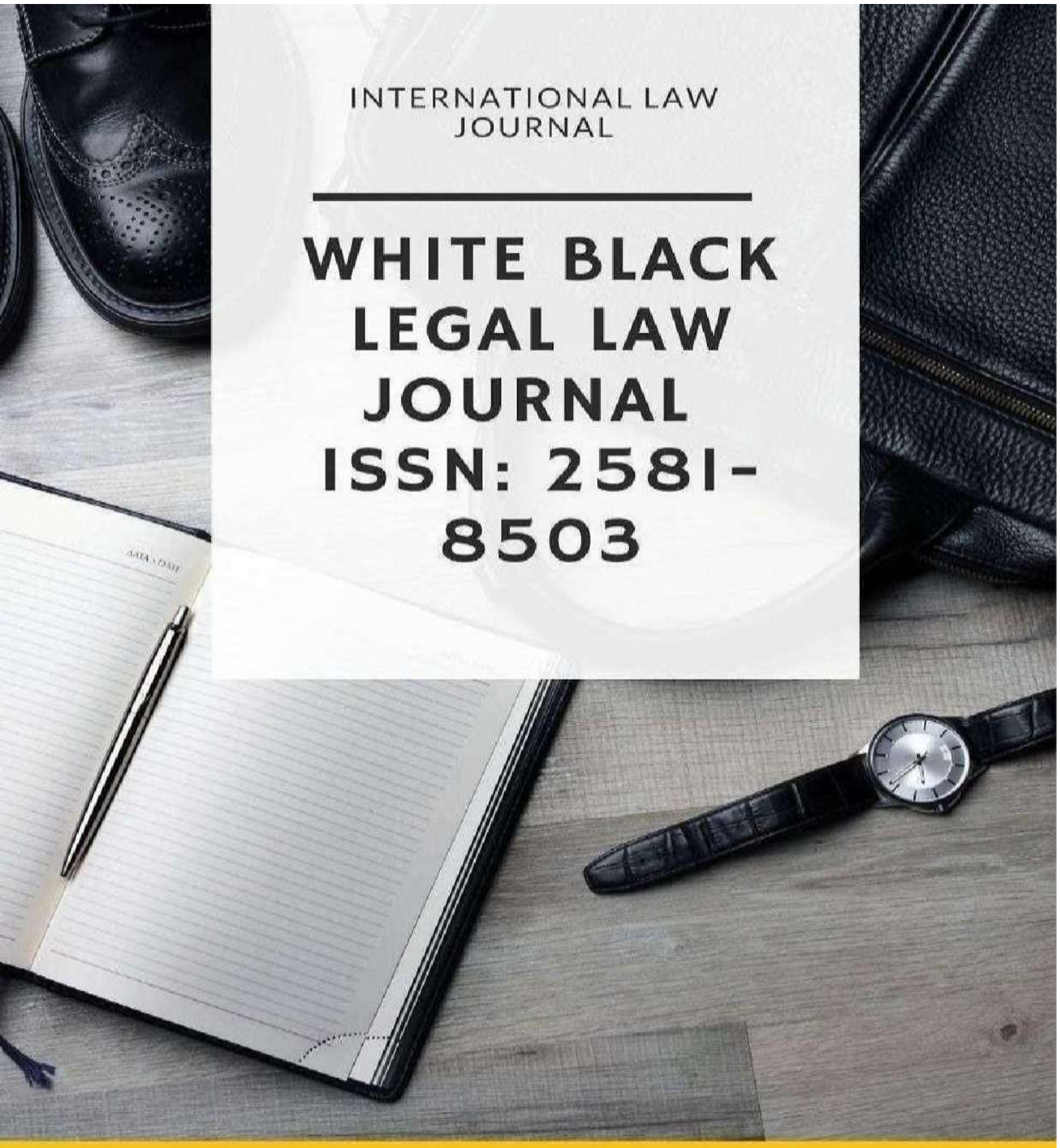

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

DISCLAIMER

EDITORIAL TEAM

Raju Narayana Swamy (IAS) Indian Administrative Service officer

Dr. Raju Narayana Swamy popularly known as Kerala's Anti Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala . He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University . He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru and diploma in Public a professional Procurement from the World Bank.

Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB , LLM degrees from Banaras Hindu University & Phd from university of Kota.He has succesfully completed UGC sponsored M.R.P for the work in the ares of the various prisoners reforms in the state of the Rajasthan.

Senior Editor

Dr. Neha Mishra

Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; Ph.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St.Louis, 2015.

Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi,

Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing Ph.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.

Dr. Navtika Singh Nautiyal

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in 'Intercountry adoption laws from Uttranchal University, Dehradun' and LLM from Indian Law Institute, New Delhi.

Dr. Rinu Saraswat

Associate Professor at School of Law, Apex University, Jaipur, M.A, LL.M, Ph.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

Dr. Nitesh Saraswat

E.MBA, LL.M, Ph.D, PGDSAPM
Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.
More than 25 Publications in renowned National and International Journals and has authored a Text book on Cr.P.C and Juvenile Delinquency law.

Subhrajit Chanda

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); Ph.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

ABOUT US

WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal providededicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

IMPLICATIONS OF THE LAW OF NEUTRALITY IN CYBERSPACE: PROBLEMS AND VIEWPOINTS

AUTHORED BY - RITIKAA HR

ABSTRACT

The fundamental objectives and goals of the law of neutrality are to safeguard the (territorial) sovereignty of neutral States and to prevent the outbreak of a global warfare. Analyzing neutrality offers a chance to explore an array of political-legal concepts and procedures that traditionally have had safeguarding and escalating reduction responsibilities and consequences in an emergency context characterized by increasing conflict and international rivalry. The implementation of conventional legal frameworks, such as the rule of neutrality, has been complicated by the quick development of technology and the creation of cyberspace. This article analyzes the idea of neutrality and how it may be used in relation to the internet. This article discusses the legal issues surrounding the application of the norm of neutrality in the internet as well as the historical and the technological context for neutrality. The article goes into more detail about how cyber wars are developing, the attribution issue, and the opportunity for creating new frameworks and norms to deal with the challenges of neutrality in the digital era.

Keywords: neutrality, cyber, international law, belligerents, armed conflict.

I. INTRODUCTION

Cyberspace is a brand-new artificial domain that cannot be heard or touched because it does not represent actual location - and escapes definition in the fundamental realm or time-space spectrum.[1] "At the speed of light, internet nowadays is seamless and crosses international borders"[2] However, cyberspace also introduces significant new vulnerabilities that could jeopardize global peace and stability.[3] Despite the fact that cyberspace has been around for a while,

[1] WALTER GARY SHARP, SR.,"CYBERSPACE AND THE USE OF FORCE," 1999, pp 1.

