THE CYBER WARFARE AND THE LAW OF ARMED CONFLICT

Mr. Abhishek Singh[1]

Dr. Devanshi Singh[2]

[1] LLM Research Scholar, School of Law, Galgotias University
[2] Assistant Professor at School of Law, Galgotias University, Greater Noida, UP India

ABSTRACT

The rapid expansion of cyberspace has introduced new challenges to the traditional frameworks governing warfare, particularly the Law of Armed Conflict (LOAC). This paper explores the intersection of cyber warfare and LOAC, focusing on the applicability of existing legal principles to cyber operations. It critically examines whether cyber operations, including cyberattacks and cyber espionage, can be classified as "armed attacks" under LOAC, and how principles such as distinction, proportionality, and necessity apply in the context of cyber operations. The paper also discusses the difficulties in attributing cyberattacks to specific states or actors, highlighting the challenges of ensuring accountability in cyberspace. Furthermore, the role of international law, including the United Nations Charter, customary international law, and regional approaches, in regulating cyber warfare is analyzed. The study suggests that while LOAC provides a foundational framework, significant gaps remain in its application to cyber warfare. The paper concludes by recommending the development of global norms, strengthened international cooperation, and mechanisms for accountability to address the growing threats posed by cyber warfare.

Keywords

Cyber Warfare, Law of Armed Conflict (LOAC), Cyber Operations, Attribution Challenges, International Law, State Sovereignty, Cybersecurity, United Nations Charter, Customary International Law, Cyber Norms, International Cooperation, Cyberattack Accountability, Proportionality and Necessity.

INTRODUCTION

The invention of cyber technologies has revolutionized the nature and face of warfare by moving the warfare-centric focus from terrestrial landscapes to cyberspace. Cyber warfare refers to planned cyber operations. Strategized cyber operations are performed for achieving definite military and political objectives, which is not possible in traditional kinetic warfare. These operations might target critical infrastructure, communication networks, or state security systems. It can be clearly seen that cyberspace has evolved into an integral domain in modern conflicts. The shift from traditional war into cyber warfare demands reconsideration of the extent to

[1] LLM Research Scholar, School of Law, Galgotias University
[2] Assistant Professor at School of Law, Galgotias University, Greater Noida, UP India

which existing legal structures evolve to meet this new norm.

Cyber warfare has imposed novelties that make it difficult to categorize under the conventional understanding of war or peace. Unlike conventional war, cyber operations occur in a gray zone where attribution is likely not certain because states can always deny involvement. That makes it harder than it already was to apply the LOAC, which demands bright line distinctions between, for example, combatants and civilians as well as thresholds before an armed attack occurs. Such events, like the coordinated cyberattacks on Estonia back in 2007, stand as examples of how states can use cyber technologies to undermine their opponents without breaching the classical limits of war.

Whether international law will be able to become flexible with cyber conflicts remains a highly debated issue. LOAC, which designed to control physical combat, has no reference to cyber warfare issues. New meanings must now be found for proportionality, necessity, and distinction in regard to cyber attacks. For example, the Stuxnet operation on Iran's nuclear plants elicited debates over whether such activities constitute an armed attack in international law. This, in turn, leads to a greater necessity for a more holistic legal framework governing state behavior in cyberspace.

Until date, the problem of attribution has remained one of the most important deterrents of cyber warfare. Cyber attacks are characteristically conducted with anonymity or under proxies, making it difficult to hold perpetrators liable under international law. Factually, responsibility and the justification of responsive actions-perhaps diplomatic, military, or other-rely on a credible process for the attribution of actions. In case no clear attribution process is followed, escalation or miscalculations in cyberspace remain highly fraught, making it doubly difficult to enforce LOAC.

The specific context of cyber warfare thus demands international efforts to update the existing legal instruments or devise new frameworks in light of the digital age. For this purpose, clarifying the traditional principles of international humanitarian law on cyber operations should be further conducted with global norms in relation to state conducts in the cyberspace. Collective work, such as the Tallinn Manual on the International Law Applicable to Cyber Warfare, is part of this effort. Agreement on these matters would balance state sovereignty with the growing need for collective security in an increasingly interdependent world.

CONCEPTUALIZING CYBER WARFARE

A key distinction that sets cyber warfare apart from conventional armed conflicts lies in its reliance on the digital domain and its inherent capacity for covert execution. Conventional attacks typically require direct physical proximity to launch. Consequently, cyber operations can be executed remotely and often without any notice, therefore allowing great stealth. The attacker can infiltrate systems, exfiltrate sensitive data, or

disrupt critical infrastructure with less direct physical damage.[3] Cyber attacks are very fast and scalable and, therefore, become very potent ones for achieving strategic objectives, thus challenging such traditional defense mechanisms prepared to meet the requirements of physical combat.

Cyber warfare is absolutely beyond the military to civilian regimes since, when considering the regime, the distinction fades between the military and nonmilitary targets. Increased vulnerabilities of critical sectors, such as energy grids, financial systems, health care, and communications networks reveal what potential damage capacities from cyber operations are. An example to look at will be the 2017 global health service disruption by ransomware WannaCry.[4] Such incidents reflect the need for enhancing cybersecurity measures by governments and organizations to protect vital assets.

This is one of the greater challenges in tackling cyber warfare: attacks are oftentimes very difficult to attribute. Many cyber operations use anonymization techniques, proxy servers, and decentralized networks that make it rather difficult to identify the perpetrators. Lack of clarity only fuels obfuscation of accountability and complicates the understanding and enforcement of international norms. For example, the 2014 Sony Pictures hack raises questions about the extent to which North Korea, accused of perpetrating the hack, can be held responsible. The lack of good attribution mechanisms may increase the risk that retaliation is based on incomplete evidence and could lead to escalations.

Cyber operations in war certainly pose a legal and ethical dilemma very different from the current international legal framework-in other words, the United Nations Charter and the Law of Armed Conflict, originally designed with conventional warfare in mind, contain no reference to cyber operations[5]. Those are gaps that provide ample room for ambiguity: states are unsure what constitutes an armed attack, proportionality's implications on responses, and whether the actions violate sovereignty. The ethical plane demands closer attention because prospecting indiscriminate damages to non- combatants and reliance on unregulated digital tools must be better understood with the support of new norms on cyber engagements.

Typology of cyber operations

1) *Offensive Cyber Operations:* This includes such offensive cyber operations, which are actions taken using adversary systems and networks in an attempt to disrupt, degrade, or destroy systems or networks. Such attacks may be against military communication systems, critical infrastructure, or financial networks. For instance, the 2010 Stuxnet attack is a strategic use of offensive cyber tools against Iran's nuclear program[6]

[3] *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Michael N. Schmitt ed., Cambridge Univ. Press, 2d ed. 2017)
[4] U.K. National Audit Office, *Investigation: WannaCry Cyber Attack and the NHS* (Oct. 2018), available at: https://www.nao.org.uk/report/investigation-wannacry-cyber-attack-and-the-nhs/.
[5] U.N. Charter arts. 2(4), 51; see also Schmitt, supra note 1, at 113–15.
[6] Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon* (Crown Publ'g 2014).

