An Analysis Of Cyber Warfare And Its Intersection With International Law

By: Lilia Gomez[1]

Abstract

Cyber warfare is an emerging form of warfare that has posed a challenge to the world since the beginning of the usage of computers and technology. With the increase of technology usage, the threat of cyber security has become more prevalent, and the standard rules of engagement are not being redefined because of it. Among these challenges, the emergence of cyber warfare has raised complex legal questions that demand careful consideration. This article will provide an analysis of the legal implications and framework surrounding cyber warfare, security and the ways in which it correlates with international law and how society will have to adjust to these emerging types of potential threats.

Introduction

Over the past two decades, cyber warfare has evolved into a critical component of global security, often overshadowing traditional physical battlefields. Unfortunately, the law of armed conflict has not kept pace with this new domain. International law still defines a "use of force" and an "armed attack" in kinetic terms, and the U.S. Law of War Manual mirrors that view, providing that a cyber attack that has a kinetic effect is to be treated as if it were that kinetic attack.[2] This shift has placed digital conflicts at the forefront of international defense strategies, marking a significant departure from conventional warfare tactics. The need for specific cyber warfare laws on the international spectrum, specifically with the United States, is critical to protect the Western Hemisphere from becoming vulnerable at a time where many states[3] such as

---

[1] Advised by Carlo Pedrioli (carlo.pedrioli@sulc.edu) and Judd Sneirson (judd.sneirson@sulc.edu).
The views expressed are those of the author and do not reflect the official policy or position of the US Government.

[2] Jacob Azrilyant "*Logic Bombs and Silicon Trenches: Use of Force in the Cyber Age",* 9 J.L. & Cyber Warfare 52, (2024).

[3] State is defined as "a state is a political division of a body of people that occupies a territory defined by frontiers. The state is sovereign in its territory (also referred to as jurisdiction) and has the authority to enforce a system of rules over the people

Russia and China, (which have traditionally been called "Super powers") are fighting to become leading super powers.

The evolving nature of cyber warfare and its impact on international law necessitate a thorough examination of the legal implications of cyber operations in the context of armed conflicts and self-defense. The recent flare-ups aggressive actions in the Israel-Hamas conflict and the involvement of various state and non-state actors in cyber operations underscore the complex challenges associated with attributing and responding to cyber warfare within the framework of international law.

When one is speaking of cyber warfare, the main topic that comes to mind is a "cyber attack or ." A cyber attack is an assault launched by cybercriminals using one or more computers against a single or multiple computers or networks. It can maliciously disable computers, steal data, or use a breached computer as a launch point for other attacks.[4] The usage of cyber attacks is the main tool of cyber warfare which is becoming increasingly common. These can be used to disrupt or disable infrastructures, steal classified information, or conduct espionage. Because of this, states have and currently are attempting to develop and improve their own cyber capabilities to defend against such attacks and to conduct their own cyber operations from against foreign entities (such as adversaries).

While the word terrorism is clearly a word connected often associated with a stereotype of a man with explosives from another country, in the context of the cyber world, terrorism is often seen in various other forms. Cyber terrorism has been described as premeditated, politically motivated attacks by sub national groups, individuals against information and computer systems, programs and data that result in violence against non-combatant targets.[5][6]

This article will provide an analysis of the current avenues of legal frameworks and how various countries (later defined as states)

---

living inside it. That system of rules is commonly composed of a constitution, statutes, regulations, and common law." Cornell Law School (Legal Information Institute) Legal Encyclopedia, (2021)≥, https://www.law.cornell.edu/wex/state.

[4] Check Point Cyber Technology, What is Cyber Warfare?, https://www.checkpoint.com/cyber-hub/cyber-security/what-is-cyber-attack/#:~:text=A%20cyber%20attack%20is%20an,launch%20point%20for%20other%20attacks (Last visited May 2023).

[5] In this article's context, this term will be used with cyber warfare to explain the correlations and differences between both.

[6] Andrew Colarik and Lech J. Janczewski, Introduction to Cyber Warfare and Cyber Terrorism", (May 2007),https://www.igi-global.com/pdf.aspx?tid=101974&ptid=225&ctid=15&t=introduction%20to%20cyber%20warfare%20and%20cyber%20terrorism.

are attempting to combat cyber warfare and how it correlates to international law. Lastly, this article will briefly discuss the problems within the current frameworks and how to adjust to future potentially forecasted events.