[2] Hathaway, Oona A., et al. The Law of Cyber-Attack. California Law Review, vol. 100, no. 4, 2012, pp. 817–85.

[3] Caton, Jeffrey L. EXAMINING THE ROLES OF ARMY RESERVE COMPONENT FORCES IN MILITARY CYBERSPACE OPERATIONS. Strategic Studies Institute, US Army War College, 2019.

this new area currently has no international regulations and even fewer accepted definitions. [4]

The concept of a cyber-weapon is essential to every analysis about technological warfare since these instruments of devastation differ from conventional weapons of war.[5] "A minimum of 140 States are working on developing cyber weapons. It is vital to differentiate between the two phrases because not every intrusion is cyberwarfare.[6] "Cyberattacks are a potent tool for achieving a wide range of goals, from espionage to propaganda, from denial of service to the destruction of vital infrastructure."[7] As a matter of fact, it might be challenging to ensure that the concept of neutrality is applicable if cyberspace is thought of as an emerging "5th dimension," a "universal prevalent," that "defies measurement in any physical dimension or time space continuum."[8] States have acknowledged that the conventional standard of neutrality continues to be relevant to present-day international Armed Conflicts, despite the fact that their behavior may not always have been in accordance with the desired level of impartiality.[9] Countries have slowly started creating local criminal statutes to govern how their citizens behave online, making it clear that the Internet is not an ungoverned untamed zone.[10]

The global public needs to choose the ways Governments shall characterize, exercise, and safeguard their sovereignty in cyberspace as well as shield the benefit of the Internet for cyber travelers.[11] Given the lack of international consensus on how to manage cyberspace, it will be challenging to establish any new framework to harmonize online behavior around the world.[12] Even though the US Department of Defense (DoD) has defined cyberspace, it occasionally finds itself unable to conduct cyber operations because there is no global consensus of "how to apply sovereignty, the law of armed conflict, and neutrality in cyberspace."[13] The Council of Europe Convention on Cybercrime is the only agreement to date to regulate cross-border Internet

---

[4] Colonel James B. Dermer, " Cyber Warfare: New Character with Strategic Results", United States Air Force, 2013.
[5] Ibid *supra* 2
[6] Lotrionte, Catherine. "Reconsidering the Consequences for State-Sponsored Hostile Cyber Operations Under International Law." The Cyber Defense Review, vol. 3, no. 2, 2018, pp. 73–114.
[7] KENNETH GEERS, "STRATEGIC CYBER SECURITY" 2009, pp 4-9.
[8] Giles, Keir. PROSPECTS FOR THE RULE OF LAW IN CYBERSPACE. Strategic Studies Institute, US Army War College, 2017.
[9] Dietrich Schindler, "Transformations in the Law of Neutrality since 1945", *Humanitarian Law Of Armed Conflict – Challenges Ahead, Essays in Honour of Frits Kalshoven*, pp 367-386.
[10] Tikk, E., Kaska, K., & Vihul, L., " International cyber incidents: legal considerations", CCDCOE, 2010, pp.79.
[11] Pearson, Christopher H. "Pattern Cladism, Homology, and Theory-Neutrality." History and Philosophy of the Life Sciences 32, no. 4 (2010).
[12] Alexander, Larry, and Maimon Schwarzschild. "Liberalism, Neutrality, and Equality of Welfare vs. Equality of Resources." Philosophy & Public Affairs 16, no.1.
[13] McGhee, James E. "Liberating Cyber Offense. Strategic Studies Quarterly, vol. 10, no. 4, 2016, pp. 46–63.

mischief, and it is widely seen as a failure.[14] It makes use of ambiguous terminology that are open to various interpretations in an effort to persuade most countries to ratify the pact.[15]

If battles continue to break out despite the UN Charter, cyber warfare presents a chance to destroy the foe with less casualties and physical harm than energetic conflict. A cyber-only triumph might make peacemaking, economic recovery, and post-war diplomacy easier. One hypothetical illustration is the Stuxnet computer worm, which was released in 2010 and targeted Iran's nuclear centrifuges. Other instances include the 2012 Aramco hack, the 2020 hospital ransomware attack and the 2007 Operation Orchard.[16] States shouldn't hold back from assisting a third nation in a cyber conflict because they fear losing their neutrality. States are changing cybersecurity by claiming their authority over this new frontier that was long seen to be limitless and ungoverned.

II. SOVEREIGNTY IN CYBERSPACE

The internet is not a location that can be defined or described. The Internet is ambient-it is simultaneously everywhere and nowhere.[17] By signing on from wherever one is physically, one can use the Internet and virtually travel through cyberspace while still keeping inside the boundaries of the country from which they set off on their voyage. The Internet is a massive network of "interconnected systems that has "considerable built-in capacity to resist power grabs and authoritarian control."[18] Commercial and governmental organizations use firewalls as a form of cyber security to shield themselves from the dangers lurking online.[19]

These firewalls are programmes that protect computers from some threats and block access to specific websites, but they do not halt the flow of electrons across state boundaries that occurs on the network. "Cyberspace has grown and spread to become a commons, a critical infrastructure that is pervasive and upon which societies throughout the world have become dependent for commerce, recreation, communication, the provision of governmental services, research,

---

[14] Tütüncü, Koray. "Liberalism, Neutrality and the Politics of Virtue." *SEER: Journal for Labour and Social Affairs in Eastern Europe*, vol. 16, no. 1, 2013, pp. 41–58.

[15] Lingelbach, William E. "Belgian Neutrality: Its Origin and Interpretation." *The American Historical Review*, vol. 39, no. 1, 1933, pp. 48–72.

[16] Faunt, Raymond A., and Philip D. Gentile. "Artificial Intelligence within the Intelligence Community: The Need to Retain the Human Dimension." American Intelligence Journal, vol. 36, no. 2, 2019, pp. 48–53.

[17] Mavropoulou, Elizabeth. "Targeting in the Cyber Domain: Legal Challenges Arising from the Application of the Principle of Distinction to Cyber Attacks." Journal of Law & Cyber Warfare, vol. 4, no. 2, 2015, pp. 23–93.

[18] Healey, Jason. When "Not My Problem" Isn't Enough: Political Neutrality and National Responsibility in Cyber Conflict. Atlantic Council, 2012.