2) *Defensive Cyber Operations DEF:* Cyber operations employ the term to mean protection and safeguarding of systems against unauthorized access, data breaches, or sabotage. It normally involves network monitoring, deployments of countermeasures, and responses to live cyberattacks.

The Distinction between Cybercrime, Cyber Terrorism, and Cyber Warfare

Terms such as "cybercrime," "cyber terrorism," and "cyber warfare" are often confused, but in international law, there are distinct concepts.

Cybercrime refers to unlawful deeds carried out through cyberspace, like fraud or identity theft hacking, amongst others, for monetary profits. Cyber Terrorism refers to applying pressures or threats to populations or governments but primarily using cyber weapons for achieving an ideological or political agenda. Cyber Warfare refers to State-organized or state-sponsored activity intended to use cyber operations for military or strategic purposes in the course of an armed conflict in order to realize such purposes.

THE LAW OF ARMED CONFLICT (LOAC): AN OVERVIEW

The LOAC is designed to have the fundamental principles balancing technical requirements of military operation with humanitarian considerations. The principle of distinction, proportionality, and necessity play a very important role in LOAC. In fact, the principle of distinction would require parties to a conflict to distinguish between combatants and civilians during the military operation so that only legitimate objects would be attacked and not the civilians. Proportionality prohibits attacks where the expected harm to civilians would outweigh the anticipated military advantage.[7] Necessity limits actions to those necessary to achieve military objectives, avoiding unnecessary suffering or destruction. Such principles underscore the objective of LOAC: to limit as much as possible the effects of war on human life and property.

As the nature of warfare has evolved, so too has the concept and application of LOAC. Traditional state- to-state warfare has given way to asymmetric conflict by non-state actors-insurgencies and terrorist groups. The shift has necessarily raised many questions of how LOAC should apply to non-conventional actors and irregular forms of combat. Technological advances like the use of drones and autonomous weapons make the application of LOAC quite complicated, specially if one considers traditional understanding and use in implication of accountability, proportionality, and involvement in hostilities.

Cyber warfare has posed unprecedented challenges, and LOAC's framework faces unprecedented challenges, especially because most cyber operations occur in a blurred legal and operational space, determining who the combatants are, what the military objectives are, and the scale of harm is complex. For example, determining whether a power grid attack by a cyber attack constitutes an armed attack under LOAC is contentious. The principle of distinction also throws a challenge in the context of dual-use targets such as communications infrastructure. This is why there needs to be an international concurrence on which principles of LOAC apply

[7] Id. art. 51(5)(b); see also Yoram Dinstein, *The Conduct of Hostilities Under the Law of International Armed Conflict* 119–20 (3d ed. 2016)

to cyber operations so that humanitarian protections continue working even in a digital world.

Principles of LOAC

1) Distinction

It requires parties to distinguish both combatants from civilians as well as military objectives from civilian objects. As such, this principle should guide cyber operations such that they only target legitimate military objectives and avoid civilian systems unless they are used in support of military activities.

2) Proportionality

The principle of proportionality for the expected incidental loss among civilians and civilian objects cannot be exceeded by the expected military advantage. In cyberspace, this means measuring incidental harm toward cyber operations, such as disrupting critical civilian infrastructure such as hospitals or energy grids.

3) Necessity

Military necessity allows actions that are otherwise prohibited under LOAC if they are those necessary to achieve a legitimate military objective. Cyber operations, like communication systems disabling from an enemy's side, must be strictly limited to the purposes of military objectives.

4) Humanity

This principle forbids unnecessary suffering and sees to it that the means and methods of warfare can never be absolutely unlimited. This principle has the fullest applicability in cyber warfare, wherein operations could produce effects on civilian populations indiscriminately if they are not conducted appropriately.

APPLICABILITY OF LOAC TO CYBER WARFARE

This principle of distinction, one of the central tenets of LOAC, becomes particularly difficult in the context of cyber warfare. The cyber operation attacks dual-use infrastructure; some forms of communication networks or energy grids may both provide civilian and military benefits. The determination of whether such targets could be legitimate under LOAC is tense since attacks on these systems could inadvertently harm a civilian population. It raises an ambiguity problem between civilian and military resources in cyberspace and has the possibility of proportionality and legality issues in cyber operations[8].

As cyber operations are decentralized in nature, the attacks will be even more difficult to attribute to a specific state or non-state actor, which is an issue in terms of how accountability works under LOAC. Traditional warfare does not usually have anonymizing techniques such as proxy servers or false flag operations, involved in cyber operations. Such ambiguity undermines the adherence of LOAC, as attacks can be evaded by attributing them to independent actors or denying responsibility altogether. Mechanisms that enhance accurate attribution

[8] Michael N. Schmitt et al., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge Univ. Press, 2d ed. 2017).

are necessary for the adherence of LOAC in cyberspace.

Consequently, proportionality and necessity, two basic principles which reflect the application of force in real wars, are particularly difficult to apply in cyber-warfare. Cyber attacks often lead to highly unpredictable effects. A given cyber operation aimed at disrupting a military capability may inadvertently cripple civilian services that rely on the same infrastructure. These three obvious potential results conflict with the principle of proportionality; it should minimize harm to civilians proportional to the military advantage gained. The same complexity applies to the principle of necessity in the case of cyber attack, where, for instance, an operation may not easily express its direct military benefit under LOAC.

Although LOAC can be envisioned as technology-neutral, there are controversies that emerge in cyber warfare, gaps for further clarification and regulation. For instance, the Tallinn Manual has attempted to translocate principles of LOAC into cyberspace, which gives insight into how already existing laws might apply to cyber operations; such interpretations, though, do not have binding force and depend on states' willingness and voluntary compliance. This cyber-specific, consensus-driven legal framework would make the vagaries of LOAC practicable in the digital sphere and arrive at humanitarian objectives. International cooperation and dialogue would therefore be important for bridging such gaps and preventing the misuse of cyber capabilities in conflict.

Challenges in Defining "Armed Attack" in Cyberspace

Applying Article 51 of the Charter of the United Nations to operations in cyberspace requires a redefinition of the term "armed attack" in this regard. The traditional definitions have understood an armed attack within the dimension of physical damage and casualties. In space, operations may be credited to attain strategic purposes without direct physical injury. Some examples include disabling any critical infrastructure and destroying the financial markets, plus stealing sensitive information about the government. These cyberattacks may have similar results to traditional military actions and raise questions about whether such non-kinetic effects qualify for consideration under international law as an equivalent to an armed attack.

Most central, though is the question of whether to define a threshold at which a cyber operation would be considered an armed attack. Not all cyber incidents attain the level of an armed conflict. Most of them are categorized under espionage, crime, or nuisance activities. It is unlikely, for example, that a DDoS attack which temporarily denies access to government websites would qualify as an armed attack. Of course, one can argue that knocking out a nation's power grid in one coordinated operation leaving the country chaotic constitutes the threshold. Set standards for articulating what constitutes a large-scale, scope and impact cyber operation in terms of effects are also necessary for fair application of Article 51[9].

