3 (2003).
[111] McNeill, *Neutral Rights and Maritime Sanctions: the Effects of Two Gulf Wars,* 31 VA. J. IND L. 631, (1991).
[112] *Id*
[113] 1-02 Department of Defense, DICTIONARY OF MILITARY AND ASSOCIATED TERMS 58 (2010).
[114] *Department of Defense Startegy for Operating in Cyberspace,* US DEPARTMENT OF DEFENSE, (2011).
[115] Sico Van Der Mee, *Deterrence of Cyber-Attacks in International Relations: denial, retaliation and signalling,* INTERNATIONAL AFFAIRS FORUM 85, 90-95 (2017).

INTERNATIONAL JOURNAL OF SPACE LAW AND POLICY
VOLUME 2 AND ISSUE 1 OF 2024
APIS – 3920 - 0014 *(and)* ISSN - 2584-1955 [IF SCORE – 7.58]
Published by
Institute of Legal Education
https://iledu.in

The goal of the government was to break through the government network of Libya and sever the military communication links, which would ultimately prevent them from relaying missiles at NATO warplanes[116]. One of the major impediments under the same has been the violation of the neutrality of third-states like Switzerland who would fall within the inevitable range of the cyber weapons[117]. Another fear it faced was about setting a precedent for countries like Russia or China to carry out such attacks on cyberwarfare, especially when there were no laws to regulate the same.

Another report which discusses the application of law of neutrality for the cyber domain and cyber warfare is the HPCR Manual on International Law Applicable to Air and Missile Warfare (the "*AMW Manual*")[118]. It was made to reiterate the international legislation governing air and missile warfare, however, it has gone ahead to also discuss about probabilities of law which would apply to cyberwarfare. Created by the "Program on Humanitarian Policy and Conflict Research" (HPCR) in Harvard University, it has been endorsed by a lot of sovereigns and can be considered as representing a consensus on something which is desired by all the states to deal with cyberwarfare[119]. Further clarity can be seen about the application of this law of neutrality when we individually understand its application for the belligerent and the neutral states.

Obligations of the Belligerent

The conventional interpretation of the law of neutrality stipulates that the parties engaged in conflict must recognize the sovereignty of the neutral states, refrain from waging hostilities against them, and refrain from using their resources for military gain. These prohibitions have been laid down in various treaties like Article 1, 2 and 3 of the 1907 Hague Convention V[120] and Article 1, 2 and 5 of 1907 Hague Convention XIII[121] and are also considered customary in nature.

a) No Harmful Interference with Cyber Infrastructure of Neutral States

This is based on the understanding that the cyber infrastructure which is present in the neutral states can easily be manipulated by the belligerents and so the same needs to be protected. It need not be considered if the infrastructure is owned by the government, corporation or any private individual, the protection needs to be extended to every infrastructure located in the neutral state[122]. This interference is not just restricted to the traditional cyber-attacks but includes every such act which may alter the functionality of the infrastructure or make them obsolete[123]. However, mere intrusion in the infrastructure of the neutral state cannot be considered as the international law does not have any provisions against the provisions of espionage[124].The provisions of territorial sovereignty also extend to the restriction on extending jurisdiction to foreign land. The same was also acknowledged by the PCIJ through the case of the S.S. Lotus[125].

b) Cyber Infrastructure and the Exercise of Belligerent Rights

To achieve the goals of the law of neutrality, which includes preventing the existing international armed conflict from getting worse, it is also required to forbid the use of belligerent rights to use the neutral cyber infrastructure. This refers to those particular infrastructures which enjoy a sovereign immunity and are used for government purposes, like those used for interaction with the military[126]. However, it has