[19] Kelsey, Jeffrey T. G. "Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare." Michigan Law Review, vol. 106, no. 7, 2008, pp. 1427–51.

education, and a host of other activities."[20] In order to keep the energy flowing freely currently experienced on the Internet, a regime of sovereignty is required because cyberspace is the basis of our civilization and the seas of commerce have emerged from the internet.[21]

Cyberspace requires the inherent rule of law that comes with sovereignty, but it also has to be accessible to international travel. Like in the case of maritime trade, free access, participation, and future development requires partnership among allies and friends in the international cyber community.[22] Despite being akin to space, cyberspace is not truly a global commons that is "managed together for the welfare of all people"[23] efficiently preventing sovereignty authority. Only a sovereign can offer the laws and regulations that the vast majority of individuals and businesses in cyberspace require.

In order to safeguard international freedoms while carefully balancing the demands of national security, this new realm requires a traversing system similar to the Law of the Sea.[24] It must acknowledge that cyber is a component of a global system of connections in which all States benefit from freedom of access and that any artificial borders would need to be in accordance with genuine concerns about national sovereignty and customary international law. This equilibrium can be achieved using a system of "transit passage."

German prosecutors first brought charges against CompuServe Deutschland's German manager in 1995 for failing to prevent German residents from being exposed to child pornographic content, many of which was produced outside of Germany."[25] States can regulate "local Internet service providers (ISPs)" to manage what content their residents can access online. Germany, Britain and France call for their regional ISPs to filter out the offensive content after receiving its complaint."[26] This safeguards the residents, but it does not prevent the objectionable data from

---

[20] Hildebrandt, Mireille. "EXTRATERRITORIAL JURISDICTION TO ENFORCE IN CYBERSPACE? BODIN, SCHMITT, GROTIUS IN CYBERSPACE." The University of Toronto Law Journal, vol. 63, no. 2, 2013, pp. 196–224.

[21] Hopper, Bruce. "Sweden: A Case Study in Neutrality." Foreign Affairs, vol. 23, no. 3, 1945, pp. 435–49.

[22] Paul, Christopher, et al. "Cyber Forces and U.S. Cyber Command." The Other Quiet Professionals: Lessons for Future Cyber Forces from the Evolution of Special Forces, RAND Corporation, 2014, pp. 23–30.

[23] "United Nations: Report of Legal Sub-Committee to Committee on Peaceful Uses of Outer Space (Assistance to and Return of Astronauts and Space Vehicles; Liability for Damage Caused by Objects Launched into Outer Space)." International Legal Materials", vol. 3, no. 3, 1964, pp. 528–50.

[24] McDougal, Myres S., and Leon Lipson. "Perspectives for a Law of Outer Space." The American Journal of International Law, vol. 52, no. 3, 1958, pp. 407–31.

[25] Albrecht, Ulrich. "THE ROLE OF NEUTRAL AND NON-ALIGNED COUNTRIES IN A WORLD OF GLOBAL POWERS." *Current Research on Peace and Violence*, vol. 11, no. 3, 1988, pp. 130–35.

[26] Jesse, Neal G. "Choosing to Go It Alone: Irish Neutrality in Theoretical and Comparative Perspective." "International Political Science Review / Revue Internationale de Science Politique, vol. 27, no. 1, 2006, pp. 7–28.

traveling through the digital world of those States.[27]

Before the year 2000, it was a common misconception that a State may be unable to regulate a web hosting company with headquarters in a different state By permitting Nazi artifacts to be advertised for purchase on French websites,[28] Yahoo, a US company, broke French law, according to a landmark ruling from French judges. “Although a complete blocking was not practicable, the court "ordered Yahoo to make a {reasonable effort} to block French users."[29] France did not remove the websites from its internet, but instead built a wall around its people to keep them safe from the Nazi products being marketed.

Despite permitting Internet use, China has carefully designed accessible content. China is seeking to “develop a network that is both closed and open enough to stifle political challenges to its hold on authority while supporting and maintaining the world's most rapidly expanding gdp.”[30] China has built a "firewall" around its citizens known as the "Great Firewall of China " in order to achieve this goal. This "firewall" screens and removes any information not authorized for a Chinese native.[31] Yahoo agreed to " filter content that might be dangerous or a threat" when it signed the Public Pledge on Self-Discipline for the Chinese Internet Industry in 2002. Online shopping requires a secure setting run by a sovereign that can protect consumers and businesses from crime. To avoid a scam, it is important to keep its commitments, by ensuring consistency in its sale offerings. eBay's founder, Pierre Omidyar, originally intended for the company to be “self-regulated by its users”,[32] "instantly studied that these goals would depend critically on government coercion and the rule of law provided by a stable country like the United States."[33] eBay was first governed by local law enforcement, but it currently employs over 800 security personnel full-time. Instead of defending their borders, States are erecting barriers in cyberspace to safeguard

---

[27] Jan Martin Lemnitzer, “Back to the Roots: The Laws of Neutrality and the Future of Due Diligence in Cyberspace”, *European Journal of International Law*, Volume 33, Issue 3, August 2022, Pages 789–819

[28] Sherman, Gordon E. “The Permanent Neutrality Treaties.” *The Yale Law Journal*, vol. 24, no. 3, 1915, pp. 217–41.

[29] Goel, Sanjay. “National Cyber Security Strategy and the Emergence of Strong Digital Borders.” Connections, vol. 19, no. 1, 2020, pp. 73–86.

[30] Gervais, Michael. “Cyber Attacks and the Laws of War.” Journal of Law & Cyber Warfare, vol. 1, no. 1, 2012, pp. 8–98.

[31] Preciado, Michael. “If You Wish Cyber Peace, Prepare for Cyber War: The Need for the Federal Government to Protect Critical Infrastructure From Cyber Warfare.” Journal of Law & Cyber Warfare, vol. 1, no. 1, 2012, pp. 99–154.

[32] Jessup, Philip C. “Diversity and Uniformity in the Law of Nations.” The American Journal of International Law, vol. 58, no. 2, 1964, pp. 341–58.