Relevant to determining whether a cyber operation amounts to an armed attack are intent and attribution. A state may invoke self-defense only where it can show that the attack is intentional and attributable to another

[9] Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* 329–33 (Cambridge Univ. Press, 2d ed. 2017).

state or actor[10]. Cyber operations, however, typically are shrouded in ambiguities whereby attackers attempt to hide their identities by utilizing tools such as anonymizing tools and third-party servers. This makes it very hard to prove intent or assign responsibility, which becomes a legal and practical barrier to invoking the right to self-defense under Article 51.

State practice remains an essential element in the development of norms in interpreting Article 51 in the context of cyber warfare. At one end of the spectrum, some states have adopted a rather expansive view of what constitutes an armed attack in cyberspace and held that operations causing significant harm to economic stability or national security are subject to a self-defense response. For example, the United States and NATO have stated that significant cyber incidents would, under Article 5 of the NATO Treaty, trigger collective defense[11]. Such developments suggest that an emerging consensus is that the nature of the consequences of cyber operations-including whether they constitute armed attacks-rather than their form, should determine the issue.

International norms in what constitutes an armed attack in cyber would need to be agreed on by the international community to continue maintaining global security and stability. Multilateral initiatives, like the Tallinn Manual, would occur through an examination of how the international law applies across cyber operations, even up to threshold levels for self-defense. Without binding agreements or universally accepted definitions, this breeds uncertainty and the potential for conflicting interpretations. However, to craft a coherent strategy for implementing Article 51 in the cyber domain, conversation among nations is necessary, and that should be based on both legal literature and practitioner cases.

Case Studies: Notable Cyber Incidents and LOAC Considerations

1) *Stuxnet Attack (2010):*

The Stuxnet worm allegedly developed by the United States and Israel attacked Iranian nuclear centrifuges with the aim of causing physical destruction to vital infrastructure. While this operation would have strategic objectives, it raises questions whether it could be entitled as an "armed attack" under LOAC since the attacking in fact directly affected military targets and did not indirectly hit civilian systems.

2) *Russian Cyber Operations Against Estonia (2007):*

Estonia was subjected to a series of DDoS attacks in 2007 against government, financial institutions, and media organizations, allegedly by Russian agents. In such attacks, no physical destruction or loss of life occurs, making it troublesome to classify as an "armed attack" under LOAC. The incident is one example of the difficulties of attribution but also the threshold of LOAC to be applied in cyber warfare.

[10] Stuart Casey-Maslen, *Autonomous Cyber Weapons Under International Humanitarian Law*, 20 J. Int'l Hum. Legal Stud. 1, 11–14 (2022).

[11] North Atlantic Treaty Organization, *Cyber Defence Pledge* (2016) Available at https://www.nato.int/cps/en/natohq/official_texts_133177.htm.

3) *Sony Pictures Hack (2014):*

In 2014, hackers reportedly supported by North Korea broke into Sony Pictures' networks, stole sensitive data and made them public. Hackers, once inside the networks, created some destructive malware on the company to cause damage on its systems and disrupt operations. Although the attack was directed against a private company, its geopolitical motivations, allegedly due to the film The Interview, led to debates on whether such actions could be labeled as a use of force in international law. It had nothing to affect physical structures or directly threaten national security, making it even harder to fit into LOAC, emphasizing the emerging problem of applying traditional legal frameworks when political considerations are involved in cyber incidents.

4) *WannaCry Ransomware Attack (2017):*

This WannaCry ransomware attack in the year 2017 had compromised over 200,000 systems in more than 150 countries and specially affected public and private sector centres like the healthcare services of the United Kingdom. The attack was blamed on a North Korean-linked group. This attack caused vast disruption without very clear military objectives. Where it significantly affected civilian infrastructure, it still was no "armed attack" in LOAC because the consequences still remain more economic and operational than a physical direct attack. Of course, this case really throws light on the problems of LOAC application to incidents of cyber attacks that mainly affect civilian systems, with the state not being directly involved in any kind of military context

ATTRIBUTION CHALLENGES IN CYBER WARFARE

One of the biggest challenges in attribution involving cyber warfare is ensuring anonymity of cyberspace. Attackers can rather easily use tactics that obscure identification by methods including IP spoofing, proxy servers or even routing attacks through multiple jurisdictions. Anonymity complicates the identification of perpetrators and thwarts or delays international law responses. This problem comes from the decentralized nature of the internet, where not tracing how operations originate will be easier without having serious technical and forensic investigation to trace back.[12]

International law, as of the Draft Articles on Responsibility of States for Internationally Wrongful Acts, aims to make states responsible for actions caused by entities within their effective control. In the context of a cyber war, the principle of application is a bit biased toward identification of a moment when a state may be considered responsible for the actions of non-state actors – hackers or private groups. A state providing material support or allowing its infrastructure to be used for cyber operations may have liability under international law. Yet, "effective control" remains a high standard often proven through concrete evidence of authorization or direct oversight.

[12] Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* 140–44 (Cambridge Univ. Press, 2d ed. 2017).

The following many cyber historical incidents of interest reveal the attribution practice. Russian government direct involvement in the 2007 known Estonia cyberattacks was never proved, while the 2014 hack against Sony Pictures attributed to North Korea have all the factors relying on circumstantial- evidence of passing grades, common codes, and tactics used from previous hacks[13]. These cases present even more challenges to conclusions of attribution to a state in this regard, especially considering the lack of any international consensus about standards for attribution.

International cooperation applied to attribution efforts brings maximum benefits from the shared intelligence, technical expertise, and forensic capabilities of states and organizations. Initiatives such as partnership in the Global Forum on Cyber Expertise (GFCE) or national cybersecurity agency partnerships can help share information with the aim of bettering attribution[14]. Political disagreement may thwart such efforts since sharing sensitive data regarding possible adversaries is viewed as an offense. Enhancing cooperation and transparency would be key to improving these attribution mechanisms and fostering accountability in cyber warfare.

Other burgeoning technologies, such as artificial intelligence and machine learning, become opportunities for enhancing attribution in cyberspace. These technologies can rummage through large datasets, pick out patterns of cyber operations, and identify distinctive digital signatures pointing to different actors. Although these advancements augment attribution accuracy, they present ethical and legal dilemmas: the reliability of such AI-generated evidence when generated and used against "the others," particularly when it frames other states or actors. The main problem related to cyber conflict attribution is the balance between technological innovation and accountability and fairness

Techniques for Attribution: Technical and Legal Perspectives

1) *Technical Attribution:*

This process involves forensic analysis of digital evidence for the actual origin of a cyber operation. This is through examination that incorporates the use of malware signatures, IP addresses, and attack vectors, yet most adversaries hide behind spoofing, false flags, or anonymization, thereby complicating the process of attribution.

