CYBER WARFARE AND INTERNATIONAL LAW

Yashika Garg, Symbiosis Law School, Pune

ABSTRACT

Cyber warfare is a relatively new form of conflict that involves the use of digital technologies to disrupt, damage, or destroy computer systems and networks. As with any form of warfare, cyber warfare raises important legal questions related to the use of force, self-defense, and international humanitarian law.

Cyber warfare has emerged as a new form of warfare in the modern world, presenting complex legal challenges in terms of the application of international law. The aim of this research article is to examine the relationship between cyber warfare and international law, analyzing the legal frameworks that apply to this form of conflict. The article argues that the current legal frameworks are insufficient to effectively deal with the challenges of cyber warfare, and proposes recommendations for legal reforms to ensure a more effective response to cyber threats. This research article explores the relationship between cyber warfare and international law, with a focus on the legal frameworks that apply to this form of conflict.

Keywords: Cyber warfare, International law, Law of armed conflict, Cyber attacks, State responsibility, Self-defense, Cyber terrorism, Cyber weapons, International norms, Cyber arms control.

LITERATURE REVIEW

The literature on cyberwarfare and international law is relatively limited, with much of it focusing on the challenges associated with defining cyberwarfare and establishing legal frameworks to regulate it.

- In a study published in the **Harvard National Security Journal**[1], The authors discuss the challenges associated with defining cyberwarfare and recommend that international law should consider the nature of cyber operations, their intended effects, and the context in which they are conducted. They argue that such an approach would provide a more flexible framework to regulate cyberwarfare.
- In a study published in the **Journal of Conflict & Security Law**[2], The authors discuss the challenges of attribution in cyberspace and recommend that international law should consider the nature of cyber attacks, the means of attribution, and the context in which they are conducted. They argue that attribution should be based on a balance of probabilities, rather than proof beyond a reasonable doubt, to make it easier to attribute cyber attacks to specific individuals or groups.

INTRODUCTION

Cyber-attack is destructive in nature. An example of such a hostile action is erasure by a computer virus resident on the hard disk of any infected computer. In this particle, *CYBER-ATTACK* refers to the use of deliberate actions and operations— perhaps over an extended period of time—to alter, disrupt, deceive, degrade, or destroy adversary computer systems or networks or the information and (or) programs resident in or transmitting these systems or networks[3].

The legality of cyber warfare remains unsettled. The International humanitarian law (IHL) has historically interpreted "armed conflict" in the context of conventional military weapons in order to respond proportionately and as necessary to stop the threat. Since modern technology has brought warfare into cyberspace, there is a need to adapt international instruments such as the IHL to meet new challenges facing the world. Although opinion is divided as to how to apply IHL to cyber-attacks, recent events confirm that cyber warfare is operational**[4].**

[1] Maj. Gen. Charles J. Dunlap, Jr., Perspectives for Cyber Strategists on Law for Cyberwar, Strategic Studies Quarterly (Spring 2011).
[2] Journal of Conflict & Security Law
[3] National Research Council (NRC) (2009). Technology, Policy, Law and Ethics regarding U.S. Acquisition and Use of Cyberattack Capabilities.
[4] Gervais, M. (2012). Cyber-Attacks and the Laws of War. Berkeley Journal of International Law, 30, 525-531. https://doi.org/10.2139/ssrn.1939615

How is Cyberwarfare Unique?

Due consideration must be given to the unique features of cyberspace when interpreting and implementing current international law to cyberwarfare. Most significantly, cyberspace is the only area that was created solely by humans. It is jointly produced, preserved, owned, and run by public and commercial partners throughout the world and evolves often in reaction to technology advancement. Information and electronic payloads are instantly deployed between any point of origin and any destination connected through the electromagnetic spectrum since cyberspace has no geopolitical or physical borders. Before being reassembled at their destination, they travel in the form of many digitized fragments via erratic routes. Despite the ease with which governments, non-state organizations, private businesses, and people may use the internet, effective identification and attribution of cyber operations are particularly challenging due to techniques like IP spoofing[5] and the usage of botnet[6].

International Legal Frameworks

International law provides a framework for regulating cyber warfare. While the exact legal status of cyber warfare is still evolving, there are several key international laws and agreements that are relevant to cyber warfare.

United Nations Charter : The UN Charter is the cornerstone of international law, and it prohibits the use of force by states against other states, except in self-defense or when authorized by the UN Security Council. While the Charter was drafted before the advent of cyberspace, it is still applicable to cyber warfare. Under the Charter, cyber attacks that cause physical harm or destruction may be considered a use of force and therefore subject to the prohibition on the use of force. A state may use force in response to a cyber-attack as a legitimate exercise of the right of self-defense. Before exercising this right, there is a need to establish the responsibility of another state for the cyber-attack. In Articles 39 and 42, the Charter contains only two exceptions to this prohibition on the use of force: actions authorized by the Security Council and acts of self-defense under Article 51 of The UN Charter.