[33] Hofmann, Claudia, and Ulrich Schneckener. NGOs and Non State Armed Actors: Improving Compliance with International Norms. US Institute of Peace, 2011.

their populations. [34]

Despite the fact that the user of the World Wide Web wasn't actually in the state, cybercrimes are nevertheless subject to state prosecution. However, in order to develop sovereignty, there must be an international framework with clear guidelines governing state behavior in that area, as well as a requirement to recognise and monitor transnational entities.[35]

III. PRESERVING INTERNET NEUTRALITY

1. LAW OF NEUTRALITY - A GENERAL OVERVIEW

In its modern sense, the word "neutrality" was used in the fourteenth century, if not earlier.[36] The initial interpretation of absenteeism in war was offered by philosopher and diplomat Hugo Grotius, who advocated taking nothing from people in tranquility until it was absolutely necessary and then only after their worth had been restored.[37] Five political purposes are served by neutrality: independence, free commerce, power balance, integration, and solidarity.[38] Neutrality has always been a flexible foreign policy instrument.[39] In order to prevent the worsening of the continuing international armed conflict, the laws of neutrality are intended to "regulate the conduct of belligerents with respect to nations not participating in the conflict, to regulate the conduct of neutrals with respect to belligerents, and to reduce the adverse effects of such hostilities on international commerce."[40]

The depletion of the adversary's trade has been a key objective of belligerents since at least the fifteenth century, and this appears to be what gave rise to the concept of neutral sovereignty at sea.[41] The "1780 and 1800 Leagues of Armed Neutrality" (European naval alliances were formed to defend neutral shipping against the UK's unrestricted search policy for French contraband

---

[34] Podeh, Elie. "The Drift towards Neutrality: Egyptian Foreign Policy during the Early Nasserist Era, 1952-55." Middle Eastern Studies, vol. 32, no. 1, 1996, pp. 159–78. JSTOR, http://www.jstor.org/stable/4283780. Accessed 23 May 2023.

[35] Udombana, Nsongurua J. "Still Playing Dice with Lives: Darfur and Security Council Resolution 1706." Third World Quarterly, vol. 28, no. 1, 2007, pp. 97–116.

[36] MUELLER, WOLFGANG. "Two Differing Concepts of Neutrality." A Good Example of Peaceful Coexistence?: The Soviet Union, Austria, and Neutrality, 1955-1991, Austrian Academy of Sciences Press, 2011, pp. 41–87

[37] Q. Wright, "The Future of Neutrality," International Conciliation, Sept., 1928; The Causes of War and the Conditions of Peace (London, 1935).

[38] Erin F. Delaney, " Solidarity Federalism", Northwestern Pritzker School of Law, Notre Dame Law Review, pp. 620-628.

[39] Jonathan Zittrain, " Net Neutrality as Diplomacy", JOUR, 2010, pp. 65-70.

[40] Rowe, NC. "A Taxonomy of Norms in Cyber Conflict for Government Policymakers." Journal of Information Warfare, vol. 17, no. 1, 2018, pp. 31–48.

[41] "Geneva Convention Relative to the Protection of Civilian Persons in Time of War." The American Journal of International Law, vol. 50, no. 3, 1956, pp. 724–83.

aboard neutral ships) paved the way for Switzerland (1815) and Belgium (1839) to be regarded as the initial states to be constantly neutral by the global community.[42] The "1856 Paris Declaration Respecting Maritime Law,"[43] which tried to eliminate criminal activity while governing ties between neutrals and aggressors on the open waterways, and the "1872 Washington Rules of Neutral Duty,"[44] which required the neutral party to exercise caution in safeguarding foreign merchants, paved the way for the codification of the law of neutrality - the Hague Conventions' of 1907, which is based on fundamental economic principles.[45]

The "Tallinn Manual" describes how the law of neutrality might be utilized to the internet setting using parallels and links to the Hague agreements and UN Charter.[46] The "Cooperative Cyber Defence Centre of Excellence (CCDCOE)" of NATO had been invited to prepare it. There is growing consensus that cyberspace is subject to the full scope of international humanitarian law (IHL). One could infer that cyberspace and cyber activities are subject to the law of neutrality in its entirety as an element of IHL.[47] Only six of the twenty-three States that have issued their opinions on international law in cyberspace have really made this clear in their Opinio Juris.[48] The "Oslo Manual", the "Tallinn Manual", and, to a lesser degree, the "HPCR Manual" make a clear picture of the topic while making the case for the "interrelated nature of cyberspace infrastructure and the danger of harm to either private or public infrastructure."[49] Even though they are all nonbinding documents, the fact that several States have generally (or expressly) backed them shows that there is some degree of consensus.[50] The 1996 "*Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons*" by the International Court of Justice (ICJ) found that "as in the case of the principles of humanitarian law applicable in armed conflict, international law leaves no doubt that the principle of neutrality, whatever its content, which is of a fundamental character similar to that of the humanitarian principles and rules, is applicable to cyberspace."[51]

---

[42] Deibert, Ronald J., and Masashi Crete-Nishihata. "Global Governance and the Spread of Cyberspace Controls." Global Governance, vol. 18, no. 3, 2012, pp. 339–61.

[43] Garrie, Daniel B. "Cyber Warfare, What Are The Rules?" Journal of Law & Cyber Warfare, vol. 1, no. 1, 2012, pp. 1–7.

[44] Goel, Sanjay. "How Improved Attribution in Cyber Warfare Can Help De-Escalate Cyber Arms Race." Connections," vol. 19, no. 1, 2020, pp. 87–95.

[45] Hague Convention (V) and (XIII), available at https://ihl-databases.icrc.org.

[46] Fang, B, "Necessities for advocating cyberspace sovereignty, Cyberspace Sovereignty," pp. 103–134.

[47] Tan, Eugene E. G. "A Small State Perspective on the Evolving Nature of Cyber Conflict: "Lessons from Singapore." PRISM, vol. 8, no. 3, 2019, pp. 158–71.

[48] Butler and Maccoby, The Development of International Law (London, 1928)

[49] Ball, Desmond, and Gary Waters. "Cyber Defence and Warfare." Security Challenges, vol. 9, no. 2, 2013, pp. 91–98.

[50] Deibert, Ronald. "Cybersecurity: The New Frontier." Great Decisions, 2012, pp. 45–58.

[51] Matheson, Michael J. "The Opinions of the International Court of Justice on the Threat or Use of Nuclear Weapons." The American Journal of International Law, vol. 91, no. 3, 1997, pp. 417–35.

The core ideas of the concept of neutrality so largely hold true regardless of whether there are particular laws for land, sea, or air conflict.[52]

1.2. Cyberspace legal doctrine in armed conflict:

The international body of law known as the law of armed conflict (LOAC) will be applicable in cyberspace if digital warfare is a possibility. Consequently, this is the main inquiry: What constitutes the development of an International Armed Conflict (IAC) and the consequent application of International Humanitarian Law (IHL) and the concept of neutrality? The straightforward response is any use of hostilities or military force, whether by physical or virtual means, between States, regardless of its intensity.[53] It might even happen if any of the parties refuses to acknowledge the IAC's position. The existence or absence of an armed conflict is significant because parties to an armed conflict are frequently governed by the jus in bello (law of war), as opposed to the stricter rules that apply in law enforcement situations."[54]