2) *Legal Attribution:*

Legal attribution depends on the connection of cyber activities to state actions under international law. States must prove clear evidence of the control, direction, or authorization of cyber operations by non-state actors involved. The "effective control" test, determined by the International Court of Justice in the Nicaragua case, is considered to be fulfilled.

[13] Jack Goldsmith, Attribution and the Sony Hack, *Lawfare* (Dec. 19, 2014), https://www.lawfareblog.com/attribution-and-sony-hack

[14] Global Forum on Cyber Expertise, *About GFCE*, https://www.thegfce.org/about/; Robert Chesney & Danielle Keats Citron, Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security, 107 *Cal. L. Rev.* 1753, 1795–98 (2019)

Case Analysis: Attribution Challenges in International Law

1) *North Korea's suspected role in the 2014:*

The attack on Sony Pictures-the United States ascribed it to North Korea: That episode puts challenges related to attribution into relief. While the United States publicly attributed the cyber-attack launched against Sony Pictures to North Korea, that did not serve to dispel doubts and further serves to demonstrate the difficulty of meeting evidentiary requirements under international law.

2) *Against Georgia (2008):*

Web and infrastructure belonging to the government of Georgia were attacked through cyber means in an armed conflict with Russia in 2008. Attribution was difficult given reliance on proxies and decentralised attack method, hence difficult to hold accountable Russia.

RULES GOVERNING CYBER WARFARE UNDER INTERNATIONAL LAW

The United Nations Charter prohibits under Article 2(4) using force against the sovereignty or political independence of another state. Yet as to what is indeed a "use of force," highly contentious issues remain under the rubric of cyber operations, where traditional uses of force include physical harm whereas cyber actions can cause much disruption without tangible destruction. For example, a cyber attack on a country's power grid or its critical financial systems that cripples the entire functioning of the system would arguably fall in the prohibited use of force, if its aftermaths can be likened to those of conventional attacks. This ambiguity requires an understanding of how Article 2(4) is applied over cyberspace.

Article 51 of the UN Charter allows a state to respond to an "armed attack" in self-defense, but a problem arises as to determining when a cyber operation crosses the threshold to qualify as an armed attack. Cyber operations that cause physical destruction or result in loss of life are likely to clearly be above that threshold, while cyber operations that disrupt critical services or steal sensitive data may well fall below that threshold. For instance, significant ransomware attacks on the health infrastructure of a country that endanger lives could raise questions about whether such acts represent an extreme right to self-defense. Delimiting these boundaries is important for the consistent application of Article 51 to cyber wars.

Article 39 of the UN Charter empowers the Security Council to determine whether any such threats to international peace and security exist, potentially including cyber operations. For instance, state- supported cyber operations against critical infrastructure or electoral systems would destabilize global stability and appropriately find themselves within the purview of action by the Security Council. Yet, to date the Council has failed to effectively address cyber threats in large part because of these geopolitical divisions among its permanent members. Most of these divisions prevent reaching consensus in whether certain cyber activities constitute a threat to peace, which underlines the necessity of intensified international cooperation and dialogue on cybersecurity issues within the framework of the UN.

Provisions of the UN Charter on sovereignty are relevant considerations in the analysis of cyber operations. There are forms of cyber operations that involve accessing and exploiting another state's networks, manipulating other states' critical systems, or surveillance that constitute a violation of the sovereignty principle, even if they do not cross the threshold of a use of force. The interference, by a state-sponsored hacking program, in targeting elections undermines the victim state's political independence. These activities test the existence norms under international law, casting debates about the applicability of sovereignty in the highly connected digital.

This dynamic nature of cyber threats makes the long-held understandable need for clear international norms in addition to what has been set out in the UN Charter undeniable. Joint efforts, such as the UN Group of Governmental Experts (UNGGE) and the Open-Ended Working Group (OEWG) on cybersecurity, aim to establish common understandings regarding the applicability of international law in cyberspace; hence, they uphold transparency, cooperation, and the non-use of cyber capabilities to target critical infrastructure. Despite that, states' disagreement over the interpretations and application of these norms reveals that even today, tremendous problems continue to exist in achieving agreement on cyber governance at the global level.[15]

The Tallinn Manual: Key Insights and Contributions

The Tallinn Manual further elucidates in relation to the importance that the term "use of force" holds under Article 2(4) of the UN Charter, whether it applies to cyber operations. The Tallinn Manual would consider a cyber operation that causes physical damage, injury, or destruction akin to kinetic force as a use of force. Other kinds of operations that significantly impair economic or social activity, like degrading a nation's critical infrastructure, might also fall into this category, but would depend on the size and effects[16]. This interpretation has framed ongoing further debates over the boundaries of acceptable state activity in cyberspace, but will likely continue to clash with state practice.

The Tallinn Manual strongly emphasizes the principle of sovereignty in cyberspace. There is no confusion as to whether states have sovereignty over their digital infrastructure or not and are directly responsible for ensuring that their territory is not used to conduct hostile cyber operations against another state[17]. Any violation thereof, such as a case of hacking into another's government networks or disrupting its elections, falls under international law as wrongful. Nevertheless, disputes remain regarding the more specific limits of cyber sovereignty, especially those related to extraterritorial cyber espionage and surveillance.

The Tallinn Manual goes on to offer very clear guidance to apply the necessity and proportionality principles to cyber operations. These require any defensive or retaliatory cyber actions to be limited to what is necessary to achieve a legitimate military or strategic objective, causing minimum harm to civilians and neutral systems. Thus, a cyber countermeasure targeting an adversary's military network must not disrupt civilian infrastructure unless absolutely unavoidable. This focus on restraint, therefore, reflects respect for international law's

[15] Michael N. Schmitt, *The Notion of 'Use of Force' in International Law and Cyberspace*, 4 Balt. Y.B. Int'l L. 11, 15-18 (2004)

[16] Michael N. Schmitt ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* 331–36 (Cambridge Univ. Press, 2d ed. 2017).

[17] Ibid

humanitarian objectives translated into the context of cyber conflict.

Despite an exhaustive analysis, Tallinn Manual has its limitations. It is an academic, non-binding document and cannot carry the weight of international treaty law[18]. Therefore, states cannot be bound by the interpretations offered by it and a divergence in the views of different governments continues to exist over its application. The approach presented here, as critics say, is to extend the traditional legal frameworks into cyberspace without realizing some unique aspects presented by digital technologies, such as the difficulties of attribution or the decentralized nature of the internet[19]. Some others pointed out that it lacks concrete guidance on emerging novelties such as cyber operations by artificial intelligence.

The Tallinn Manual has greatly affected state practice and academic research since it offers a model through which international law in relation to cyber operations can be interpreted. Indeed, most states and international organizations seek recourse to this manual as a basis upon which their national policies and norms can be developed. For example, NATO has affirmed that the Tallinn Manual has been applied to its applicable cybersecurity programs. Although not a binding document, the impact of the manual itself underscores its significance as an important resource toward developing and regulating cyber warfare under international law.