The Significance of Cyber Warfare in International Law

In recent years, cyber warfare has become an increasingly common and convenient tool held in the back pockets of various states, such as Russia, China and even third world states such as North Korea. The usage of cyber-attacks has become more frequent, and their effects have become more devastating. It is no secret that these states have utilized and generated cyber-attacks for political and monetary gain over the years. As such, it is critical that we one understands the implications of cyber warfare on the spectrum of international law.

International law has traditionally focused on physical warfare, but with today's society's perspective of the cyber community, it is necessary to update and develop legal frameworks to encompass the new reality of armed conflict. It is crucial to recognize that cyber warfare can result in significant consequences, including the disruption of critical infrastructures, the theft of sensitive information, and interference with democratic processes. These impacts have been observed in notable incidents, such as the 2016 U.S. Presidential Election, where social media platforms like Twitter and Facebook were exploited by bots, and more recently, in the Ukraine-Russia conflict and the Israeli-Hamas conflict. These examples highlight the far-reaching and potentially destabilizing effects of cyber operations on global security and political stability.

Another aspect of cyber warfare is the principle of proportionality. Proportionality is a core principle in international law, which provides that the legality of an action shall be determined depending on the respect of the balance between the objective and the means and methods used as well as the consequences of the action. This principle implies an obligation to appreciate the context before deciding on the legality or the illegality of an action.[7] This assessment is the responsibility of those who act.[8] To put this in an international law and cyber warfare context, it prohibits attacks which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination, which would be excessive in relation to the concrete and direct military advantage anticipated. The adherence to

[7] Doctors Without Borders, "The Practical Guide to Humanitarian Law", https://guide-humanitarian-law.org/content/article/3/proportionality/#.

[8] Amnesty International, "Collateral Damage or Unlawful Killings?" Violations of the Laws of War by NATO during Operation Allied Force http://www.amnesty.org/ailib/intcam/kosovo.

humanitarian law ensures that this principle of international law is addressed. This helps prevent cyber attacks and limits collateral damage on noncombatant citizens and infrastructure.

Cybersecurity and international law are closely related as cyber activities and warfare can have cross-border implications. International law applies to the conduct of states in their international relations, including within the cyber domain. This includes state sovereignty, the prohibition of the use of force, and the protection of human rights.

State sovereignty refers to the international law principle that indicates that states possess the authority and power within their own territory and have the right to govern themselves without interference from external entities, such as other states. This principle recognizes that each state is independent and equal in its decision-making and has authority to regulate its own laws, policies, and governmental structures.

The prohibition of the use of force, a principle that is fundamental in international law, ~~principle~~ which prohibits states from utilizing military force against one another except in cases of self-defense or when authorized by the United Nations' Security Council. This principle, as indicated within in Article 2(4) of the United Nations Charter[9], aims to maintain international peace and security by preventing armed conflicts between states. An example that illustrates this is the 1990 invasion of Kuwait by IraqThe international community recognized the use of force, and responded with economic sanctions against Iraq, ultimately leading to a military intervention authorized by the United Nations to liberate Kuwait and restore sovereignty within that region. This example underscores the importance of upholding the prohibition of the use of force to prevent aggression and preserve stability in the international spectrum.

The protection of human rights is prevalent in international law. It plays a role to protect human dignity[10] and mitigates the suffering of individuals affected by armed conflicts. Its significance extends to cyber warfare, where the purpose of humanitarian law becomes increasingly vital. The International Committee of the Red Cross (ICRC) is concerned about cyber warfare because of the

[9] United Nations Charter, "Prohibition of the Treat or Use of Force," art. II, ¶ 4, https://legal.un.org/repertory/art2/english/rep_supp7_vol1_art2_4.pdf (2022).
[10] "Defined in academic and legal contexts as a form of inherent worth or status that is claimed to belong equally to all individuals, serving as the foundation for fundamental moral or political obligations and rights." Debes, Remy, "Dignity", The Stanford Encyclopedia of Philosophy (Edward N. Zalta & Uri Nodelman (eds.), https://plato.stanford.edu/archives/spr2023/entries/dignity/ (2023).

vulnerability of cyber networks and the potential humanitarian cost of cyber attacks.[11]

In the perspective of cyber warfare, attacks may target critical infrastructure, civilian populations, or disrupt essential services and adhere to humanitarian law to ensure that the principles of international law mentioned above are addressed. This helps prevent cyber attacks and limits collateral damage on noncombatant citizens and infrastructure.

