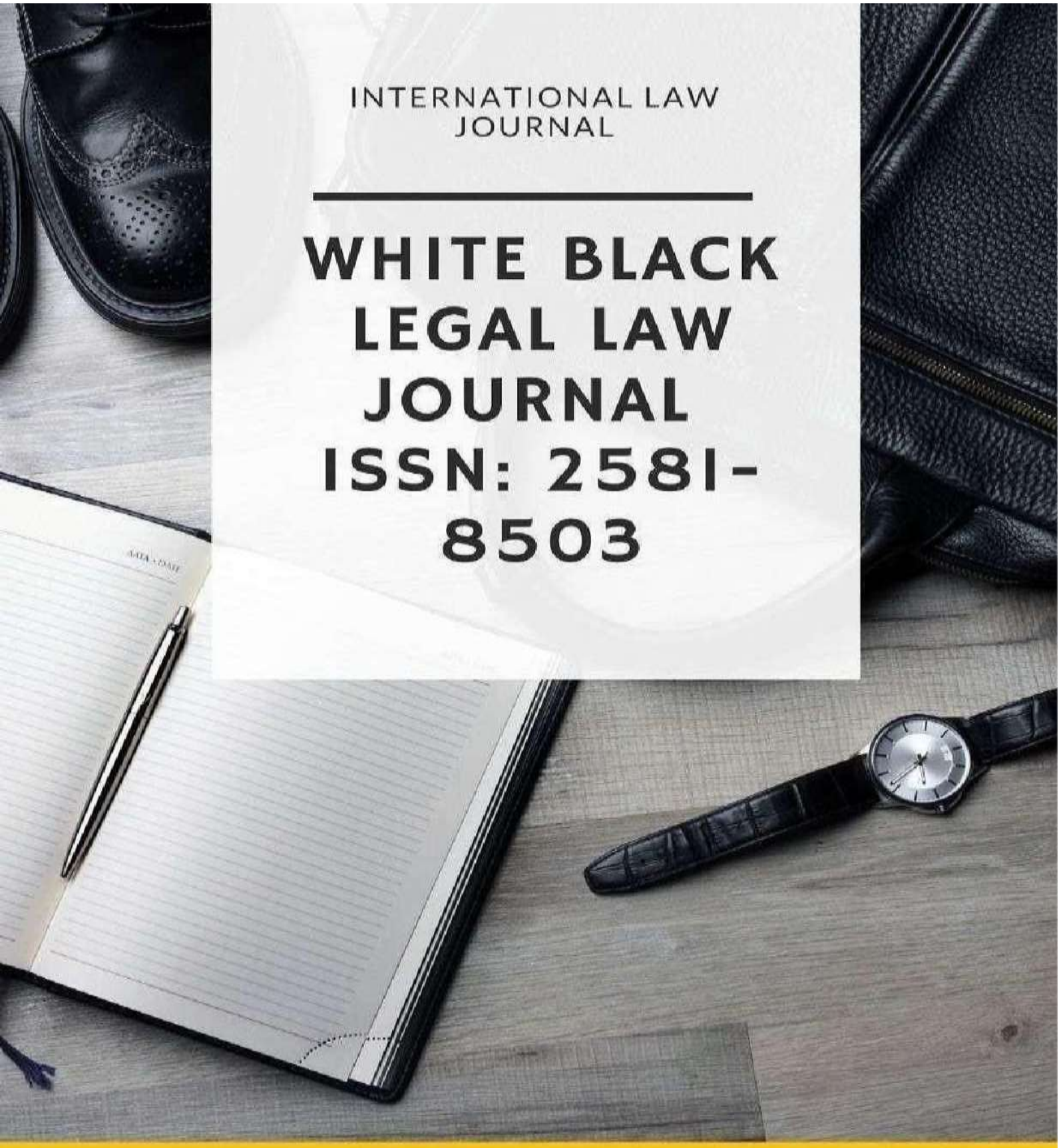

INTERNATIONAL LAW JOURNAL

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.