116 *Id*
117 *Id*
118 Program on Humanitarian Policy and Conflict Research at Harvard University, Manual on International Law Applicable to Air and Missile Warfare, §10.
119 Danielle Higson, *Applying the Law of Neutrality while Transitioning the Seas of Cyberspace,* 6 AMERICAN UNIVERSITY NATIONAL SECURITY LAW BRIEF 1, 14-28 (2016).
120 Hague Convention V, Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land, Oct. 18, 1907.
121 Hague Convention XIII, Concerning the Rights and Duties of Neutral in Naval War, Oct 18, 1907.
122 Wolff Heintscel Von Heinegg, *Neutrality in Cyberspace,* CYCON, 1-12 (2012).
123 THE FEDERAL MINISTRY OF DEFENCE OF THE FEDERAL REPUBLIC OF GERMANY, HUMANITARIAN LAW IN ARMED CONFLICTS – MANUAL 1101 - 1155 (Oxford University Press 1992).
124 The Case of the S.S. Lotus, PCIJ Ser. A No. 10 (1927).
125 *Id*
126 Geneva Convention, Additional Protocol I, Article 52 (2), June 8, 1977.

INTERNATIONAL JOURNAL OF SPACE LAW AND POLICY
VOLUME 2 AND ISSUE 1 OF 2024
APIS – 3920 - 0014 *(and)* ISSN - 2584-1955 [IF SCORE – 7.58]
Published by
Institute of Legal Education
https://iledu.in

not been qualified if the same would be extended to the cyber infrastructure which is owned by the private enterprises outside the neutral state. In such a situation, the individual infrastructure can be considered as helping the belligerent state's army and they would be treated as a legitimate military object by the opposing state. Also, the belligerent state may not use its cyber infrastructure if the same is located near the territory of the neutral state[127]. Also, the belligerent state cannot make use of its own cyber infrastructure as well if the same has been erected in a neutral territory. It doesn't matter if it was set up before or after the starting of the international conflict. The same can be derived from Article 3 of the Hague Convention V, 1907[128].

c) Exceptions to the Prohibitions imposed

The prohibitions which have been imposed on the cyberspace need to be looked at while keeping in mind the unique nature of cyberspace. Due to the inter-dependence of the various telecommunication networks, it is nearly impossible for the belligerent state to stop hostile date from passing via the neutral state's cyber infrastructure. This makes the application of Article 8 of Hague Convention V, 1907 to the functioning of these cyber operations almost necessary[129]. An interpretation of the same can be concluded to mean that only when the cyber operation is functioning from the neutral state's infrastructure can it be assumed that the belligerent rights are being exercised from the neutral territory[130]. However, the same needs to be read along with Article 2 of the Convention.

Obligations of Neutral State

The law of neutrality imposes a set of obligations not only on the belligerent, but also on the neutral state. One of the main duties included under the same the duty to remain impartial[131] along with a prohibition to tolerate the belligerent rights or violation of the provision of neutrality among others.

a) Cannot Withstand the Exercise of Belligerent Rights Upon them

If we were to interpret Article 5 of the Hague Convention V, it can very much be concluded that one of the duties imposed on the neutral state is that they shouldn't be allowing or tolerating the use of their cyber infrastructure for carrying out the belligerent rights, given that the neutral territory has exclusive control over it[132]. The term "allow" presupposes that the neutral state has a knowledge about the malicious activities being carried out. In case of cyber-attack, the transactions would take place at such a high speed that it becomes near impossible for the neutral state to know about the happening of the event and violate the obligation[133]. In most cases, the neutral state wouldn't even have constructive knowledge about the malicious activities being carried out. This is a presupposition and there may be a distant possibility that with the advancement with technology, it would be possible for the neutral country to get the constructive knowledge, changing the entire stance.

b) Prevent the violation of Law of Neutrality

This obligation imposed on the neutral states during the armed conflict is not absolute in nature and depends upon the feasibility and the infrastructural capability of the neutral state[134]. It is a subjective standard where the neutral state are required to take all probable steps based on their capability to present themselves as a neutral state[135].This implies that they must take all required action, including the

[127] *Id*
[128] Hague V, *supra* note 27.
[129] Hague V, *supra* note 27, Article 8.
[130] *Id*

[131] Department of the Navy Office of the Chief of Naval Operations and Headquarters, The Commander's Handbook on the Law of Naval Operations (Newport 1997).
[132] Dietrich Schindler, *Transformations in the Law of Neutrality since 1945*, Humanitarian Law of Armed Conflict – Challenges Ahead, Essays in Honour of Frits Kalshoven 367-386 (1991).
[133] DOD, *supra* note 16.
[134] San Remo Manual on International Law Applicable to Armed Conflicts at Sea, para. 22, Dec. 31, 1995; The Federal Ministry of Defence of the Federal Republic of Germany, Humanitarian Law in Armed Conflicts Manual, 1992.
[135] HPCR Manual on International Law Applicable to Air and Missile Warfare, Rule 168(a), July 2013.

