CYBER WARFARE AND GLOBAL LEGAL CHALLENGES

Ritesh Kumar, PG Diploma in Cyber Law, Indian Law Institute (ILI), New Delhi

ABSTRACT

The term cyber warfare is one that is used in mainstream media and as with information warfare, there are many differing definitions. In 2001, Alford [1] defined cyber warfare as:

'Any act intended to compel an opponent to full our national will, executed against the software controlling processes within an opponents' system'.[2]

Cyber warfare refers to the use of digital attacks by one nation-state to disrupt the vital functioning of another nation's computer systems. These attacks can include a range of actions, such as hacking, denial-of-service attacks and the deployment of malware. The main intention of cyber warfare is to cause some significant harm to the targeted region. This damage can be physical as well as virtual. Cyber warfare represents one of the most significant challenges to global security in the 21st century. As nations increasingly rely on digital infrastructure, the potential for cyberattacks to disrupt economies, governments and societies has grown exponentially. The cyber domain presents unique challenges that distinguish it from traditional forms of warfare. The anonymity afforded by the internet allows aggressors to operate covertly, complicating attribution and accountability. As technology continues to evolve, the implications of these actions raise critical questions in the realm of international law, state sovereignty and human rights. Moreover, the transnational nature of cyberspace means that attacks can originate from anywhere, making it difficult for states to implement effective legal and diplomatic responses.

This paper explores the evolving landscape of cyber warfare, the legal challenges posed by cyber warfare, focusing on the inadequacies of existing international law, its implications for international law, the difficulties in attribution and the implications for state sovereignty. The paper also scrutinizes key case laws that have shaped the legal landscape of cyber warfare and proposes recommendations for a more robust legal framework to address these challenges of regulating cyber operations.

[1] L. Alford, Cyber warfare: A new doctrine and taxonomy, US Air Force, 1640 accessed 25/05/14 (April 2001).
[2] Cyber warfare: Issues and challenges, https://www.researchgate.net/publication/276248097 (last visited on March 13, 2025), Page No. 8.

Introduction

The advent of the digital age has revolutionized the way nations interact, conduct business and wage war. Cyber warfare, defined as the use of digital attacks to disrupt, damage, or destroy an adversary's computer systems, networks, or information, has emerged as a potent tool in the arsenal of modern states. The rise of cyber warfare has transformed the landscape of conflict, presenting unprecedented challenges to international law and global security. Unlike traditional warfare, cyber warfare operates in a domain that is often ambiguous, intangible and characterized by rapid technological advancements.

This paper explores the multifaceted legal challenges posed by cyber warfare, focusing on key international legal principles and relevant case studies that illustrate the complexities involved.

Through a detailed examination of legal frameworks, state responsibility and the implications of cyber operations, the analysis aims to shed light on the pressing need for a cohesive and adaptive legal response to the challenges of cyber warfare. This paper aims to explore these challenges, focusing on the inadequacies of existing legal frameworks, the difficulties in attributing cyber attacks and the implications for state sovereignty.

Kinds of Weapons used in Cyber Warfare –

1. **Malware**

   a. Purpose: Gain unauthorized access, steal data, or sabotage systems.

   b. Types:

      1) Viruses/Worms: Self-replicating programs that spread through networks (e.g., *Stuxnet*, which targeted Iran's nuclear facilities).

      2) Trojans: Malware disguised as legitimate software to create backdoors (e.g., *Emotet* for stealing financial data).

      3) Ransomware: Encrypts data until a ransom is paid. (e.g., *WannaCry* disrupted hospitals globally in 2017).

4) Spyware: Secretly monitors activity (e.g., *Pegasus* spyware targeting journalists and activists).

5) Wipers: Destroys data (e.g., *NotPetya* masqueraded as ransomware but wiped systems in Ukraine and beyond).

2. Distributed Denial-of-Service (DDoS) Attacks:

a. Purpose: Overwhelm servers or networks to crash them.

b. Example: The 2007 DDoS attacks on Estonian banks, media and government sites, attributed to Russian actors.

3. Advanced Persistent Threats (APTs):

a. Purpose: Long-term espionage or sabotage by infiltrating networks undetected.

b. Example: APT29 (Cozy Bear), linked to Russia, targeted the 2016 U.S. election and the SolarWinds hack (2020).

4. Zero-Day Exploits:

a. Purpose: Exploit unknown vulnerabilities in software/hardware before patches are available.

b. Example: The EternalBlue exploit (developed by the NSA and leaked in 2017) was used in WannaCry and NotPetya attacks.

5. Botnets:

a) Purpose: Networks of infected devices (zombies) controlled remotely to launch large-scale attacks.

b) Example: The Mirai botnet hijacked IoT devices to take down major websites like Twitter and Netflix in 2016.

6. Phishing and Social Engineering:

a) Purpose: Trick users into revealing sensitive data or granting access.

b) Example: State-sponsored phishing campaigns (e.g., Chinese group APT10 targeting corporate intellectual property).

7. Logic Bombs:

a) Purpose: Malicious code triggered by specific conditions (e.g., a date or event).

b) Example: The Sony Pictures hack (2014), attributed to North Korea, used logic bombs to erase data.

8. AI-Powered Cyber Weapons:

a) Purpose: Automate attacks, evade detection, or generate deepfakes for disinformation.

b) Example: AI-generated fake videos (deepfakes) used to spread propaganda or manipulate stock markets.