WWW.WHITEBLACKLEGAL.CO.IN

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 a professional diploma in Public 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

www.whiteblacklegal.co.in
Volume 3 Issue 1 | March 2025 ISSN: 2581-8503

REVISITING THE EFFECTIVE CONTROL TEST IN THE LIGHT OF CYBER ATTACKS

AUTHORED BY - SUNIDHI S. HEGDE

Abstract

The increasing reliance of human society on the Internet has led to new forms of state-sponsored attacks including in cyberspace. This paper delves into the complexities of attributing state responsibility in international law, particularly in the context of cyber warfare. It discusses the challenges posed by the evolving nature of cyber threats and the inadequacies of the existing legal framework of attribution through the effective control test established by the International Court of Justice. A careful study of the degree of control established by the ICJ in Nicaragua case and the Bosnia Genocide case as opposed to the ICTY decision in the Tadic case, shows the different standards existing in International Law. The analysis highlights the need for a more flexible standard of attribution to hold state sponsors of cyber-attacks accountable, proposing the adoption of the overall control standard. This standard would enable accountability based on evidence beyond a reasonable doubt, rather than requiring absolute certainty of state control over non-state actors. Drawing from the precedent set by the ICJ in the Iran hostage case, the paper argues for extending the application of vicarious liability to cyber-attacks orchestrated by citizens acting under governmental direction. However, it acknowledges the challenges of adopting a lower burden of proof, including the risk of prosecuting innocent states. The paper emphasizes the importance of addressing these concerns and identifies the need for further research on related issues. Overall, it underscores the significance of evolving legal frameworks and international cooperation in promoting cybersecurity and upholding the rule of law in cyberspace.

Keywords: *attribution, cyber-attacks, effective control, International Court of Justice, state responsibility*

Introduction

In an era where the absolute power of States faces challenges on various fronts, upholding State responsibility remains crucial for global security. However, establishing a coherent framework to delineate State responsibility within international law has proven to be a challenging task. Despite the rise in instances of State-sponsored terrorist activities since the conclusion of the Cold War, attributing responsibility for such acts remains immensely challenging.[1] This challenge is compounded in cyberspace due to the rapidity and anonymity associated with cyberattacks, making it challenging to differentiate between the actions of terrorists, criminals, and nation-states, as noted by the White House.[2]

Due to the covert nature of cyberspace, States might encourage civilian groups within their territories to carry out cyber-attacks. They could then shield themselves behind a thin veil of plausible deniability, allowing them to evade accountability for these actions. Thus, it becomes essential to look into whether the existing principle of International law would be effective in tackling the challenges of cyber-attacks.

The Principle of State Responsibility

The principle of State responsibility is a well-established Customary International Law established through numerous precedents[3] and conventions, like *Nicaragua judgement*[4] and *Wimbledon judgement*[5] stipulating that a state is to be held accountable for the breach of its commitments to another state. The International Law Commission in Draft Articles on Responsibility of States for Internationally Wrongful Acts 2001[6] has codified this principle which has been heavily relied upon by the International Court of Justice and the international tribunals as an authoritative source laying out Customary International Law in cases like *Bosnia and Herzegovina v Serbia and Montenegro*.[7]

[1] Burgess, D. R., 2006. Hostis Humani Generi: Piracy, Terrorism and a New International Law, University of Miami International and Comparative Law Review, 13, 293-312.
[2] White House 2003. National Strategy to Secure Cyberspace, 19.
[3] Factory at Chorzow (Germany v. Poland), Judgement, 1927 PCIJ Series A No. 9, at 21; *See also* Velásquez Rodríguez v. Honduras case, IACtHR Series C No. 4, ¶ 170 (1988).
[4] Military and Paramilitary Activities in and Against Nicaragua (Nicaragua. v. U.S.), 1986 I.C.J. 14, (June 27).
[5] The S.S. Wimbledon (1933) Annual Digest of Public International Law Cases. Cambridge University Press, 2, pp. 193–193, ¶ 30.
[6] International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, Report of the International Law Commission on the Work of Its Fifty-Third Session, U.N. Doc. A/56/10 (2001) [hereinafter ILC Report].
[7] Bosnian Genocide case (Bosnia and Herzegovina v Serbia and Montenegro), Judgement [2007] ICJ Rep 91.