State Sovereignty and Non-Intervention Principles in Cyberspace

The principle of sovereignty extends to a state's digital infrastructure, networks, and data flows in cyberspace. Hacking into government systems or interfering with the election process by whatever method is an infringement of sovereignty. This particular principle becomes complex on account of the de facto decentralized and interconnected nature of the internet, particularly in cases of operations originating from third-party servers or crossing multiple jurisdictions. The states' sovereignty interpretation on cyberspace differs, as some state that full territorial control should be followed, while others emphasize that it is a global digital environment.

The principle of nonintervention bans state interference in matters that concern other states, be it their internal or external activities, using a cyber platform. Such acts include: circulating disinformation; hacking elections; and cyber operations destructive to a government's power and authority. For example, rumors of international cyber intervention in national democratic elections from the United States and France have evoked more relevant discussions about whether the current international norms are sufficient in regulating such actions. Perhaps some of these instances already call for more protection and regulation about cyber operations that would destabilize political systems.

Sovereignty in cyberspace also intersects with the problem of transboundary data flows, as data often traverses several countries in its course. States hosting the infrastructure through which data passes may have little control or knowledge about malicious activities conducted over these networks. This presents jurisdictional challenges regarding enforcement of sovereignty and dealing with operations in cyberspace which take advantage of global networks. International agreements on the management of cross-border data flows are

[18] Id. at 72–75 (rules on necessity and proportionality in cyber countermeasures).
[19] Kristen E. Eichensehr, *The Law & Politics of Cyberattack Attribution*, 67 UCLA L. Rev. 520, 555–60 (2020).

essential to ensuring the respect of state sovereignty in cyberspace for developing countries.

Extraterritorial cyber operations, for example, running surveillance programs or cyber espionage, bring into question the limits of sovereignty. Such revelations as those about global surveillance programs conducted by some states set off concern about whether those programs are compatible with international law. Although espionage is not ruled out under international law, such operations that disrupt or manipulate another state's infrastructure may infringe sovereignty and the principle of non-intervention.

Clarifying the legal boundaries of extraterritorial cyber operations is critical to preventing abuses and fostering accountability.

THE ROLE OF CUSTOMARY INTERNATIONAL LAW IN CYBER WARFARE

This customary international law is developed through consistent state practice with opinio juris-the belief that a particular practice is legally obligatory. Customary international law, in the case of cyber warfare, is very important to fill up many of the gaps left open by the limited number of treaties focusing on cyber activities. Although such uncertainty remains with regard to the non-existence of a comprehensive international treaty on cyber warfare, more states are acknowledging certain principles in their national policies and in their diplomatic statements[20]. That is why customary norms related to these developments have emerged. They are more a reflection of the growing recognition of cyberspace as an integral domain of international relations requiring regulation through established legal frameworks.

Another relevant principle of customary international law in cyber warfare is the rule prohibiting cyber operations against vital infrastructure. Attacks against infrastructure, including power grids, water supply systems, and healthcare, present a enormity threat against the safety and security of populations. Since cyber operations were used against target states in conflict, the rule that infrastructure should be protected from malicious cyber activity gradually has evolved to become an accepted rule[21]. States basically agree that cyber operations causing significant physical or societal harm, similar to traditional attacks, amount to a breach of international norms and could be subject to self-defense under Article 51 of the UN Charter[22].

Respect for sovereignty in cyberspace is another bedrock area of customary international law. States are expected to exert control over their own digital infrastructure and to refrain from allowing their territory to be used for cyber operations that harm other states. Though a proper concept of sovereignty in cyberspace has yet to be fully defined, there is growing agreement among states that cyberattacks or interference in domestic affairs—the hacking of government databases or, for example, disinformation campaigns—violate the sovereignty of the state in question. This growing consensus presages a customary norm extending the

[20] Michael N. Schmitt ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* 6–8 (Cambridge Univ. Press, 2d ed. 2017).
[21] Jeffrey T. Biller & Michael N. Schmitt, *Critical Infrastructure and the Law of Armed Conflict*, 55 Tex. Int'l L.J. 337, 345–48 (2020).
[22] Jeffrey T. Biller & Michael N. Schmitt, *Critical Infrastructure and the Law of Armed Conflict*, 55 Tex. Int'l L.J. 337, 345–48 (2020).

principle of territorial integrity into the digital sphere.

Another area in which customary international law has evolved is that of the practice of cyber espionage, often conducted for intelligence-gathering purposes. International law does not prohibit espionage, but it is subject to specific limitations in certain circumstances, such as when it involves cyber activities that harm another state's[23] security or economy. States are generally obligated by international norms concerning the non-interference in the internal affairs of other states, meaning not engaging in wholesale cyber surveillance or espionage that destabilizes political systems or invades personal privacy on a large scale.

In that sense, opinio juris, meaning the belief that a practice is legally obligatory, is crucial in making customary international law in cyber warfare. Formal positions by the states, diplomatic statements, and the use of legal language in treaties, resolutions, and declarations are essential components that lead to the eventual norm. For instance, the fact that dozens of countries have endorsed the Tallinn Manual reflects an emerging consensus on how international law applies to cyber operations and therefore strengthens customary legal norms. The more states declare certain types of cyber activities unlawful— such as attacking civilian infrastructure or interfering in elections—the more those practices may consolidate into binding customary law, shaping state behavior and future legal development.

Customary international law is, however of greater significance because the developments in cyber warfare strategy require more explicit codification of such norms in international treaties or conventions. Without binding legal instruments, customary norms may be enforced inconsistently and may be interpreted differently by states. The vagueness about the concepts of attribution, proportionality, and threshold for self defence must be clarified in international consensus which may materialise out of multilateral negotiations or by frameworks drawn up by international bodies-possibly again at the level of the United Nations.

Role of State Practice and **Opinio Juris**

1) State Practice and Its Role in Shaping Cyber Norms

It's state practice that not only gives meaning to the development of customary international law in situations where cyber activities are concerned but also shows consistent actions and behavior of states reacting to cyber operations. This practice embraces the following: a national cybersecurity strategy has been developed, norms of cyber defense have been established, or a cyberattack has been publicly attributed to certain actors. For example, states have developed different lines of defense to protect their critical infrastructure from cyber threats and hold a shared view on the need to protect digital domains. States also increasingly make public accusations against the attackers of the cyberattacks, like the Wanna Cry ransomware attacks in 2017 as major incidents. States contribute towards the evolution of norms about accountability and responsibility in cyberspace by attributing their attacks to specific attackers. This also reflects state practice to participate in multilateral dialogues, such as those conducted by the United Nations Group of Governmental Experts. States exchange views and negotiate agreements to push through international cooperation on cyber issues, which in turn strengthens the emerging customary norms.

[23] *Tallinn Manual 2.0*, supra note 2, at 17–22.