Applying LOAC to this part of the internet is challenging because it is clear that this body of regulation did not take cyberspace into account.[55] Because LOAC isn't specifically applicable to cyberspace and fails to consider the distinctions between cyber conflicts and traditional energetic conflict, it must be applied by analogy. "Additionally, any novel forms of warfare are now covered under the Geneva Conventions Additional Protocol I, which broadens the scope of LOAC. A State is required to evaluate every "new weapon, means, or method of warfare to ensure that its employment would not violate international law."[56]

Both conventional law and conventions contain the body of international law [jus ad bellum], which governs when a State uses aggression over another state.[57] The UN Charter says that "all members shall refrain in their international relations from using the threat of force or the use of physical force against the territorial integrity or political independence of any state."[58] Although "*jus in bello* and *jus ad bellum"* are two distinct concepts of law, a person may resort to the jus ad

---

[52] Gervais, Michael. "Cyber Attacks and the Laws of War." Journal of Law & Cyber Warfare, vol. 1, no. 1, 2012, pp. 8– 85

[53] Warbrick, Colin, and Peter Rowe. "The International Criminal Tribunal for Yugoslavia: The Decision of the Appeals Chamber on the Interlocutory Appeal on Jurisdiction in the Tadic Case. The International and Comparative Law Quarterly, vol. 45, no. 3, 1996, pp. 691–701.

[54] "Protocol Additional to the Geneva Convention of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I)" art. 36, June 8, 1977, available at https://www.ohchr.org

[55] McGhee, James E. "Cyber Redux: The Schmitt Analysis, Tallinn Manual and US Cyber Policy." Journal of Law & Cyber Warfare, vol. 2, no. 1, 2013, pp. 64–103.

[56] Ibid., supra 53.

[57] Healey, Jason. When "Not My Problem" Isn't Enough: Political Neutrality and National Responsibility in Cyber Conflict". Atlantic Council, 2012.

[58] van Loon, Fabio. "Codifying Jus in Bello Spatialis—The Space Law of Tomorrow." Strategic Studies Quarterly, vol. 15, no. 1, 2021, pp. 10–27.

bellum concept when discussing the restrictions (Article 2(4) UNC), "exceptional legality, and definition of use of force and armed conflict."[59] However, this is merely a possibility.[60]

The primary distinction and connection between the two legal conceptions, according to the ICJ, is the "ability to discern between the "most grave forms of use of force" i.e., those equivalent to an armed attack and "other less grave forms."[61] In accordance with article 51 of the UN Charter, an armed attack constitutes a need for using self-defense. Nothing in the current UN Charter "shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations, until the Security Council has taken such measures as may be necessary to maintain international peace and security."[62] Although a state never loses its right to use force in self-defense [under Article 51] in response to a use of force within the meaning of Article 2(4), the right of self-defense under customary international law may not always justify an armed response,[63] Article 2(4) of the Constitution's right to self-defense for states may not necessarily call for an armed response.[64]

There has been much debate over what each term implies because the UN Charter uses the terms "use of force," "armed attack," and "aggression" in a number of its provisions without defining any of them expressly. Cyberattacks are launched for many different causes, and they can result in many different things." The absence of kinetic force necessitated a determination of "whether a cyber attack is a prohibited use of force under the Charter and customary international law."[65] In order to establish whether cyber activities breach Article 2(4) of the UN Charter's prohibition on the threat or use of force, several States and academics support the "scale and effect" test outlined in the Nicaragua Case of the International Court of Justice.[66]

---

[59] Mégret, Frédéric. "Jus in Bello and Jus Ad Bellum." Proceedings of the Annual Meeting (American Society of International Law), vol. 100, 2006, pp. 121–23.
[60] Caton, Jeffrey L. DISTINGUISHING ACTS OF WAR IN CYBERSPACE: ASSESSMENT CRITERIA, POLICY CONSIDERATIONS, AND RESPONSE IMPLICATIONS. Strategic Studies Institute, US Army War College, 2014.
[61] International Court of Justice (ICJ), "Case concerning oil platforms", pp. 161–219, available at https://www.icj-cij.org.
[62] Subedi, Surya P. "Neutrality in a Changing World: European Neutral States and the European Community." The International and Comparative Law Quarterly, vol. 42, no. 2, 1993, pp. 238–68.
[63] Article 2(4) of the United Nations Charter, available at https://www.un.org/securitycouncil.
[64] Diamond, Eitan. "Applying International Humanitarian Law to Cyber Warfare." Law and National Security: Selected Issues, edited by Pnina Sharvit Baruch and Anat Kurz, "Institute for National Security Studies, 2014, pp. 67–84.
[65] Deibert, Ronald J. "The Virtual Absence of Malice: Cyber Security and Threat Politics." International Studies Review, vol. 11, no. 2, 2009, pp. 373–75.
[66] International Court of Justice (ICJ), "Case concerning Military and Paramilitary in and against Nicaragua", para 165, available at https://www.icj-cij.org.

The majority of scholars employ Michael N. Schmitt's seven-factor method to identify instances of use of force in cyberspace.[67] The application of force does not include indirect techniques for economic, political, or psychological warfare.[68] Cyber warfare is one in which the deployment of cyber weapons (such as viruses, worms, and logic bombs) results in material loss or human suffering in addition to the destruction of the targeted computer programme or data.[69] The law of neutrality rarely applies online, just as the law of armed conflict does."[70] In some situations, the combination of cyberattacks could be viewed as a military assault.[71]

1.3. Obligations of Neutral States:

The Hague Conventions XII (HC XII) Concerning the Rights and Duties of Neutral Powers in Naval War and the Hague Convention V (HC V) Respecting The Rights and Duties of Neutral Powers and Persons in Case of War on Land contain the principles of international law governing neutrality.[72] When there is war, certain customs generally apply. Therefore, there must be a global war for the law of neutrality to be in force. "The obligations of neutral States to abstain from providing particular kinds of aid to hostile nations only come into effect in disputes of a specific duration and severity and are not relevant to every military hostilities in which the jus in bello principles pertain."[73] It is the neutral state's right to maintain a neutral commerce while it is the belligerents' responsibility to do so. A neutral state also has the right to the inviolability of its territory, which requires belligerents to refrain from certain hostile behavior, such as moving forces, ammunition, and other materials of conflict across neutral territory (Articles 2 and 8 of the Hague Convention on the Law of the Sea); setting up and utilizing wireless communication systems to communicate for military purposes (Articles 3 and 4 of the Hague Convention on the Law of the Sea); and recruiting "combatant corps" on the territory.[74] The neutral states also have obligations to appropriately exercise this right, namely the obligations of abstinence, prevention,

---

[67] Michael N. Schmitt, "TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE", Cambridge University Press, pp. 29-106, available at https://library.oapen.org

[68] Chang, Lennon YC, and Peter Grabosky. "The Governance of Cyberspace." Regulatory Theory: Foundations and Applications, edited by PETER DRAHOS, ANU Press, 2017, pp. 533–52.