While Cyberspace is a novel field of study in international law, the United Nations General Assembly (UNGA) and the UN Group of Governmental Experts on Information Security have developed the concept of State Responsibility in Cyberspace, offering guidelines for acceptable behaviour by governments in the field of cybersecurity.[8]

Further, the law on state responsibility is extended to cyberspace by the International Group of Experts in the Tallinn Manual 2.0. Article 2 of the ILC Draft and Rule 14 of Tallinn Manual[9] provides that the essentials for state responsibility of an internationally wrongful act include: (a) *When conduct consisting of an action or omission is attributable to the state under international law*, and (b) *constitutes a breach of an international obligation of the state.* The conditions of attribution in several situations have been elucidated in ARSIWA and the Tallinn Manual.

Attribution

Attribution in international state responsibility refers to the process of identifying and assigning accountability to a state for its actions or omissions under international law. It is a crucial aspect of holding states accountable for violations of international obligations, such as committing acts of aggression, human rights abuses, or cyberattacks. Attribution involves determining whether the state directly perpetrated the wrongful act, supported or encouraged non-state actors in carrying out the act, or failed to prevent the wrongful act from occurring despite having the capacity to do so. However, attribution can be challenging, especially in cases where states attempt to conceal their involvement or where the nature of the act, such as cyber warfare, involves anonymity and deception. Despite these challenges, attribution is essential for maintaining international peace and security, ensuring justice for victims, and upholding the rule of law in the international community. As held in the *German Settlers case*, States can act only by and through their agents and representatives and a State should be responsible only for those actions. International Law generally applies this to organs of the State. However the attribution gets difficult when the entity in question is not an organ but an autonomous unit or owned privately. ARSIWA answers these problems with Articles 5 and 8

[8] UN GGE 2013 Report, ¶ 20; UN GGE 2015 Report, ¶ 27, 28(b).
[9] Talinn Manual 2.0 on the International Law Applicable To Cyber Operations (Michael N. Schmitt ed., 2d ed. 2017), [hereinafter Talinn Manual 2.0].

holding actions of autonomous entities exercising governmental functions and private entities responsible respectively.[10]

Effective Control Test

As a fundamental principle, the actions of private individuals or entities typically do not attribute responsibility to the State according to international law. However, there are instances where such actions can be attributed to the State due to specific factual connections between the individual or entity and the State itself. Article 8 of ARSIWA[11] addresses two scenarios where this may occur. The first scenario involves private individuals carrying out wrongful actions under the direct instructions of the State. The second scenario encompasses situations where private individuals operate under the direction or control of the State in a broader sense. In both cases, it is crucial to consider the principle of effectiveness in international law, ensuring that there is a genuine link between the individual or group acting and the State apparatus.

The position of ILC is that the State can be held responsible when the specific operation of the entity is directed or controlled by the State and this shall not be applicable if the actions were incidental or peripherally associated with the operation which is outside what the State directed or controlled. The degree of this control as held by ICJ in *Nicaragua case* is very high to mean 'effective control' which was later considered by the court in the *Bosnia Genocide case* as the appropriate test in dealing with attribution.

This test is particularly relevant in cases where a state may seek to avoid responsibility for the actions of groups or individuals operating within its territory but not directly under its formal control. According to the test, the state can be held accountable if it exercises effective control over the non-state actor or group involved in the wrongful conduct. Effective control implies a level of influence or authority by the state over the actions of the non-state actor, to the extent that the state can prevent or direct their actions. Factors such as financial support, training, provision of resources, coordination, and overall supervision are considered in determining the extent of this control.[12] The ICJ has applied this test in various contexts, including cases

[10] ILC Reports, *supra* note 6.
[11] Id.
[12] Military and Paramilitary Activities in and Against Nicaragua (Nicaragua. v. U.S.), 1986 I.C.J. 14, (June 27).

involving armed conflicts, human rights violations, and state-sponsored terrorism, to ascertain state responsibility for the actions of non-state actors.

The ICJ has time and again considered this test to be the Customary International Law in terms of the ambit of Article 8 of ARSWIA. It has further rejected a broader 'overall control' test applied in the *Tadic case*[13] stating-

> *"the "overall control" test has the major drawback of broadening the scope of State responsibility well beyond the fundamental principle governing the law of international responsibility: a State is responsible only for its own conduct, that is to say the conduct of persons acting, on whatever basis, on its behalf... the "overall control" test is unsuitable, for it stretches too far, almost to breaking point, the connection which must exist between the conduct of a State's organs and its international responsibility."*[14]

However, the development of newer modes of attacks has led to a problem of attribution where the States could hide behind the veil of entities that require no control, direction or active involvement of the State to launch attacks on behalf of States, thereby escaping liability due to the application of the effective control test. One such possible area is cyberspace, where the existing principles of International Law need to be revisited to check their feasibility.