INTERNATIONAL JOURNAL OF SPACE LAW AND POLICY
VOLUME 2 AND ISSUE 1 OF 2024
APIS – 3920 - 0014 *(and)* ISSN - 2584-1955 [IF SCORE – 7.58]
Published by
Institute of Legal Education
https://iledu.in

use of force, to put an end to the belligerent state's illegal activities. The belligerent state cannot consider these as hostile acts and need to deal with the same. On the aspect of preventing a probable exercise of belligerent rights, there is no clarity on whether it would extend to the cyberspace as the same is only restricted to one's territory and national airspace[136].This is due to the fact that accepting this requirement would require constant monitoring of cyber operations that originate or are sent over their infrastructure, making it nearly impossible to determine whether the data is malicious. So, for the major part, the neutral state is responsible for the activities which fall under Article 8 of The Hague Convention XIII and are carried out by belligerent state.

c) The Repercussions of Non-Compliance with Neutrality

During the Post-World War II international armed conflicts, neutral states frequently disregarded their duty to maintain neutrality, either endorsing one side or attempting to hide their violations in subtle ways. According to the law of neutrality, in such a scenario, it is a right of the other belligerent party to take steps which terminates these violations[137]. This specific type of countermeasure has been offered t make sure that the belligerent state can retain the status quo and that the neutral states can fulfil their obligations. The same has been very categorically mentioned by the International Law Commission in its report on "Responsibility of States for Internationally Wrongful Acts[138]". This makes it necessary for the belligerent state to prove that there was a violation of their security concern before taking any such step against the neutral state. The US Department of Defense (US DoD) contains the following details in their manual for the scenarios.

- The type of cyber activity
- The third country's capacity and readiness
- The role of the third country[139].

POSSIBLE APPLICATION IN REAL LIFE

It becomes necessary to understand how all these theoretical assumptions and understandings would play out in real life and the same would be understood via this section assuming two probable situations which might be faced by the countries- using servers located in a neutral state to launch a cyberattack and relay information through the "CERT" network.

Let us take an illustration for understanding the first illustration. State A and State B are two belligerent states in which State A is executing a cyberattack against State B using malware that is released in the neutral state C's cyber infrastructure in order to harm State B's infrastructure[140]. Since the spread of the malware to a "movement of troops" or "munition of war" via a neutral state, it may be interpreted, under the law of neutrality, as an invasion of State C's territory and a breach of that law.

However, HC-XIII Article 10 of the Law of the Seas states that a neutral state's law would not be broken simply by allowing the belligerent state's warship to trespass through it[141]. If the same is to be applied in the present scenario, and the malware is considered as the warship, the belligerent state has not violated the law of neutrality as the neutral state was used as a mere passage for the transmission of the malware. This discrepancy results from the fact that the sea domain's specific distinct characteristics dictate the law of neutrality, while the land domain's code of neutrality is based on its actual borders and territories.

It is unclear which of the two sets of the rule would be made applicable in the cyber context.

[136] *Id*
[137] San Remo, *supra* note 41.
[138] Responsibility of States for Internationally Wrongful Acts, Article 22, 49-52, International Law Commission, 2001.
[139] DOD, *supra* note 16
[140] Jeffrey T.G. Kelsey, *Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare*, MICHIGAN LAW REVIEW, 1427-1451 (2008).
[141] Convention XIII concerning the Rights and Duties of Neutral Powers in Naval War, Art. 10, 12, Oct. 18, 1907.