[69] Goines, Timothy M. "Overcoming the Cyber Weapons Paradox." Strategic Studies Quarterly, vol. 11, no. 4, 2017, pp. 86–111.

[70] Anderson, Steven J. "Hypothesizing a Cyber-Power Targeting Theory." Airpower Lessons for an Air Force Cyber-Power Targeting Theory, Air University Press, 2016, pp. 87–130.

[71] NATO, Brussels Summit Communiqué, 2021

[72] Schmitt, Michael N. "THE LAW OF CYBER TARGETING." Naval War College Review, vol. 68, no. 2, 2015, pp. 10–29.

[73] Bradshaw, Samantha, et al. "THE EMERGENCE OF CONTENTION IN GLOBAL INTERNET GOVERNANCE." Who Runs the Internet?: The Global Multi-Stakeholder Model of Internet Governance, Centre for International Governance Innovation, 2017, pp. 45–66.

[74] Bremmer, Ian. "Democracy in Cyberspace: What Information Technology Can and Cannot Do." Foreign Affairs, vol. 89, no. 6, 2010, pp. 86–92.

impartiality, and acquiescence.[75]

1.3.1. Abstention:

Articles 2 and 3 of the HC on Civil War and Article 6 of the HC on the Conduct of Hostilities prohibit neutral states from engaging in violent behaviors against aggressors, giving them "armed aid," or permitting the occupation of their land for conflicts.[76] This means that "neutral governments should refrain from participating in cyber actions or actions that have a direct or indirect impact on cyberspace,[77] as doing so would boost one belligerent military operation at the expense of the other.[78] (The only countries to address this duty were the Netherlands and Switzerland.)

Cyber arsenals used in military operations could be a wide variety of "artifacts," from specialized, highly advanced programmes like Stuxnet to less sophisticated, more generalized attacks with ransomware or DDos assaults using virus routers for disrupting the economy (as in NotPetya). Any tool, substance, instrument, system, piece of machinery, or piece of computer code that is created or intended for use in a cyberattack could also be considered a cyber weapon.[79] This ban exclusively applies to government exports of war materials; it has nothing to do with business shipments. The language of Article 7 HC V is clear: "A neutral power is not called upon to prevent the export or transport, on behalf of one or other of the belligerents, of arms, munitions of war, or, in general, of anything which can be of use to an army or a fleet."[80] In other words, the abstention duty has no impact on the rights of individuals and businesses to conduct business with belligerent States.[81]

It is vital to note that the neutral Government is not required to stop its people from aiding any hostile state entity while the states' operations are carried out of its borders.[82] However, in these

---

[75] Roscini, M. (2015) 'Cyber operations as a use of Force', Research Handbook on International Law and Cyberspace.
[76] Ibid., supra 45.
[77] Wolff Heintschel von Heinegg, ''Benevolent' Third States in International Armed Conflicts: The Myth of the Irrelevance of the Law of Neutrality', in: International Law and Armed Conflict: Exploring the Faultlines, 543-568.
[78] Wanner, Bastien, and Solange Ghernaouti. "Conceptualizing Active Cyber Defence in Cyber Operations: Quo Vadis, Switzerland?" St Antony's International Review, vol. 15, no. 1, 2019, pp. 58–82.
[79] Kilovaty, Ido. "Rethinking the Prohibition on the Use of Force in the Light of Economic Cyber Warfare: Towards a Broader Scope of Article 2(4) of the UN Charter." Journal of Law & Cyber Warfare", vol. 4, no. 3, 2015, pp. 210–56
[80] Ibid., supra 45.
[81] George K. Walker, 'Information Warfare and Neutrality', 33 Vanderbilt J.Trans.L., pp. 1079-1202, at 1182.
[82] Allen, Patrick D. "Cyber Maneuver and Schemes of Maneuver: Preliminary Concepts, Definitions, and Examples." The Cyber Defense Review, vol. 5, no. 3, 2020, pp. 79–98.

circumstances, the involved individuals risk losing their standing as neutral parties and their legal rights."[83] The online criminal would lose their impartial status and any associated statutory safeguards if they committed a cyber-hostile act against a belligerent that appeared to have been carried out by a neutral person rather than the Neutral's army or technology division.[84]

During peacetime, espionage is rarely addressed by international law, and cyber espionage is much less so.[85] However, a violation of the target State's sovereignty would result from a cyber espionage operation because the principle of territorial sovereignty forbids exercising jurisdiction over foreign territory.[86] This is predicated on the idea that a neutral State can be held accountable for the cyber operations under a generally accepted burden of proof provided by conventional global legislation of state accountability.[87]

1.3.2. Prevention:

Any transgressions of its neutrality may be put an end to or prevented, if necessary, by the use of force.[88] In the sea and aviation realms, the preventative duty is more lenient but nevertheless obligatory.[89] the neutral State's duty to exercise due diligence while employing the tools at its fingertips.[90] In addition, a "neutral State shall not intentionally let or condone a belligerent from using its borders and the cyberinfrastructure that is solely under its authority to wage conflicts.[91] "The neutral country should employ every fair strategy at their service so that it can put an end to the attack once it becomes informed of it."[92] "An aggressor can opt to react by deliberately harming the neutral nation's internet connection if the other nation is unable or unwilling to not take measures to stop an internet strike."[93] The utilization of telegraphic, radio, or telephone

---

[83] Articles 6 and 17 of Hague Convention V and Article 7 of Hague Convention XIII.
[84] Dietrich Schindler, 'Transformations in the Law of Neutrality since 1945', in: Humanitarian Law of Armed Conflict – Challenges Ahead, Essays in Honour of Frits Kalshoven, pp. 367-386.
[85] Deibert, Ronald. "Cybersecurity: The New Frontier." Great Decisions, 2012, pp. 45–58.
[86] Wright, Quincy. "Rights and Duties Under International Law: "As Affected by the United States Neutrality Act and the Resolutions of Panama." The American Journal of International Law, vol. 34, no. 2, 1940, pp. 238–48.
[87] Articles 4, 5, 8, and 16 of "responsibility of states for internationally wrongful acts", ILC ASR, available at https://legal.un.org/ilc
[88] Articles 5 of Hague Convention V and Article 25 of Hague Convention XIII.
[89] Rulli, Tina. "Conditional Obligations." Social Theory and Practice, vol. 46, no. 2, 2020, pp. 365–90.
[90] Articles 8 and 25 of the Hague Convention XIII and 15 of the San Remo Manual, as well as Articles 42, 46, and 47 of the Hague Rules of Aerial Warfare, available at https://www.icrc.org.
[91] Waxman, Matthew C. Cyber Strategy and Policy: International Law Dimensions. Council on Foreign Relations, 2017.
[92] Yoram Dinstein and Arne Dahl, "Oslo Manual on select topics of law of armed conflict", Rules and Commentary, available at https://library.oapen.org
[93] *Ibid*., supra at 63.