Cyber Warfare

In recent times, with the rapid development in technology, cyber-attacks have become increasingly common, capable of shutting down nuclear centrifuges, electrical grids, and defence systems. As they pose a grave threat to national security, they must be classified as acts of war which would come within the application of International Law. One of the major attacks so far has been the 2010 Stuxnet attack where a computer worm was used to bring Iran's nuclear program to a halt through sophisticated attacks on the nuclear centrifuges, which appeared to have been launched by states across the world.[15] This was followed by an attack turning off the Internet in Burma preceding the country's election.[16] Later in 2011, evidence surfaced about a suspected government-backed cyber-attack initiative in China. A

[13] Prosecutor v. Dusko Tadic (Appeal Judgement), IT-94-1-A, International Criminal Tribunal for the former Yugoslavia (ICTY), 15 July 1999, ¶ 117.
[14] Bosnian Genocide case (Bosnia and Herzegovina v Serbia and Montenegro), Judgement [2007] ICJ Rep 91.
[15] Jonathan Fildes, Stuxnet Worm 'Targeted High-Value Iranian Assets,' BBC NEWS (Sept. 23, 2010, 6:46 AM), http://www.bbc.co.uk/news/technology-11388018.
[16] Burma Hit by Massive Net Attack Ahead of Election, BBC NEWS (Nov. 4, 2010, 3:33 PM), http://www.bbc.co.uk/news/technology-11693214.

documentary aired on China Central Television, a state-run broadcaster, seemingly captured a distributed denial of service attack being conducted by the Chinese military on a Falun Gong website based in Alabama. This revelation came shortly after a report by the cybersecurity company McAfee, which indicated that a 'state actor,' widely presumed to be China, had been involved in a prolonged cyber-attack campaign targeting various governments, U.S. corporations, and United Nations entities.[17] Many scholars have referred to these attacks as cyberwarfare, suggesting that the law of war might apply. But these are significantly different from the nature of armed conflict for conventional doctrines to be applicable.

Attribution Challenges in Cyberspace

The Tallinn Manual 2.0[18] and the UN GGE Reports of 2013 and 2015 on ICT[19] have extended the existing law to cyberspace including the principle of State responsibility established in ARSIWA. However, the nature of cyberspace is such that it cannot be equated with conventional means of attacks and thus creates a need to relook into the existing principles of attribution.

Despite significant advancements in technical capabilities for cyber attribution, the legal framework surrounding cyberattack attribution remains largely undefined due to several reasons. One primary challenge is the deliberate efforts of attackers to conceal their identities or mislead investigators, making attributions difficult and time-consuming. Even when the machines or IP addresses responsible for cyberattacks are identified, linking them to a specific state is often complex and may require extensive intelligence and police work. Furthermore, there is a lack of consensus on the standards of proof, public attributions, and the legal consequences of attribution, hindering efforts to establish clear international legal rules for cyber operations targeting civilians and infrastructure.[20]

As a result, some states can exploit the ambiguity surrounding cyber attribution to conduct attacks with impunity, knowing that the repercussions may be limited to mere diplomatic condemnations. However, the increasing sophistication of cyber threats, capable of causing

[17] David Barboza & Kevin Drew, Security Firm Sees Global Cyberspying, N.Y. TIMES, Aug. 3, 2011, at A11.
[18] TALINN MANUAL 2.0, *supra* note 9.
[19] UN GGE 2013 Report, ¶ 20; UN GGE 2015 Report, ¶ 27, 28(b).
[20] Jordan Robertson & Michael Riley, *Mysterious Turkey Pipeline Blast Opened New Cyberwar*, BLOOMBERG (Dec. 10, 2014), https://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar.

significant harm and even catastrophic damage, underscores the importance of accurately identifying and attributing cyber intrusions.[21] Failure to do so not only perpetuates risks of confusion and escalation but also exacerbates the potential for destructive conflicts between states. Therefore, confident attribution of cyber intrusions and the establishment of agreed-upon norms limiting such actions are essential for maintaining stability and security in cyberspace.[22]