INTERNATIONAL JOURNAL OF SPACE LAW AND POLICY
VOLUME 2 AND ISSUE 1 OF 2024
APIS – 3920 - 0014 *(and)* ISSN - 2584-1955 [IF SCORE – 7.58]
Published by
Institute of Legal Education
https://iledu.in

If we were to consider the land domain, a majority of the cyber transmission would lead to violation of the belligerent rights in every second case, which is not a viable approach taken. This would be undermining the relevance of the existing regime[142]. On the other hand, if we were to consider the law of the sea, a different set of questions of compatibility will come into play. The warship passages cannot be prohibited but for the cyber domain, it is near inevitable for the servers to pass through the neutral routes[143]. So, the picture is clearly not as clear as it appears in the first instance and there cannot be any law which can be said to apply mutatis mutandis to the given scenario.

The other scenario which is considered is if the state C establishes a Computer Emergency Response Team (CERT), owned and managed by the government, which is responsible for protecting both the private and the public cyber entities situated in the state[144]. Due to the cyber warfare going on between A and B, the CERT is receiving a lot of information about a probable cyber-attack which is aimed at the infrastructure situated at A. Due to the agreement between the states, state C relays this information to State A based on which A is able to prevent the attack.

The law of neutrality would come into picture in such a scenario as it would be considered a duty on the part of the neutral state to abstain from involving in the ongoing conflict. The Hague Convention XIII in Article 6 also mentions the same for the maritime domain[145]. In such a situation, the law of neutrality may have been violated by the disclosure of information by State C. However, such a conclusion would then undermine the very purpose of establishing a CERT network across states. Dozens of states are the part of these networks and expecting them to retain information due to the law of neutrality creates a contradictory position. This would make the law of neutrality both undesirable and non-achievable.

These two illustrations very categorically explain the probable confusion which would be created when the nations would use interpret the existing conventions and laws to be applied in the cyber domain. This would get further exacerbated when we consider the real life scenario which happened in Georgia in July, August 2008.

CASE STUDY: RUSSO-UKRAINIAN CYBER ATTACKS

As the Russia-Ukraine war has completed almost 600 days, no one remains aloof about the tension between both the countries. With constant attacks being launched on the ground and in air, the cyber-attacks have also become a constant part of war. There have been various invasions by Russia raising questions on the balance between offence and defence in cyberspace, the effectiveness of the cyber offences and the need for strategic planning and coordination. There have been various phases of these cyber-attacks varying from Russia shocking the invasion force and employing cyber units in a protracted war of attrition[146].

Russia attempted to infiltrate Ukrainian networks with malicious malware by using phishing, denial-of-service assaults, and software vulnerabilities. Eight distinct families of malicious software that Russia employed in these attacks were discovered by one company[147]. While media outlets, financial institutions, and energy and telecom companies, and Ukrainian government websites were the main targets. Most of the important industries were affected by the hacks. Up until now, Russia's greatest cyber triumph has been the interference with Viasat Inc's KA-

[142] PROGRAM ON HUMANITARIAN POLICY AND CONFLICT RESEARCH AT HARVARD UNIVERSITY, COMMENTARY TO THE HPCR MANUAL ON INTERNATIONAL LAW APPLICABLE TO AIR AND MISSILE WARFARE: ELABORATED BY THE DRAFTING COMMITTEE OF THE GROUP OF EXPERTS UNDER THE SUPERVISION OF PROFESSOR YORAM DINSTEIN (Cambridge University Press 2013).
[143] D. W. BOWETT, THE LAW OF THE SEA 1 (1967).
[144]TechTarget, Computer Emergency Response Team (CERT), https://www.techtarget.com/whatis/definition/CERT-Computer-Emergency-Readiness-Team.
[145] HC XIII, *supra* note 28, Art. 6; Hague Rules of Air Warfare, Art. 44, 1923.
[146] Dan Black, *Russia's War in Ukraine: Examining the Success of Ukrainian Cyber Defences*, 2 IISS, 10-17 (2023).
[147] Dave Clemente, *Cyber Security and global interdependence: what is critical?* CHATHAM HOUSE, (2013).

INTERNATIONAL JOURNAL OF SPACE LAW AND POLICY
VOLUME 2 AND ISSUE 1 OF 2024
APIS – 3920 - 0014 *(and)* ISSN - 2584-1955 [IF SCORE – 7.58]
Published by
Institute of Legal Education
https://iledu.in

SAT satellite[148]. However, Ukraine was successful in evading most of the impact of these cyberattacks. Without their robust and successful cyber defence, Ukraine may have suffered far more from this cyberattack.