By applying humanitarian law to cyber warfare, states can navigate the complex legal and ethical challenges posed by this evolving domain, safeguarding human rights, and promoting the preservation of humanitarian values even in the virtual battleground. The integration of humanitarian law into cyber warfare plays a crucial role in maintaining stability, protecting innocent lives, and upholding the fundamental principles of humanity.

Global Background

Legal Recourse In Cyber Warfare: An Overview

There are several international agreements and norms that have been developed to address specific aspects of cybersecurity, such as the protection of critical infrastructure and the suppression of cybercrime.[12][13] However, none of the international agreements have true legal recourse. These are voluntary binding agreements as there is not an established judicial system to address any consequences for a breach of an agreement.[14] ~~legal merit~~. This has led to States failing to provide a safety net to prevent any cyber attack from occurring. The problem is not the governmental entities but rather the formulation of laws that prevent nonstate actors such as individual hackers and IT agencies from infiltrating governmental and private sector cyber infrastructures. This can lead to an organization becoming vulnerable.

This type of vulnerability allows cyber attacks to become asymmetric. This concept, which shifts warfare from the traditional military warfront to another spectrum which involves extremist organizations to challenge the security of well-established states. These attacks are difficult to predict, highly coordinated, and are

[11] Cyberwarfare and International Humanitarian Law: The ICRC's Position – prepared by the International Committee of the Red Cross, (2013).
[12] The suppression of cybercrime will be addressed later within this article.
[13] Thresea Hitchens & Goren Nislu, "Center for International & Security Studies", U. Maryland, International Cybersecurity Information Sharing Agreements, (2017), http://www.jstor.org/stable/resrep20426.
[14] The consequence of a lack of legal recourse will be addressed later within this article.

often done anonymously. This makes attribution and prosecution challenging. Given the transnationality of cybercrimes, effective responses will require full global policing by law enforcement and intelligence agencies. These types of examples include (but are not exclusive to) information-sharing, collaboration and capacity-building.

It is crucial to keep in mind that different states may have their own domestic laws controlling cyber warfare, and these laws may be applied to certain extremist organizations and individuals for their online behavior. However, there have been a number of legal frameworks and international agreements that have been developed to govern a state's behavior in cyberspace. For instance, NATO experts formulated the Tallinn Manual.[15] The United Nations also developed a framework that provides guidance on a state's responsibility when it comes to cyberspace behavior. It is imperative to note that while these manuals are important for the sake of combating cyber warfare, none have legal precedents as indicated previously, as they lack legal merit.[16]

Understanding the legal implications of cyber warfare is crucial because it can help prevent and mitigate conflicts. International law can provide clear guidelines for responsible usage of cyber capabilities and can help prevent misunderstandings that could lead to conflicts. One important aspect of cyber warfare in international law is attribution. The term "attribution" denotes the operation whereby the conduct of some human beings, through commission or omission, are regarded in law as that of the state for the purpose of establishing its responsibility for an internationally wrongful act.[17] It can be difficult to determine who is responsible for a cyber attack, as it is possible to disguise the origin of the attack. However, implementing international laws can provide guidelines for attributing responsibility and holding offending organizations or states accountable for their actions.

Domestic Law

The United States does not have official laws that combat cyber warfare. However, in 2021 Congress held a Congressional Study Group that addressed international and domestic legal issues governing cyberactivity and cyberwarfare. These sessions focused on regulatory guidance and advising of how the United States can focus on defenses to critical cyber activities. During this time, experts also addressed the importance of the U.S. starting to formulate domestic

[15] The Tallinn Manual will be addressed seperately within this article.
[16] Legal merit will be discussed later within this article.
[17] M. Milanovic, "Special Rules of Attribution of Conduct in International Law" (2020),https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=2926&context=ils.

laws governing cyber activity.[18] Additionally, Congress moved towards a stance that serious cyber intrusions are in fact international law violations and therefore spearheaded preventative measures within the United States.

The United States' approach on prevention of cyber warfare against the country is to provide military support and "defend forward."[19] This mindset has been associated with several military operational organizations such as USCYBERCOM whose ~~overall totality of~~ existence is based on the engagement with foreign and domestic adversaries who are consistently attempting to infiltrate U.S. networks and infrastructures.