2) Opinio Juris and the Legal Obligation in Cyberspace

It follows that opinio juris is an essential aspect of customary international law since it implies that states believe certain practice is binding in terms of the said law. In cyberspace, opinio juris may be observed when states clearly declare such cyber operations fall under international law. For instance, most of the states have made declarations stating that they consider norms of international law currently in force, such as the prohibition of unlawful interference in another state's internal affairs, as also fully applicable to cyber activities. That implies that countries recognize specific prohibitions, as in the targeting of critical infrastructure illegally or interfering in national elections through cyber means. For instance, the United States has threatened to retaliate with a proportional response in case of a cyberattack conducted against its critical infrastructure, thereby supporting the idea of cyber defense as a legitimate national interest according to international law. In the same vein, a consensus by the 2015 UN Group of Governmental Experts highlighted that the principles of sovereignty, nonintervention, and prohibition against the use of force apply to cyber activities and that states believe these principles should govern cyberspace. Declarations and legal stances taken by states contribute, finally, to the crystallization of customary norms and to the degree that they recognize that some cyber operations violate international law.

HUMANITARIAN IMPLICATIONS OF CYBER WARFARE

Cyber warfare will uniquely, and in fact perilously threaten civilian infrastructure as cyberattacks will essentially target critical systems that have heretofore been vital to the functioning of modern societies; attackable by either disruption or destruction in power grids, health care, transportation networks, and water systems through cyber means. Due to the tremendous level of interconnectivity among these systems, an attack on one point can cause cascading effects and thus enhance the damage. For instance, a cyberattack on a country's electrical grid system could disrupt water supply provisions or delay medical services, gravely harming the public health and safety. The impact that can be anticipated often extends considerably beyond the immediate disruption, causing both short- and long-term damage to a nation's economy, security, and stability.

The LOAC had declared that there are two important principles related to distinction and proportionality in cyber warfare. In this case, the principle of distinction dictates the parties engaged in war to distinguish between military and civilian objects, thus civilian infrastructure would not be attacked by military forces during such an operation[24]. Such operations, targeting civilian infrastructure, such as hospitals or electric power grids, would violate this principle since these systems are protected under LOAC for their civilian nature. Even if a system so happens to have both civilian and military functions, the distinction principle requires that it be targeted militarily exclusively with civilian damage being distinguished from and minimized.[25]

[24] Int'l Comm. of the Red Cross (ICRC), *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law*, 45–48 (2009)

[25] *Tallinn Manual 2.0*, supra note 3, at 430–32.

Even the principle of proportionality places some limitations on the level of accepted attacks. Collateral damage to civilians or civilian objects under LOAC is not allowed to be excessive in relation to the anticipated military advantage that an attack will confer[26]. Discussing cyber warfare, this in effect means that the effect on military objectives through a cyber attack must be rationally balanced with effects on civilians and civilian objects. Thus, an attack on a power grid, for example, may interfere with military action but could be considered disproportionate if the civilian damage outweighed the military advantage in circumstances where hospitals, schools, and other residential areas were targeted as well.

Perhaps one of the most inherent challenges of cyber warfare is cascading effects: discontinuity in one system could lead to unforeseen effects elsewhere in interconnected systems. An attack on a water supply network might, for example disable transportation systems, while an attack on a hospital network could have the effect of disabling emergency medical services. The indeterminacy of these effects makes it challenging to apply the principles of LOAC because it is very challenging to predict the full extent of civilian damage in advance[27]. Moreover, attribution in cyber warfare complicates accountability. Anonymity and complexity in conducting cyberattacks may make it challenging to identify the perpetrator, which can create an obstacle in enforcing LOAC and guarantee justice in instances of violations of LOAC.

Cyber Operations and Human Rights Law

Cyber operations could implicate IHRL strongly because they can disrupt access to essential services and information. Hence, such operations can compromise rights of utmost importance like the right to life, the right to privacy, and the right to access information. Such rights are protected through various international conventions, including the ICCPR, the UDHR, and regional human rights treaties. These rights continue to exist during armed conflict and provide a legal framework upon which the human rights implications of cyber warfare could be assessed.

One of the most serious problems concerning cyber operations and IHRL is their potential violation of the right to health, mainly when attacks target health care structures. Hospitals and medical services form an essential feature of public health and the treatment of individuals, particularly those affected in the conflict. Such cyberattacks that disrupt hospital networks or expose life-saving equipment for use can jeopardize the lives of patients, constituting, thus, a direct violation of the right to health. IHRL identifies the right to health as, inter alia, being linked to the guarantee of available medical care. Purposive or negligent attacks on such care may lead to gross violations of human rights. An attack on a hospital, although the premises might have some military value, could be classified as disproportionate if it interferes with the provision of necessary medical care to civilians.

There is a potential violation of the right to privacy in cyber operations such as surveillance or data breach. Since personal information can now be stored and transmitted online, it is susceptible to unauthorized access

[26] Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), art. 51(5)(b), June 8, 1977, 1125 U.N.T.S. 3.

[27] Jeffrey T. Biller & Michael N. Schmitt, *Rethinking the Principle of Proportionality in Cyber Conflict*, 50 Geo. J. Int'l L. 673, 693–97 (2019).

by states, non-state actors, or private entities. Cyberattacks aimed at espionage, hacking, or theft of personal data may infringe an individual's right to privacy where one implies private information, such as personal medical records, financial information, or private communications. For instance, mass surveillance by states can violate people's privacy rights, especially when sufficient legal safeguards or oversight are not present during implementation. The ICCPR insists that any interference with the privacy of a person must be appropriate, proportionate, and in accordance with law. States should ensure that their cybersecurity does not infringe on individuals' right to privacy and is not misused for excessive surveillance and collection of information during armed conflict

CONTEMPORARY CHALLENGES AND GAPS IN LOAC, FOR CYBER WARFARE

The Emergence of Autonomous and AI-Driven Cyber Weapons and Challenges for LOAC LOAC has faced unprecedented challenges with these autonomous and AI-driven cyber weapons because these systems can independently identify targets and execute cyber attacks without any human input. Such a manner poses critical concerns regarding responsibility, predictability, and compliance with LOAC principles, such as those dealing with distinction and proportionality[28]. The principle of distinction requires distinction between military and civilian objects; therefore, civilian infrastructure should not be targeted. Autonomous cyber weapons, however, may not have the sophistication in self-deciding if certain targets constitute the fact of civilian targets. This leaves the civilians exposed to possibly increased harm.[29]

Besides, the proportionality principle would require attacks not to cause harm to civilians to the extent of the anticipated military advantage in the operation, which would be arduous to apply to autonomous cyber operations since the unpredictability of the AI system threatens to lead to unintended[30], more serious damage through the cascade effect of a cyberattack. For example, an attack on the army's communication network may mushroom into inadvertently doing a great amount of damage to a large part of the civilian services, such as hospitals or public utilities, and thus affecting most civilians. The insecurity of current legal structures guiding their use and employment increases the dangers posed by autonomous weapons in cyber and thus suggests a call for regulation, thereby ensuring uniformity of usage with LOAC[31].