Without clear and universally accepted rules and practices for attributing cyberattacks, there is nothing to prevent attackers in cyberspace. Due to the inherent difficulties and time-consuming nature of cyber attribution, when state involvement is suspected, international law puts states in a difficult position when responding to cyber intrusions that fall below the threshold of the use of force. Essentially, the lack of transparent and widely shared attribution mechanisms leaves states unable to effectively hold perpetrators accountable for their actions in cyberspace. This creates a situation where attackers face minimal consequences for their behavior, which in turn perpetuates the cycle of cyber threats and attacks. Thus, establishing transparent and widely accepted attribution rules and practices is crucial for deterring malicious actors and fostering a safer cyberspace environment.

Need for Change

Having established the nature of cyberspace which makes attribution challenging, extending the effective control test of the ICJ to cyber militias would imply that state sponsors of cyber attacks would only be held accountable if their effective control could be definitively proven. Given the substantial technical challenges in identifying the perpetrators of cyber attacks due to the intricacies of the internet's architecture, such a stringent standard would essentially provide immunity to state sponsors of cyber attacks. In a complex global cyber attack, even the absence or alteration of certain data commands could be enough to undermine claims of state control and evade accountability.[23] Without the adoption of new techniques like the probabilistic tracing project mentioned earlier, or in cases involving less sophisticated hackers, proving effective control would render state responsibility for cyber attacks nearly impossible to establish.

[21] U.S. Department of Defense, Cyber Strategy Summary 1 (2018), https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.
[22] Willian Banks, *Cyber Attribution and State Responsibility*, 2021, International Law Studies, The Stockton Centre for International Law Vol. 97.
[23] Id.

In the absence of any treaty specifically addressing cyberspace or the implementation of the ICTY's overall control standard, there exists a precedent within the ICJ framework to support a more flexible standard of State responsibility. In the *Iran hostage case*,[24] the ICJ ruled that a State could be held responsible if its citizens, acting on behalf of the government, carried out specific operations. While the court did not attribute the citizens' actions directly to the government, it found the government liable for failing to fulfill its obligations to protect foreign diplomatic staff. This reasoning could be applied to cyber attacks in two ways: either holding the government vicariously liable for attacks orchestrated by its citizens acting under governmental direction, or holding the government accountable for its awareness of international obligations regarding cyber-attacks. Such an approach moves beyond the rigid effective control framework and enables the accountability of state sponsors when significant evidence of involvement exists.

This tackles the problem created by reliance solely on the effective control standard which allows governments to conceal their involvement in cyber operations too easily. Therefore, it may be more appropriate under international law to prove overall control by a government in a cyber attack, rather than requiring complete control. Utilizing the ICJ precedent of the Iran hostage case offers another avenue for holding state sponsors of cyber attacks accountable.

However, adopting a standard of State responsibility with a lower burden of proof than effective control raises concerns about potentially prosecuting innocent states. Addressing these concerns may involve clarifying that the burden of proof remains high even under the overall control standard. Other issues include determining the appropriate forum for prosecuting state sponsors of cyberattacks, whether through the ICJ, national courts, or specialized tribunals.

Conclusion

As human society becomes increasingly reliant on the Internet, it becomes imperative to develop the capabilities to deter, detect, and mitigate the impact of cyber-attacks. The International Community is working on how to govern cyberspace effectively, which includes shaping the legal framework for cyber warfare from its inception. Due to the technical challenges in proving attribution for cyber-attacks and the high burden of proof imposed by

[24] United States Diplomatic and Consular Staff in Tehran U.S. v. Iran, 1980 I.C.J. 3, 29 May 24.

the effective control standard laid by the ICJ, there is a need to change the existing principle of attribution and lower the degree of control required for holding a State responsible. This reduced standard holds State sponsors accountable when sufficient evidence exists beyond a reasonable doubt, rather than requiring absolute certainty. However, determining a standard for State responsibility is just one aspect of promoting cybersecurity. Other related issues, such as identifying the appropriate forum for prosecuting State sponsors of cyber-attacks, require further research and attention from scholars and policymakers.

References