USCYBERCOM was established in 2010 and headquartered in Maryland, with the National Security Agency. This organization provides support to US elections and works to identify, mitigate, and respond to threats such as terrorists use of the internet, and adversaries' attempts to influence and disrupt U.S. social cohesion and democratic processes.[20]

USCYBERCOM operates globally in real time against determined and capable adversaries. Its mission is to direct, synchronize, and coordinate cyberspace planning and operations to defend and advance national interests in collaboration with domestic and international partners. USCYBERCOM defends military informational systems, supports all military branches with cyberspace operations, as well as defends the country from significant cyber attacks.[21] Nothing is more evident of an example than the 2016 presidential election in which it was determined that the Russian government interfered through the hacking of the Democratic National Committee. This act questioned whether it was considered a violation of international law or "international norms of

---

[18] Brookings Report, Legal Regimes Governing Cyberactivity and Cyberwarfare (Session 12), May 11, 2022.

[19] S. Ravich,, & E. Cardon, "*Defending Forward in The Cyber Domain, Foundation for Defense of Democracies",* (Dec. 20, 2022), https://www.fdd.org/analysis/2020/12/15/defending-forward-defending-forward-in-the-cyber-domain/#:~:text=%E2%80%9CDefend%20forward%E2%80%9D%20means%20protecting%20America%E2%80%99s%20most%20critical%20networks,States%20to%20support%20and%20protect%20at-risk%20U.S.%20systems.

[20] U.S. Cyber Command, Cyber 101: "U.S. Cyber Command History", (Oct. 4, 2022), https://www.cybercom.mil/Media/News/Article/3179270/cyber-101-us-cyber-command-history/#:~:text=Established%20on%2021%20May%202010,Meade.

[21] USCYBERCOM operates globally in real time against determined and capable adversaries. Its mission is to direct, synchronize, and coordinate cyberspace planning and operations to defend and advance national interests in collaboration with domestic and international partners. USCYBERCOM defends military information systems, supports all military branches with cyberspace operations, as well as defends the country from significant cyberattacks.

behavior" [22] since it was governmental interference into another state's political system. This resulted in states establishing laws that govern election interference as well as the Biden Administration sanctioning Russia for their actions after it was found they interfered once again in the 2020 presidential election.

Over the years, several presidential administrations have attempted to develop a military operational framework under the Office of Legal Counsel. This framework consisted of what Robert Chesney describes as a "separation of power" analysis.[23] At times, this type of engagement does not require congressional authorization if military cyber operations are conducted alone and outside of normal war operations, such as through the execution of physical movements.

International Law

There is no doubt that international law on cyber warfare needs to be established. The recent attacks following the Israeli-Hamas unrest has proven that there is a need for international laws that should address cybercrimes. Iran's cyber operations in support of the Hamas regime have showed its sophistication of cyber capabilities that some may say have straddled the international law line of demarcation for cyber warfare. Iranian cyber threat activity has been prevalent since the October 2023 attack on Israel by Hamas. Iran has been spearheading a series of cyber attacks in support of Hamas to weaken the Israeli government.

The Ukraine-Russia conflict has also shown how cyber attacks are prevalent within armed conflicts. In the months leading up to and after Russia's invasion began, Ukraine experienced a series of disruptive cyber operations, including website defacements, distributed denial-of-service (DDoS) attacks, and cyber attacks to delete data from computers belonging to government and private entities. For example, the United States has assessed that Russian military cyber operators have deployed multiple families of destructive wiper malware, including WhisperGate, on Ukrainian Government and private sector networks. These disruptive cyber

[22] Jens Ohlin, "Did Russian Cyber Interference in the 2016 Election Violate International Law?", 95 Texas L.R.1579 (2017).
[23] Robert M. Chesney,"The Domestic Legal Framework for US Military Cyber Operations", Aegis Series Paper No. 2003, Hoover Working Group, on National Security, Technology, and Law, Aegis Series Paper No. 2003 (July 29, 2020), available https://www.lawfareblog.com/domestic-legal-framework-us-military-cyber-operations.

operations began in January 2022, prior to Russia's illegitimate invasion of Ukraine and have continued throughout the war.[24]

As of the writing of this article, there is not a complete body of law that covers all circumstances. However, some attributes of international law that are relevant to cyber warfare (as previously indicated) include the prohibition on the use of force and the laws on the interference of domestic affairs of other states and humanitarian law.

In terms of specific non-binding legal references, there is one major reference called the Tallinn Manual: International Law Applicable to Cyber Warfare that was developed by the NATO's Cooperative Cyber Defense Center of Excellence. It is important to emphasize that it is solely a guideline for states to consider applying when assessing the legality of cyber operations under international law. It is not legally binding and only utilized as a reference point on how to combat cyber attacks.