Balancing National Security with Privacy and Freedom

Surveillance, monitoring, and collection of data are parts of the military strategy in cyber warfare but usually violate some of the most fundamental human rights: the right to privacy and freedom of speech. States, in the name of national security, often have latitude for highly extensible programs of surveillance and data collection

[28] Michael N. Schmitt ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* 427–35 (Cambridge Univ. Press, 2d ed. 2017).
[29] Marco Roscini, *Autonomous Weapons and the Principle of Distinction in Armed Conflict*, 19 Int'l Hum. Legal Stud. 1, 10–12 (2019).
[30] Jeffrey T. Biller & Michael N. Schmitt, *Rethinking the Principle of Proportionality in Cyber Conflict*, 50 Geo. J. Int'l L. 673, 693–97 (2019).
[31] Stuart Casey-Maslen, *Autonomous Cyber Weapons Under International Humanitarian Law*, 20 J. Int'l Hum. Legal Stud. 1, 23–29 (2022).

including surveillance of communications that breaches the privacy rights of individuals as enshrined in international human rights law, specifically the International Covenant on Civil and Political Rights (ICCPR)[32]. This tension between the imperative for national security that may require intelligence gathering or counter-cyber operations and the obligation to respect civil liberties holds the challenge. For instance, the large-scale use of cyber surveillance on potential threats may violate individual rights to privacy, especially when undertaken without satisfactory lawful guidelines or regulation. Similarly, large breaches in data collection, or cyber vulnerability crafted for surveillance, can and do lead to the wrongful collection of sensitive personal information, thereby violating the rules of necessity and proportionality under the ICCPR. Such a balance between security and the necessary protection of privacy and freedom of speech remains one of the biggest challenges for states and international entities to address. Ethical and legal limits must be drawn on the subject of cyber surveillance to avoid abuse and safeguard fundamental rights, even in times of conflict.

The Need for a Comprehensive Cyber Warfare Treaty

Thus, the framework is mutilated as postulated in the international lands of cyber warfare since LOAC and IHRL would provide some founding, although there are no specific provisions incorporated because of the very nature of cyberspace itself. Even by the efforts of the United Nations and the Tallinn Manual, there is no setting up of a binding, comprehensive international treaty that would set up rules exclusively for cyber warfare. This therefore creates big gaps in uncertainty as regards the application of international law to cyber operations, especially when it involves questions on attribution, accountability, and state conduct in cyberspace issues.

A binding treaty on cyber warfare would clarify the ambiguities left by existing laws in relation to how cyber operations in armed conflict shall be conducted, applied, or observed, and distill principles of distinction, proportionality, and necessity in such military activities. Such a treaty can also build-in dispute mechanisms, so countries may resolve those conflicts which arise from cyberattacks in a manner not at variance with international law. Efforts such as the UN OEWG on Information Security reflect ever-increasing recognition of the need for international cooperation for norms in cyber operations, yet a holistic treaty remains elusive. The diversity of state interests, technological disparities, and varying perspectives on sovereignty and security account for this difficulty in reaching agreement on binding legal norms for cyber warfare. Nevertheless, there must be continued discussion and negotiation to close existing gaps and forge a uniform instrument that can truly help tackle the complexities of modern cyber conflict.

COMPARATIVE ANALYSIS OF NATIONAL APPROACHES TO CYBER WARFARE LAW

United States: Cyber Warfare as a Core Element of National Defense

The United States perceives cyber warfare as an integrated part of its national defense strategy because it can further enhance capabilities both in offense and defense. The Department of Defense's Law of War Manual provides methodology for applying traditional LOAC principles to cyber operations, emphasizing that these

[32] International Covenant on Civil and Political Rights, art. 17, Dec. 16, 1966, 999 U.N.T.S. 171.

principles continue to apply-jus in bello-in the context of cyber warfare, such as distinction, proportionality, and necessity. The U.S. also developed the U.S. Cyber Command, coordinating offensive and defensive cyber operations to demonstrate a mature approach towards managing cyber threats.

One of these doctrines that can be cited is the "Defend Forward" strategy, which allows a country to take preemptive cyber actions against enemies in disrupting the adversary's cyber capabilities before an attack reaches U.S. networks[33]. This approach to national security has significantly raised legal and ethical issues, relating particularly to proportionality-that is, whether the response is commensurate with the threat posed-and sovereignty, by which is meant the violation of another state's electronic space without due consent. The equation of national interests against international law is another hallmark of U.S. cyber warfare policy.

European Union: A Diplomatic and Legal Approach to Cyber Warfare

The European Union has a distinctive approach towards cyber warfare, which focuses on cooperation between nations, capacity building, and the observance of international law. In the EU, there is not one single military doctrine about cyber warfare; its policy is more inspired by the General Data Protection Regulation (GDPR) and initiatives like the EU Cybersecurity Act[34], which aims at increasing cyber resilience among the member states and the infrastructure in the EU generally. In summary, GDPR is mainly concerned with data protection, and in so far as this affects cyber operations, it should ensure that personal data is not improperly accessed or misused during cyber conflicts.

The EU would promote the formation of norms on state behavior in cyberspace, including, within and through the UN framework, encouraging discussion and development of international legal standards to regulate the use of cyber technologies in the context of armed conflict. The EU addresses cyber issues with an accountability-based system as it encourages nations to undertake proper diplomatic measures to avoid cyber conflicts and respect norms on sovereignty, non-intervention, and the protection of civilians in cyber warfare. Multilateralism will be key for the EU to secure a free rules-based international order in cyber operations; however, it gives more importance towards alliance cooperation with international players taking into account its unclear military cyber strategy.

China and Russia: Sovereignty-Centered Approaches to Cyber Warfare Both China and Russia use sovereignty-based approaches to cyber warfare that reveal a larger political strategy and strategic accord in the cyberspace. For instance, China adopts a cyber strategy that emphasizes cyber sovereignty, where it insists that any state should have the power to hold control over digital space within its borders. Aspects of this approach include using cyber capabilities for national security and espionage motives, such as hacking into the networks of foreign companies in the process of stealing their intellectual property. Mainly, China makes use of cyber operations to exert political influence, surveilling and suppressing dissident activity on the internet. This usage is very focused on securing national systems and preventing foreign states or actors from

[33] U.S. Dep't of Def., *Summary: Department of Defense Cyber Strategy 2018*, at 1–2, https://media.defense.gov/2018 (describing the "Defend Forward" doctrine).

[34] Regulation (EU) 2016/679, General Data Protection Regulation, 2016 O.J. (L 119) 1; Regulation (EU) 2019/881, Cybersecurity Act, 2019 O.J. (L 151) 15.

interfering with digital infrastructure.

Russia, however has been implementing a rather different vision-a specific strategy based on informational warfare and the distribution of disinformation, mainly during elections[35]. Therefore, many perceive Russian cyber operation as being part of a greater effort that reaches public opinion, interferes with political processes, and an attempt to interfere with the internal affairs of other countries. These cyberattacks, though typically covert, have given rise to some debate over state responsibility under LOAC, specifically as regards attributing and intent behind cyber operations[36]. Russia's tactics blur the lines between cyber espionage, sabotage, and psychological operations, which generates debate over the classification of such operations under international law.