It is crucial to emphasize at this point that Ukraine deserves the majority of the credit for its defense accomplishments. Undoubtedly, international collaborations with Western governments and commercial technological companies have made a substantial impact on Ukraine's capabilities. However, decades of investment and expertise in handing unprecedented levels of cyber warfare have furnished the essential foundational capacities to harmonize domestic endeavours with various types of external assistance. While most of the strategies used by Ukraine are not known as the war is ongoing, it is reasonable to infer that Ukraine has sought to put the "national cybersecurity system" into practice as described in its 2016 national cyber-security plan[149].

A week prior to the invasion, on February 17, 2022, the Ukrainian parliament passed laws enabling both public and private cloud computing infrastructure to be moved to foreign locations[150]. Under Martian law, these regulations were further strengthened. This made it possible for Ukraine to use reputable cloud service providers to backup and secure important governmental information and registration. The emergency transfer of essential services to data centres in Europe, which are protected from conventional threats like the alleged missile strikes which happened on the government data in Ukraine, was also made possible by this.

Officials from Ukraine have acknowledged the effect that the shifting of the cloud has had on the economy's ability to run and the continuation of essential government services. They has asserted that the Russian cyberattack has not prevented even a single registry from operating. Officials from Ukraine's National cyber Security Cluster emphasized during the end-of-year conference how important it was for legislative changes to be made in order to support CII protection and other facets of the country's defensive strategy.

However, there is a high probability that the law of neutrality would not have been violated in any of these scenarios. Russia in all probability would have denied all the involvement with the cyber-attacks as military operations even if the same has been announced by UK and other international allies.[151] The recognition of the cyberattacks as a computer security issue or a cyberwarfare would also be something which could be determined based on the treatment by Ukraine of the same. This makes it improbable to reach any conclusive decision on the application of law of neutrality in the ongoing Russo-Ukrainian war.

WAY FORWARD

Before the law of neutrality is applied to the cyber domain, one of the first conditions that must be met is that every norm pertaining to the traditional domains of conflicts must be carefully considered. This is to address the substantial distinctions between the traditional and cyber worlds. The same was also represented by the authors who drafted Tallinn Manual 2.0[152]. The same was reflected in the previous instance where even the easiest of consideration lead to a confusion regarding the law applicable for the cyber domain. This issue can be resolved only when the specific requirements of this domain is considered and an interpretation of the existing statutes is done based on the same[153].

[148] Gabby Roncone and John Wolfram, *Cyber war on the edge: a balance of Access and Action*, CYBERWARCON '22, (November 10, 2022), https://www.cyberwarcon.com/cyber-war-on-the-edge.
[149] Raphael Satter and James Pearson, *Exclusive: Ukraine prepares potential move of sensitive data to another country: official*, REUTERS (March 09 2022), https://www.reuters.com/world/europe/exclusive-ukraine-prepares-potential-move-sensitive-data-another-country-2022-03-09/.
[150] *Id*
[151] DAVE, *supra* note 54.
[152] MICHAEL N. SCHMITT, TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS (Cambridge University Press 2017).
[153] HUNTLEY, *supra* note 42.

For instance, without requiring any significant changes, laws that forbid the physical presence of belligerents on a neutral state's land, sea or air to prevent violations of the law of neutrality can be applied to the cyber domain. This means that no hacker of the belligerent state should be placed in the neutral state for operating the cyber infrastructure[154]. Similarly, a prohibition which exists on the supply of cash to belligerent state would also be made applicable to any form of digital transfer. However, to make any of these principles applicable, a broader reading of the law needs to be allowed by the international organizations.

In all practical sense, by giving the states a bigger role in the application of the law of neutrality would serve as a major breakthrough. This can be done by recognizing the legal significance of the practice they have been carrying out in cyber domain and the way the same would impact the military attacks. There is a long way to go before proper laws will come into place for the cyber domain and the same wouldn't be possible till the States are working together with the international organizations and common grounds are reached regarding the issues concerned.

[154] HC XIII, *supra* note 34, Art. 1.