The Tallinn Manual

As, previously stated, one of the most significant sets of non-binding rules that address the use of cyberspace when conducting military operations is the Tallinn Manual. This manual provides guidance on how international law applies to various scenarios involving cyber operations, including those that take place during wartime conflict.

The original Tallinn Manual[25] was first published in 2013 by an independent group of experts originated by the NATO Cooperative Cyber Defense Centre of Excellence (CCDCOE). It addressed the most severe cyber operations, which are those that violate the prohibition of the use of force, entitle states to exercise their right to self-defend, or occur during armed conflict. It emphasizes the existing rules of international law. The manual aims to address the increasing relevance of cyber operations in the context of armed conflict and provides a framework for understanding and analyzing the legal aspects of such.

---

[24] U.S. Department of State, Statement by the Secretary of State on the U.S. Response to Actions Taken by Russia Against Ukraine: "Attribution of Russia's Malicious Cyber Activity Against Ukraine", (May. 2022.), https://www.state.gov/attribution-of-russias-malicious-cyber-activity-against-ukraine/.

[25] Michael N. Schmitt, "Tallinn Manual on the International Law Applicable to Cyber Warfare", (2nd ed., Cambridge Univ. Press 2017), https://www.onlinelibrary.iihl.org/wp-content/uploads/2021/05/2017-Tallinn-Manual-2.0.pdf.

The Tallinn Manual has become an influential cornerstone for legal advisers and policy experts dealing with cyber issues.[26] Over the years it has drawn upon existing international law, treaties, state practices, and legal opinions to analyze how the established legal principles and rules can be applied in the cyberspace domain. The principles established by the Report remain relevant, providing a solid foundation for ongoing discussions on securing the future of the digital world. The 95 principles established by international law experts have become authoritative. Each rule is related to international law and how it codifies the combating of cyber warfare. These include provisions for states on how to respond if cyber force is used by another state that results in significant humanitarian damage to include loss of life.

One would ask how important this manual is when it is not legally binding. By formulating a framework of rules, this encompasses all laws applying to cyberspace that all NATO allies have already established within their own borders. An example of this is the establishments as described previously in the United States, such as military development programs and Congress intervention. Additionally, the comprehensive report attempts to merge the rules of international law and its relevancy with cyber space.

While the Manual has a significant contribution to cyberspace governance, it faces substantial challenges in achieving legal merit for combating cyber warfare. Despite its comprehensive approach to applying existing international law to cyber operations, the manual lacks binding authority as it represents expert opinion rather than codified international law. This non-binding nature significantly limits its enforceability and universal acceptance among states. Additionally, the rapid evolution of cyber technologies often outpaces the manual's ability to provide timely and relevant guidance, potentially rendering some of its provisions obsolete shortly after publication. The manual also struggles with the fundamental issue of attribution in cyberspace, a critical element in establishing state responsibility and justifying responses to cyber attacks. Furthermore, its focus on state-centric warfare may not adequately address the increasing role of non-state actors in cyber conflicts.

Lastly, the diverse and often conflicting national interests in cyberspace have hindered widespread agreement on the manual's interpretations, particularly regarding the thresholds for use of force and armed attack in the cyber domain. These limitations collectively undermine the Tallinn Manual's legal efficacy in providing a robust framework for combating cyber warfare on a global scale.

---

[26] Michael N. Schmitt, "Tallinn Manual on the International Law Applicable to Cyber Warfare" (2nd ed., Cambridge Univ. Press 2017), https://www.onlinelibrary.iihl.org/wp-content/uploads/2021/05/2017-Tallinn-Manual-2.0.pdf.

The Budapest Convention On Cyber Warfare

The Budapest Convention on Cyber Warfare was a critical step towards the establishment of laws and the usage of cyber weapons during armed conflicts. It is a treaty that was established in 2011 by the Netherlands and signed by over 20 states to include superpowers such as the United States, China, Russia, and the United Kingdom. The treaty establishes that cyber attacks can only be launched during armed conflict and that they must comply with the doctrine of proportionality and distinction. This treaty recognizes the importance of protecting communication networks and critical infrastructures from cyber attacks.