India's Cyber Warfare Policies and Preparedness

India's approach to cyber warfare is still relatively embryonic, but this country has heavily invested into enhancing its capabilities to achieve improved cyber defense and cyber warfare capabilities as it responds to its growing cyber threats from state and non-state actors. The National Cyber Security Policy 2013 puts together the bases of building a comprehensive cybersecurity framework, which starts with securing critical infrastructure, developing a skilled workforce, and enhancing cyber resilience.[37]

India has also established a special cyber command in Indian Armed Forces with the aim to protect national assets from cyberattacks and provide military operational support. But there remains much hassle regarding legal frameworks, institutional coordination, and international engagement. Thus far, there is no effective, comprehensive legal framework for governing cyber operations; simultaneously, coordination between agencies and different stakeholders in cyber defense is ineffective. Indian cyber- defense policy must learn to be responsive to the new cyber-war landscape where more strategic and coordinated activities can be expected from state as well as non-state actors. International cooperation would form a kind of nexus in such a new scenario under which India would have to drive through these yet-to-be calming challenges to pursue effective cyber defense and risk minimizing the eruption of potential conflict.

CONCLUSION

International cooperation is needed to address the cross-border dimensions of cyber threats. Consequently, states should be proactive in those forums established by the United Nations Open-Ended Working Group (OEWG) and the Group of Governmental Experts (GGE) on matters related to cybersecurity governance. Regional mechanisms, like Europe's cyber diplomacy, as well as ASEAN's overarching cybersecurity framework, offer useful templates for cooperation.

[35] U.S. Senate Select Comm. on Intelligence, *Russian Active Measures Campaigns and Interference in the 2016 U.S. Election*, Vol. 1 (2019), https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf.
[36] Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* 312–17 (Cambridge Univ. Press, 2d ed. 2017)
[37] Ministry of Electronics & Information Technology, *National Cyber Security Policy 2013*, https://www.meity.gov.in/writereaddata/files/National_cyber_security_policy-2013%281%29.pdf.

Universal, normative standards regarding state behavior in cyberspace must be established to reduce ambiguity and prevent escalations. Step one may be Tallinn Manual 2.0, but there is much that is needed in efforts to formalize international law through norms. Norms should cover better protection for critical infrastructure, the prohibition on cyber attacks against civilian objects, and state transparency in cyber operations.

Attribution is going to remain a huge challenge in cyber warfare. The states and international organizations need to invest in technical and legal mechanisms of knowing the perpetrators of cyberattacks. An independent international body to attribute cyber incidents similar to the International Criminal Court could be a deterrent to unlawful cyber operations.

REFERENCES

1. **International Treaties and Conventions**

- *Geneva Convention of 1949*, art. 3, Aug. 12, 1949, 75 U.N.T.S. 31.
- *International Covenant on Civil and Political Rights*, Dec. 16, 1966, 999 U.N.T.S. 171.
- *United Nations Charter*, art. 2, June 26, 1945, 59 Stat. 1031, 3 Bevans 1153.
- *Hague Convention IV on Laws and Customs of War on Land*, art. 22, Oct. 18, 1907, 36 Stat. 2277, 1 Bevans 631.
- *Convention on Cybercrime*, Nov. 23, 2001, ETS No. 185.

2. **Case Law**

1. *Nicaragua v. United States of America*, ICJ Rep. 1986, at 14.
2. *Case Concerning Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States)*, 1986 I.C.J. 14.
3. *Aerial Incident of 10 August 1999 (Pakistan v. India)*, ICJ, 1999, para. 13.
4. *Israel's Targeted Killings Case* (Public Committee Against Torture in Israel v. Government of Israel), 2006.
5. *Prosecutor v. Tadić*, Case No. IT-94-1-A, Judgment, Int'l Crim. Trib. for the Former Yugoslavia, July 15, 1999.
6. *The Oil Platforms Case (Iran v. United States)*, 2003 I.C.J. 161.
7. *Case Concerning Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda)*, 2005 I.C.J. 116.
8. *The Nicaragua Case* (Nicaragua v. United States), International Court of Justice, 1986.
9. *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, Advisory Opinion, ICJ, 2004.
10. *The Cyber Espionage Case of 2016* (USA v. China) - UN Security Council Consideration.

3. Books and Articles

- Schmitt, Michael N., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge Univ. Press, 2d ed. 2017).
- Casey-Maslen, Stuart, *Autonomous Cyber Weapons Under International Humanitarian Law*, 20 J. Int'l Hum. Legal Stud. 1 (2022).
- Maurer, Tim, *Cyber Mercenaries: The State, Hackers, and Power* (Cambridge Univ. Press, 2018).
- Lin, Herbert, & Kerr, Jackie, *Attributing Cyber Attacks: The Emerging Role of Cyber Threat Intelligence Companies*, 10 Hoover Institution Cyber Policy Briefs 1 (2019).
- Schmitt, Michael N., *Cyber Warfare and the Law of Armed Conflict*, 90 International Law Studies 128 (2014).
- Goldsmith, Jack, *Cybersecurity Treaties: A Skeptical View*, 35 Wash. Int'l L.J. 1 (2020).
- Milan, Stefania, *Regional Efforts for Cyber Governance: Lessons from ASEAN*, 10 J. Internet L. 21 (2020).
- Duggal, Pavan, *Legal Issues in Indian Cyber Warfare Policy: A Critical Analysis*, 16 J. S. Asian L. 34 (2020).
- Roscini, Marco, *EU Cyber Diplomacy and the Role of International Law*, 24 Int'l Comm. L. Rev. 54 (2022).
- Hollis, Duncan, *Why Do We Need Cyber Norms?* Just Security (Mar. 2020), https://www.justsecurity.org.

4. Reports and Manuals

- U.S. Dep't of Def., *Department of Defense Law of War Manual*, §§ 16.1.1-16.1.2 (Dec. 2016, updated Dec. 2019).
- United Nations, *Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*, U.N. Doc. A/75/816 (July 22, 2021).
- Ministry of Electronics & Information Technology, Govt. of India, *National Cyber Security Policy, 2013* (July 2, 2013), available at https://www.meity.gov.in.
- U.N. Institute for Disarmament Research, *Strengthening Cyber Attribution: Building Mechanisms for State Accountability* (2021).
- European Commission, *EU Cybersecurity Strategy for the Digital Decade*, COM(2020) 823 final (Dec. 2020).

5. *Online Sources*

- Schmitt, Michael N., *The "Defend Forward" Cyber Strategy: What is the International Law Perspective?*, Just Security (Nov. 2020), https://www.justsecurity.org.
- Duggal, Pavan, *India and Cyber Warfare: Current and Future Challenges*, The Times of India (Dec. 22, 2021), https://timesofindia.indiatimes.com