- Security Council Authorizations

[5] "IP spoofing" refers to the creation of Internet Protocol (IP) packets with a forged source address with the purpose of concealing the identity of the sender or impersonating another computing system.
[6] A "botnet" is an interconnected series of compromised computers used for malicious purposes. A computer becomes a "bot" when it runs a file that has bot software embedded in it.

- Right of Self-Defense
- Does Cyber-attack constitute an armed attack?
- State Responsibility - State Actors, Non-State Actors
- Duty to prevent Cyber-attacks
- Violation of the duty to prevent Cyber-attacks

International Humanitarian Law : International humanitarian law (IHL) governs the conduct of armed conflict, including cyber warfare. IHL requires that attacks be directed only at military targets and that they not cause unnecessary harm to civilians or civilian objects. Cyber attacks that result in the destruction of civilian infrastructure or that cause unnecessary harm to civilians may be considered violations of IHL.

The *International Humanitarian Law* provides the primary legal framework within which to understand constraints on the use of offensive cyber operations. The IHL addresses two separate questions. First, when is it legal for one nation to use force against another? This body of law is known as *jus ad bellum*. Second, what are the rules that govern the behavior of combatants who are engaged in armed conflict? This body of law is known as *jus in bello*. It is separate and distinct from *jus ad bellum*.

Geneva Conventions: The Geneva Conventions set out the rules for the treatment of civilians and prisoners of war during armed conflict. Cyber attacks that result in harm to civilians or prisoners of war may be considered violations of the Geneva Conventions.

Tallinn Manual: The Tallinn Manual is a non-binding legal guide that was developed by a group of experts convened by the NATO Cooperative Cyber Defence Centre of Excellence. The Tallinn Manual provides a detailed analysis of the legal issues surrounding cyber warfare and concludes that existing international law, including the UN Charter and customary international law, applies to cyber warfare. It also recognizes the right of states to use cyber operations in self-defense.

Council of Europe Convention on Cybercrime: The Council of Europe Convention on Cybercrime is the first international treaty that addresses criminal activity committed over the internet. The Convention requires states to criminalize a wide range of cyber crimes, including hacking, identity theft, and cyber terrorism.

JUDICIAL PRONOUNCEMENTS

The use of cyber warfare in armed conflicts is a relatively new phenomenon, and as such, there are only a few cases where international law has been applied to cyber warfare. However, there have been some notable cases that have helped to shape the legal framework for cyber warfare.

1. *Israel and Syria* : In 2007, the Israeli Air Force conducted an airstrike on a Syrian nuclear reactor. The attack reportedly included a cyber component, where Israeli forces allegedly used a computer virus to disable Syrian air defenses. The incident was not publicly acknowledged by either side, but it is widely believed to have been the first example of cyber warfare being used in conjunction with traditional military operations.
2. *Estonia Cyber Attacks* : In 2007, Estonia experienced a series of cyber attacks that disrupted government and commercial websites. The attacks were believed to have been carried out by Russian hackers in response to a dispute over the relocation of a Soviet-era war memorial.The incident highlighted the need for international norms and laws to govern cyber warfare.
3. *Stuxnet* : In 2010, the Stuxnet virus was discovered to have been used to sabotage Iran's nuclear program. The virus was reportedly developed by the United States and Israel, and it caused significant damage to Iran's nuclear facilities. The incident raised questions about the legality of using cyber warfare to sabotage critical infrastructure.

Challenges in Applying Legal Frameworks to Cyber Warfare

There are several challenges in applying the legal frameworks of IHL and international law to cyber warfare. One of the *Primary challenges* is the difficulty in identifying the perpetrator of a cyber attack. Unlike traditional military operations, cyber attacks can be conducted anonymously or through intermediaries, making it difficult to attribute responsibility for the attack. *Another challenge* is the issue of proportionality. In traditional military operations, the principle of proportionality requires that the level of force used in an attack be proportionate to the military objective. However, in the case of cyber warfare, it is often difficult to determine what constitutes a proportional response. For example, a cyber attack that disables a critical infrastructure system may not involve the use of physical force, but could still have devastating consequences. A *third challenge* is the lack of consensus on what constitutes an act of aggression in cyberspace. While the United Nations Charter prohibits the use of force in international relations, there is no clear consensus on whether a cyber attack constitutes a use of force. Some argue that cyber attacks that cause physical damage or loss of life should be

considered a use of force, while others argue that only attacks that involve the use of physical force should be considered a use of force.