It also encourages states to not only take preventative measures to secure their own systems, but also aid other nations to prevent and respond to any major cyber attack. For example, under the Budapest Convention, treaty states are required to ensure that the offenses against and by means of computers that are criminalized in their domestic law, and that their criminal justice authorities have the powers prescribed in their procedural law not only to investigate cybercrime but any offense where evidence is in electronic form.[27]

However, the Budapest treaty has its limitations. First, being a part of the treaty is on a volunteer basis, meaning not all states agreed nor signed on to it. Secondly, it does not provide clear legal guidance on the attribution of an attack, which means that it would make it difficult to hold any party responsible. The guidance within the agreement can be changed at any time depending on the state's individual needs and circumstances that seem relevant. Lastly, the treaty only applies to state actors and not to terrorist groups and other non-state actors. This can be viewed as problematic considering that over the years, these groups have been at the forefront of being the major players in cyber attacks.

Obstacles To The Application Of International Law To Cyber Warfare

Challenges In Countering Cyber Attacks

Combatting cyber attacks is a difficult task that requires significant resources, expertise, and collaboration. These malicious activities involve exploiting vulnerabilities in computer systems or networks to gain unauthorized access, steal data, or cause damage. One of the main reasons why cyber attacks are challenging to combat is their ever-evolving nature. Hackers and cybercriminals consistently develop new tactics and techniques to bypass security

[27] Council of Europe, Cybercrime Convention Committee, "The Budapest Convention on Cybercrime: Benefits and Impact in Practice", last visited May 2023.

measures and exploit vulnerabilities. For instance, they may use sophisticated malware or phishing emails that appear legitimate to trick users into giving up sensitive information or installing malware. Additionally, cyber attacks can target different types of systems, including cloud computing, and mobile devices, making it harder to secure them all.

Recently, states have shown their vulnerability in cyberspace. An example would be the U.S. election of 2016 in which President Donald. J. Trump prevailed. Within this timeframe, it was established that Russia and other states infiltrated various systems to interfere with the election process. On January 2017, a report published by the Office of the Director of National Intelligence ("ODNI Report") is one of the most authoritative, declassified reports on Russian interference in the 2016 election. The report attributes the Russian election meddling operation to President Vladimir Putin himself. The report also states that the operation was intended to "undermine public faith in the U.S. democratic process, denigrate Secretary Hillary Clinton, and harm her electability and potential presidency".[28]

This type of cyber interference is harder to combat. The Russian hacking showed the United States' vulnerability within what is often perceived as having a strong safeguard within the cyber community. Similarly, some states may not have robust security measures in place, such as firewalls, intrusion detection systems, or data backups. As a result, cyber attackers can exploit these weaknesses to launch attacks that are difficult to detect and mitigate.

Political Ramifications Of Cyber Warfare

Political implications when it comes to combatting cyber warfare, seem to be a major reason why minimizing the potential of cyber warfare has not always been a major priority for It is safe to say that cyber warfare is one of the most significant modern threats to security on a global scale.

However, every state's definition of cyber warfare has been a political challenge, and consensus is lacking among nations. This has made it difficult for states to agree on the rules of engagement and respond accurately to any cyber attacks. The definition of what is considered a crime that could fall under an international law is at the level of what that particular state believes is important. If Chinese cyber hackers stole the mechanisms of Apple and its servers or the NATO's servers, would it be a crime or viewed as a violation

[28] Alex Xiao, "Responding to Election Meddling in the Cyberspace: An International Law Case Study on the Russian Interference in the 2016 Presidential Election", 30 Duke J. Comp.& Int'l L. 3, 49-78 (2020) (discussing Russian interference in the 2016 election) https://scholarship.law.duke.edu/djcil/vol30/iss2/6.

of the law of war?[29] The consequences of treating attacks such as these as a violation of the law of war can be severe compared to the violation of criminal laws that an impasse in selecting the appropriate choice of law could derail an entire negotiation.[30]

Another perspective is also that the United States and Russia have different interpretations of what constitutes a cyber attack. While the United States believes that cyber attacks should be considered an act of war, Russia on the other hand, believes that it is a form of espionage.[31] These interpretations affect how these states respond to cyber attacks, which in turn creates a level of uncertainty within the international community.

Proposed Solutions

In order to combat cyber attacks, states would need to mutually agree to adopt a multi-layered approach that includes prevention, detection, response, and recovery. An overall solution to preventing cyber warfare is establishing international norms and agreements governing cyber activities. This involves developing rules of engagement for cyber warfare, setting standards for responsible behavior in cyberspace, and creating mechanisms for cooperation and methods of sharing information among nations. Agreements like these could help reduce the risk of accidental or intentional escalation of cyber conflicts and promote stability in cyberspace. This also entails a development of contingency plans that involve conducting regular drills to test the effectiveness of these measures.