communication infrastructure is a key exemption to this obligation.[94] "The neutral power's duty to implement steps to stop such communication of "cyber weapons" across neutral cyberinfrastructure, is on only when the neutral state is aware of such an act."[95]

1.3.3. Impartiality:

In a maritime battle, the entry of hostile warships or their spoils into its harbors, roadsteads, or waterways[96] should be subject to the impartiality rule.[97] "For the benefit of either side in a conflict, of weapons, combat weapons of mass destruction, or generally items that could be useful to a navy or military."[98] It must carry out this duty without discrimination.[99] Neutrals must act with fairness when limiting or forbidding access to or usage of their cyberinfrastructure. "So far these means are made available for the two, a neutral Power is not required to prohibit or limit [communications]."[100] This however raises the whole Tulip systems (TSHost) dilemma.[101]

1.3.4. Acquiescence:

The belligerent could be allowed to apply specific measures for protection of their own or assistance against aggressive troops in the opposition's nation if that State is hesitant or reluctant to thwart the appropriation of its area for aggressive actions against it.[102] "When a hostile state uses its right to remedies to put an end to a breach, the neutral's obligation to comply [i.e., acquiesce] takes effect.[103]

1.4. Obligations of belligerents:

The "duty of the aggressors to uphold the territorial integrity of neutral States across all worldwide conflicts, acknowledging that the fundamental principles of the law of neutrality will hold true regardless of the length and severity of a war on a global scale."[104] The significance of this can be

---

[94] Article 8 of Hague Convention (V).
[95] *Ibid*., supra at 45.
[96] Article 9 HC V and XIII.
[97] Brown, Philip Marshall. "Malevolent Neutrality." The American Journal of International Law, vol. 30, no. 1, 1936, pp. 88–90.
[98] *Ibid*., supra 45.
[99] Article 7 of Hague Convention (V).
[100] Boyle, Ashley S. Moving Towards Tallinn: Drafting the Shape of Cyber Warfare. American Security Project, 2012.
[101] *Ibid*., at 73.
[102] Hershey, Amos S. "Neutrality and International Law." International Journal of Ethics, vol. 26, no. 2, 1916, pp. 168–76.
[103] Kennedy, Craig. "SWEDEN: THE ALIGNED NONALIGNED." A Hard Look at Hard Power:, Strategic Studies Institute, US Army War College, 2020, pp. 293–326.
[104] Mohan B. Gazula, "Cyber Warfare Conflict Analysis and Case Studies", Massachusetts Institute of Technology, 2017, pp. 28-87.

understood by ICJ's Nuclear case.[105] Belligerents are forbidden from carrying out any operations or using their privileges against an impartial nation or on their soil, among other things. Additionally, they are not allowed to set up bases of operations there or transport personnel, weapons, or materials across it.[106] These restrictions are stated and are regarded as having a customary nature.[107]

The start of hostilities is governed by HC III Relative to the Opening of Hostilities. A notification of the occurrence of a state of conflict must be delivered through telegraph to neutral powers, although it is not applicable to them once they receive it.[108] However, the neutral powers cannot depend on the defense that they weren't given notice if it is established beyond the realm of possibility that they had knowledge of the presence of a combat situation.[109] These clauses will restrict the use of neutrality legislation to cyberwarfare. No State has admitted liability for any cyberattacks yet. It would be necessary to identify the States engaged in the battle if a cyberattack progresses to the point of becoming a cyberwar.[110] Even if a cyberattack is classified as an "armed attack," the attacker's identity is typically unknown. The law of neutrality would not apply in this situation since the neutral State would not be conscious of a military conflict.[111]

When there is a cyber operation against a neutral state, the belligerents are prohibited from "the utilization of network-based tools to interfere with, reject, undermine, modify, or delete data."[112] Conflicting parties must, alternately, "refrain from taking conduct that might, if deliberately approved by either Power, be an infringement of neutrality when on neutral land or in water bodies, and that "[a]ny act of aggression is a breach of neutrality and is therefore prohibited."[113] Cyber actions that "encourage a foe's trust in their ability to safeguard them"[114] would be considered a forbidden perfidious act that violates international humanitarian law, betrays it, and

---

105 Warf, Barney. "Geographies of Global Internet Censorship." GeoJournal, vol. 76, no. 1, 2011, pp. 1–23.
106 "The Oxford Process on International Law Protections in Cyberspace: a compendium", Oxford institute for ethics, law and armed conflict, pp. 77-121
107 Articles 1, 2, and 3 of HC V and 1, 2, and 5 of HC XIII.
108 Döge, Jenny. "Cyber Warfare. Challenges for the Applicability of the Traditional Laws of War Regime." Archiv Des Völkerrechts, vol. 48, no. 4, 2010, pp. 486–501.
109 Hobbs, Carla, editor. EUROPE'S DIGITAL SOVEREIGNTY: FROM RULEMAKER TO SUPERPOWER IN THE AGE OF US-CHINA RIVALRY. European Council on Foreign Relations, 2020.
110 Sherman, Gordon E. "The Neutrality of Switzerland." *The American Journal of International Law*, vol. 12, no. 4, 1918, pp. 780–95.
111 Borchard, Edwin. "War, Neutrality and Non-Belligerency." The American Journal of International Law, vol. 35, no. 4, 1941, pp. 618–25.
112 Ibid., supra at 63.
113 Ibid., supra at 45.
114 Nasu, H, "The Laws of Neutrality in the Interconnected World: Mapping the Future Scenarios, in The Future of Law of Armed Conflict." Oxford University Press."

causes the enemy's harm, death, or arrest."[115] A belligerent would be breaking the Geneva Convention if they used their logo in their scams.[116]

IV: REMEDIES TO VIOLATIONS

Neutral States have an implied duty to consent to and allow the execution of the belligerents legal remedies. A belligerent hostile act against a neutral state, such as a cyber action against its area or cyberinfrastructure, or a violation of the neutral state's territorial inviolability, such as a cyberoperation from its territory or cyberinfrastructure, can give rise to the right and obligation of the aggrieved neutral state to seek redress. If the neutral State breaches its commitments, the right of the aggrieved belligerents to put into effect the law of neutrality enters into force. The available remedies are countermeasures, restorative justice, and reparations. There are a few general needs for any remedy.[117] The most fundamental ones are the recognition of an infringement of the law of neutrality,[118] the request for the nation in question to uphold its duties,[119] and the termination of any kind of punitive response after the breach has been remedied.[120]