CRITICAL ANALYSIS

The intersection of cyberwarfare and international laws presents several challenges and complexities. One of the main challenges is the difficulty in identifying the perpetrators of cyber attacks and attributing responsibility to specific states or actors. This makes it difficult to enforce existing international laws and norms that regulate state behavior in cyberspace. Another challenge is the lack of consensus on the appropriate legal framework for regulating cyberwarfare. Existing international laws, such as the United Nations Charter and the International Humanitarian Law, were developed for traditional warfare and may not be applicable to the unique characteristics of cyberwarfare. This has led to ongoing debates among policymakers, academics, and practitioners on the appropriate legal framework for governing cyberwarfare.

Furthermore, there is a lack of clear guidelines on what constitutes an act of cyberwarfare and when a state is justified in using cyber attacks in self-defense. This has led to concerns over the potential for escalation and miscalculation in international relations, as well as the potential for unintended consequences resulting from cyber operations.

RECOMMENDATIONS

The future of international law in regulating cyber warfare is likely to be shaped by a number of factors, including technological developments, changes in the nature of warfare, and evolving norms and practices among states. Here are some suggestions for how international law could be further developed to regulate cyber warfare:

1. ***Strengthening international norms*** : One approach to regulating cyber warfare is to develop and strengthen international norms of behavior. This could involve developing rules of engagement for cyber operations, creating mechanisms for sharing information about cyber threats, and establishing norms around the responsible use of cyber weapons.
2. ***Updating existing laws and treaties*** : As the nature of warfare evolves, existing laws and treaties may need to be updated to reflect new realities. For example, the Geneva Conventions were developed in the context of conventional warfare, and may need to be updated to reflect the unique challenges posed by cyber warfare.

3. ***Creating new laws and treaties*** : In addition to updating existing laws and treaties, there may be a need to create new legal frameworks specifically tailored to cyber warfare. This could involve creating new international treaties or conventions that establish rules and norms around cyber warfare.
4. ***Enhancing international cooperation*** : Cyber warfare is a global phenomenon, and effective regulation will require international cooperation. States could work together to share information about cyber threats, coordinate responses to attacks, and develop joint strategies for regulating cyber warfare.
5. ***Investing in cybersecurity*** : Finally, it is important to recognize that effective regulation of cyber warfare will require significant investments in cybersecurity. This could involve investing in technology to prevent cyber attacks, training personnel to respond to cyber threats, and developing effective legal and regulatory frameworks to govern cyber operations.

Overall, the future of international law in regulating cyber warfare will depend on the willingness of states to work together to develop effective legal frameworks and norms of behavior. While the challenges of regulating cyber warfare are significant, the potential risks of unchecked cyber aggression make it imperative that the international community continues to work towards effective regulation.

CONCLUSION

Cyberattacks are global in scope. Despite useful legal countermeasures, domestic laws and policies that make cyberattacks illegal cannot fully and effectively stop an activity that is actually an international idea. Only a worldwide response by the international community coming up with a new cyberattack legislation will effectively address this global menace.

To start, the issue must be agreed upon, including the definitions of phrases like "cyber-attack," "cyberwarfare," "damage," "use of force," and "armed conflict," as well as the terms "distinction" and "proportionality" as they relate to cyberwarfare.

In conclusion, the topic of cyberwarfare and international laws is a complex and multifaceted issue. While there have been some efforts to develop international norms and laws that govern state behavior in cyberspace, there are still many challenges and uncertainties that need to be addressed. As the use of technology continues to play an increasingly important role in international relations, it is important for policymakers and scholars to continue to engage in discussions and debates on the appropriate legal framework for regulating cyberwarfare.

REFERENCES/BIBLIOGRAPHY

- "International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed," by Eric Talbot Jensen and Ronald T. P. Alcala, Harvard National Security Journal (2014).
- "The Tallinn Manual on the International Law Applicable to Cyber Warfare," edited by Michael N. Schmitt, Cambridge University Press (2013).
- "The International Law of Cyber Operations," by David P. Fidler, Oxford University Press (2016).
- "The Law of Cyber-Attack," by Richard J. Aldrich and Brian M. Mazanec, Journal of Conflict and Security Law (2011).
- "The Application of International Law to State Cyberattacks," by Thomas J. Cox, Georgetown Journal of International Law (2013).
- "The Emerging Law of Cyber War and Cyber Peace," by Paul Rosenzweig, Georgetown Journal of International Law (2011).
- "Cyberwarfare: Issues and Implications for International Law," by Harold Hongju Koh, American Journal of International Law (2013).
- "Cyber Warfare and International Law: A Comparative Analysis," by K. Sridhar and S. K. Suman, Journal of International Law and International Relations (2015).
- SIU Library https://library.siu.edu.in/index.php