In response to the growing risk posed by these activities, the U.S. has recognized the need for a multifaceted cyber defense strategy, which includes the use of force as a potential tool to combat cyber warfare. While the application of kinetic force in response to cyber-attacks remains a debated issue under international law, it is essential for the U.S. to articulate a clear policy that outlines when cyber operations may cross the threshold into the use of force. This needs to be consistent with the international agreements of article 2(4) of the Charter prohibits the threat or use of force and calls on all members to respect the sovereignty, territorial integrity and

[29] The law of war is the component of international law that regulates the conditions for initiating war and the conduct of warring parties. Law of War, E Scholarly Community Encyclopedia (Oct 08, 2022), https://encyclopedia.pub/entry/28473#:~:text=The%20law%20of%20war%20is,critical%20terms%20of%20international%20law.

[30] Laurence Muir,. "The Case Against an International Cyber Warfare Convention", 2 Wake Forest L. Rev. Online 5 (2011).

[31] Cyber Operations Tracker, Council on Foreign Relations, https://www.cfr.org/cyber-operations/, (last visited 2022).

political independence of other States.[32] Cyber attacks capable of causing physical destruction or significant loss of life may justifiably be considered equivalent to conventional armed attacks, thus triggering the right of self-defense.[33]

In theory, the U.S. can employ cyber operations as an effective response to deter or disrupt foreign actors engaging in cyber attacks. For example, the concept of "active defense" has gained prominence in the defense field. This is the capability of the U.S. to counterattack in cyberspace, targeting the command-and-control infrastructure of adversaries involved in launching these attacks.[34] This approach not only reinforces the deterrent effect but also limits the scope of escalation, ensuring that the response is tailored to the threat posed. By adopting active defense measures, the U.S. can effectively neutralize threats while adhering to the principles of the rules of law and international law.

Disadvantages Of The Solution

A technological disadvantage of this solution is that attackers will always find a way around any system and laws. Tracking down private entities or terrorist adversaries to prosecute will be a difficult task. A state may view certain things as a threat, where others would not. An example of this is the usage of TikTok. The United States government views TikTok as a potential threat that can provide hackers with private information that eventually can lead to leaving a country in a vulnerable state and potential Chinese propaganda. However, China, the originators of this app, do not believe that is the case and are attempting to block the potential ban. [35]

The proposed TikTok ban in the United States has sparked significant legal and diplomatic debate, highlighting the complex interplay between national security concerns and international digital commerce. As the Biden administration continued to scrutinize the Chinese-owned app's data practices and potential ties to the Chinese government, China responded with a multifaceted

[32] *Id.*
[33] Marco Roscini, "Cyber Operations and the Use of Force in International Law", (Oxford University Press 2014) 53.
[34] Oona A. Hathaway, et al. "The Law of Cyber-Attack" 100 California Law Review 4, (2012).

[35] Celine Gruaz & Gabriel Lazo., "Necessary and Proportionate? TikTok Bans and American Obligation Under International Human Rights Laws" (March 10, 2023), https://bpb-us-e2.wpmucdn.com/sites.uci.edu/dist/2/4290/files/2023/03/NP-Human-Rights-and-a-TikTok-Ban-FINAL.pdf.

approach to mitigate the risk of a ban. Beijing's strategies include lobbying efforts in Washington, proposed data security measures, and the exploration of a potential spin-off of TikTok's U.S. operations[36]. These efforts are set against the backdrop of escalating tensions between the two nations, particularly in the realm of technology and data sovereignty. The ongoing negotiations and legal challenges surrounding TikTok's fate in the U.S. market underscore the evolving nature of digital governance and the challenges posed by transnational technology platforms in an era of increasing geopolitical competition.

The challenge of addressing cyber warfare on a global scale is further complicated by the need to regulate individual and private entities' cybersecurity practices. While interstate agreements can be formulated, the decentralized nature of the internet presents a significant hurdle in implementing comprehensive cybersecurity measures. The current paradigm of a largely unrestricted internet would necessarily shift towards a more monitored and regulated environment if robust cyber laws were to be enacted and enforced effectively.