3.1. Reparations:

A typical reaction to a breach of the law of neutrality has been an outright complaint of the breach against the offenders and a call for the "cessation of the infractions as well as certain form of restitution, for example through diplomatic channels.[121] Any State that has been the victim of an international law infringement is entitled to compensation, according to the rules of customary international law. Reparations can take many different forms, such as restitution, recompense, or satisfaction.[122] The US Army Air Forces' 1944 bombing of Schaffhausen, Switzerland, is yet another example.[123] It has always been an issue of dispute to determine how much compensation a State is entitled to.[124] Given how challenging and contentious it is to determine the costs and

---

[115] Article 37, ibid., supra at 53.
[116] International Committee of the Red Cross (ICRC), Rule 61, available at https://ihl-databases.icrc.org.
[117] Sean Cordey and Kevin Kohler, "The Law of Neutrality in Cyberspace", Center for Security Studies (CSS), ETH Zürich, CYBERDEFENSE REPORT, 2021, pp 50-52.
[118] Anderson, Steven J. "Hypothesizing a Cyber-Power Targeting Theory." Airpower Lessons for an Air Force Cyber-Power Targeting Theory, Air University Press, 2016, pp. 87–130.
[119] Corfu Channel, United Kingdom v Albania, ICJ, Rep 244, ICGJ 201 (ICJ 1949), p. 18.
[120] Ibid., supra at 81.
[121] Brown, Philip Marshall. "International Law Reparations." The American Journal of International Law, vol. 28, no. 2, 1934, pp. 330–34.
[122] Ibid., supra at 98.
[123] Articles 37 and 35 ILC ASR, HC IV, and AP 1
[124] Noam Neuman, "Neutrality and cyber space bridging the gap between theory and reality", International law studies, vol. 97, 2021 pp.768-798.

damages caused by cyberattacks, this will undoubtedly hold true in the cyber domain as well. According to *jus angary*[125] a belligerent is permitted to use or destroy vessels, transmission lines, railway stations, that are owned by a neutral company or private individual in the event of an armed emergency.[126] The criterion is that it gives adequate compensation for it, which is typically understood as total restoration of the pre-battle state of affairs.[127]

3.2. Retorsion:

Retorsion is the term for hostile actions that do not violate international law and therefore may be used whenever necessary. When other remedies are not possible (for example, as a result of proportionality) or are inappropriate from a political standpoint, retorsion may be helpful. Examples of this include designating someone as *persona non grata*, breaking off bilateral relations, rescinding economic concessions, or dissolving trade ties.[128] Examples of cyber-specific retorsion include notifying foreign cyber operatives, keeping track of hostile cyber activity on a system using "honeypots," and decreasing hostile cyber activity carried out by other States.[129]

3.3. Countermeasures:

Countermeasures are remedies that would be illegal under international law if they weren't proportionate "self-help"[130] actions intended to stop another State from acting illegally or, in some situations, to obtain compensation. A belligerent may not resort to acts of reprisal or retaliation against a neutral State except for illegal acts of the latter."[131] "The possibility of taking urgent counter-measures is particularly relevant in cyberspace, given the widespread use of concealment procedures and the difficulties of traceability."[132] Estonia was the very first nation to specifically state in its 2019 legal position that a State can carry out cyber countermeasures on behalf of, or in concert with, a State facing illegal cyber operations."[133] Moreover, "countermeasures cannot

---

125 Jennings, W. I. "The Right of Angary." The Cambridge Law Journal, vol. 3, no. 1, 1927, pp. 49–58.
126 Ibid., supra at 45.
127 Norwegian Shipowners' Claims, Norway v United States, Award, (1922), ICGJ 393 (PCA) 1922.
128 Roberto Echandi. "Non-Compliance with Awards: The Remedies of Customary International Law." Proceedings of the Annual Meeting" (American Society of International Law), vol. 106, 2012, pp. 118–22.
129 Johnson, Durward E., and Michael N. Schmitt. "Responding to Proxy Cyber Operations Under International Law." The Cyber Defense Review, vol. 6, no. 4, 2021, pp. 15–34.
130 France (2019), "International Law applied to Operations in Cyberspace", p. 7.
131 Tsagourias, Nicholas. "THE SLOW PROCESS OF NORMATIVIZING CYBERSPACE." AJIL Unbound, vol. 113, 2019, pp. 71–75.
132 Kilovaty, Ido. "Rethinking the Prohibition on the Use of Force in the Light of Economic Cyber Warfare: Towards a Broader Scope of Article 2(4) of the UN Charter." Journal of Law & Cyber Warfare, vol. 4, no. 3, 2015, pp. 210–44.
133 Waxman, Matthew C. Cyber Strategy and Policy: International Law Dimensions". Council on Foreign Relations, 2017.

infringe on essential basic responsibilities like the use-of-force ban."[134]

V. CONCLUSION:

In conclusion, the application of the law of neutrality to cyberspace presents both barriers and opportunities. While the law of neutrality was originally formulated to regulate traditional armed conflicts and maintain impartiality among belligerent parties, its application to the rapidly evolving domain of cyberspace requires careful consideration and adaptation.

On one hand, applying the law of neutrality to cyberspace can help establish guidelines and norms for state behavior in the cyber realm. It can promote restraint, reduce the risk of escalation, and prevent the indiscriminate use of cyber capabilities during conflicts. Neutrality principles, such as the prohibition on targeting civilian infrastructure, can serve as a foundation for developing cyber-specific rules and promoting responsible state conduct. By incorporating neutrality principles into cyber doctrines and policies, states can foster a more stable and secure cyberspace environment. On the other hand, it also faces significant restrictions due to the unique characteristics of the domain. Unlike traditional warfare, cyberspace operates in a borderless and interconnected manner, where attribution and the distinction between civilian and military entities can be blurred. Moreover, the asymmetrical nature of cyber capabilities often means that non-state actors and private entities play a significant role, making it difficult to apply traditional state-centric concepts of neutrality.

To effectively apply the law of neutrality to cyberspace, there is a need for global cooperation, dialogue, and consensus-building among states, private sector actors, and civil society. The development of cyber-specific norms and rules should take into account the evolving technological landscape and the changing nature of conflicts. Multi Stakeholder approaches that involve various actors can help address the complexities of cyberspace and ensure that neutrality principles are adapted and applied in a manner that upholds both security and human rights.

[134] Hitchens, Theresa, and Nilsu Goren. International Cybersecurity Information Sharing Agreements. Center for International & Security Studies, U. Maryland, 2017.