This transition raises complex questions about the balance between security and freedom in the digital realm. A parallel can be drawn with the current approach to hate speech regulation in Europe. Many European countries have implemented strict laws against hate speech online, requiring platforms to monitor and remove offending content promptly. While these measures aim to create a safer online environment, they have also sparked debates about freedom of expression and the potential for overreach in content moderation. Similarly, any global cybersecurity framework would need to carefully navigate between necessary oversight and the preservation of internet freedoms, ensuring that security measures do not unduly infringe upon freedom of rights pertaining to online activities.

Additionally, because of the anonymity of the technology involved, attribution of a cyber-attack to a specific state may be difficult. While a victim state might ultimately succeed in tracing a cyber-attack to a specific server in another state, this can be an exceptionally time-consuming process, and even then, it may be impossible to definitively identify the entity or individual directing

[36] Didi Tang & Haleuya Hadero, "The TikTok Law Kicks off a New Showdown Between Beijing and Washington. What's Coming Next?", (April 26, 2024), https://apnews.com/article/tiktok-ban-china-lawsuit-biden-42840d6596dbb6671442db94fe95cddd.

the attack. For example, the "attacker" might well have hijacked innocent systems and used these as "zombies" in conducting attacks.

Historically states acting on the perceived legal requirement that they must conclusively attribute a cyber attack to another state, or its agents have chosen to respond to cross-border cyber attacks as they would to criminal matters, employing only "passive" measures to and urging the states from which the attacks originated to investigate and prosecute those responsible.[37]

Advantages To Solutions

The development of a comprehensive global framework presents numerous advantages in addressing the evolving landscape of digital threats. Such a system would establish a unified set of laws and norms, creating a more predictable and stable international environment in cyberspace. By treating cyber attacks through the same lens as physical warfare, this approach would leverage existing legal structures and precedents, facilitating a more seamless integration of cyber considerations into established international law.

This alignment would not only clarify the rules of engagement within cyberspace but also provide a solid foundation for deterrence, as potential aggressors could face clearly defined consequences for their actions within the international criminal court system. Furthermore, a global system would foster increased cooperation among nations, enabling not only accountability, but more effective information sharing, joint response efforts, and collective defense strategies against cyber threats.

This would hold states accountable for their actions in cyberspace, regardless of their technological capabilities or geopolitical influence. By establishing universal standards and enforcement mechanisms, the international community could more effectively address issues of attribution, retaliation, and proportionality in cyber conflicts. This would help mitigate the current asymmetry in cyber capabilities among nations and reduce the potential for escalation of cyber incidents into kinetic conflicts. Moreover, applying the laws of war to cyber attacks would provide a clearer pathway for conflict resolution and post-incident recovery, potentially reducing the long-term impacts of cyber warfare on global stability and economic well-being. As cyber threats continue to evolve and intensify, the implementation of such a systemic approach becomes increasingly critical in safeguarding international security and promoting a more stable digital future.

[37] J. Madubuike-Ekwe, "Cyberattack and the Use of Force in International Law" Beijing Law Review, 12, 631-649 (2021).

Conclusion

As states increasingly rely on digital infrastructure, the potential for conflicts in cyberspace has become more of a pressing concern. Traditional concepts of warfare are ill-equipped to handle the nuances of cyber attacks, blurring the lines between state and non-state actors. As such, there are many adversities that arise when one is attempting to apply international law to cyber space. As it seems, armed cyber operations within cyber warfare have already been established. However, the uncertainty of applying laws outside of armed conflict seems to be a problem that has not been resolved by any state. There is much work that needs to be done collectively among all the states. In order to function properly within the cyber world, states will need to all be in agreement.

Understanding cyber warfare through the lens of international law is crucial for preventing and mitigating conflicts. Treaty interpretation is different from customary international law. Although states practice can be relevant for treaty interpretation under the rubric of subsequent practice of the parties, there are substantial constraints on the application of this methodology.[38] By providing clear guidelines for the responsible use of cyber capabilities, international law can help prevent misunderstandings and ensure that cyber attacks are met with an appropriate response. As cyber warfare continues to evolve, it is critical that we must continue to reassess legal parameters of the use of force to address this new reality of conflict. The realization is that, while many states have their variation or suggested non-binding legal framework when it comes to the prevention of cyber warfare, there are not any cyber specific international laws, to include treaties between states, or similar formulation and methodologies. Any state that relies solely on cyber warfare will avoid any type of law or at least figure out a way around the system, whereas other states who have strong anti cyber warfare systems will address an attack with some sort of cyber response.

[38] International Covenant on Civil and Political Rights art. 17, Dec. 19, 1966, S. EXEC. DOC. E (1978), 999 U.N.T.S. 171.