9. Supply Chain Attacks:

a) Purpose: Compromise software/hardware vendors to infect downstream users.

b) Example: The SolarWinds hack (2020) inserted malware into a trusted IT management tool, impacting U.S. agencies.

10. Cyber-Physical Weapons:

a) Purpose: Target industrial control systems (ICS) or critical infrastructure.

b) Example: Stuxnet (2010) physically damaged Iranian uranium centrifuges by altering their operational speeds.

11. Digital Arrest:

a) Purpose: Criminal impersonate law enforcement officers and scare people in coughing up money

b) Example: Hyderabad Resident AV Mohan Rao, a 79- year old retired consultant, lost Rs 2 crore to scammers posing a officers from Mumbai Police.

The Legal Landscape Governing Cyber Warfare-

1. The Inadequacies of International Law

International law, particularly the United Nations Charter, was designed to regulate traditional forms of warfare and does not adequately address the unique characteristics of cyber warfare. The principles of sovereignty, nonintervention and the prohibition of the use of force, as enshrined in the UN Charter, are difficult to apply in the context of cyber-attacks. For example, Article 2(4) of the UN Charter prohibits the threat or use of force against the territorial integrity or political independence of any state. However, it is unclear whether a cyber-attack that disrupts a nation's critical infrastructure but does not result in physical damage or loss of life constitutes a "use of force" under international law.

2. International Humanitarian Law (IHL) [3]

International Humanitarian Law (IHL), particularly the Geneva Conventions, provides crucial guidelines for armed conflicts, including principles of distinction, proportionality and necessity. These principles must be considered in the context of cyber warfare:

1. **Distinction:** Combatants must distinguish between military targets and civilian objects. In cyber operations, the challenge lies in identifying military objectives without inadvertently targeting civilian infrastructure.

[3] Dr. Nils Melzer, Cyber warfare and International Law-2011

For example, the 2007 cyber attacks on Estonia, attributed to Russian actors, led to significant disruptions in civilian services.

2. **Proportionality:** Any attack must do proportional harm to civilian life relative to the anticipated military advantage. Cyber operations can have cascading effects, complicating assessments of proportionality.

3. **Necessity:** Attacks must be necessary for the achievement of military objectives. The potential for collateral damage in cyberspace raises ethical and legal dilemmas regarding what constitutes a necessary action.

3. United Nations Charter

The United Nations Charter prohibits the use of force in international relations except in self-defence or with Security Council authorization. Cyber operations that result in significant damage can potentially violate this principle. Certain laws must be derived from customary law as reflected in state practice and ‘ opinio juris’ and identified in international jurisprudence. For instance, the 2010 Stuxnet virus, which targeted Iran’s nuclear facilities, raises questions about whether such an attack constitutes a use of force under international law.

4. The Tallinn Manual [4]

The Tallinn Manual, a non-binding document developed by a group of international legal experts, represents one of the most comprehensive attempts to apply existing international law to cyber warfare. The manual outlines how international law, including the laws of armed conflict, applies to cyber operations. However, the manual is not without its limitations. For example, it does not address the issue of state responsibility for cyber-attacks conducted by non-state actors, such as hacktivist groups or cybercriminals.

[4] Schmitt, M. N. (Ed.). (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge University Press.

5. The Role of Customary International Law

Customary international law, which is derived from the consistent practice of states accompanied by opinion juris (the belief that such practice is legally obligatory), may play a role in filling the gaps left by treaty law. However, the rapid evolution of cyber technology and the lack of consistent state practice in responding to cyber-attacks make it difficult to establish customary norms in this area.

Indian Laws dealing with Cyber Warfare –[5]

India does not have a dedicated "cyber warfare law", but several existing laws and policies, more so from IT Act 2000 which address cyber threats, cyber terrorism and national security concerns related to cyber warfare. If left unchecked India attracts nearly 1 trillion cyber attacks annually and by the time Nation turns 100 in 2047, the country would be a target of 17 trillion cyber attacks, according to projections.

Below are the key legal frameworks and institutions that deal with cyber warfare and related offenses:

1. Information Technology Act, 2000 (IT Act)

The primary law governing cyber activities in India. Key sections relevant to cyber warfare include:

a) **Section 66F (Cyber Terrorism)**:

i. Criminalizes acts that threaten national security, such as unauthorized access to restricted systems, data theft, or disruption of critical infrastructure.

ii. Punishment: Life imprisonment.

b) **Section 70 (Protected Systems)**:

[5] Shrikar Ventrapragada, https://blog.ipleaders.in/need-know-cyber-warfare/, (last visited on March 13, 2025).

i. Criminalizes unauthorized access to government-designated "protected systems" (e.g., power grids, defense networks).

c) **Section 43 & 66**:

i. Address unauthorized data breaches, computer contamination (malware) and DDoS attacks.

d) **Section 69**:

i. Allows the government to intercept, monitor or decrypt data for national security purposes.

2. Bhartiya Nyaya Sanhita 2023 (Earlier, Indian Penal Code (IPC), 1860):

a) **Section 147 (Waging War Against India)**:

i. Applies to cyberattacks intended to destabilize India's sovereignty (e.g., attacks on defense systems).

b) Section 196 (Promoting Enmity):

i. Targets cyberattacks aimed at inciting communal or social discord (e.g., disinformation campaigns).

c) Sections 323 (Data Theft) & 324 (Sabotage):

i. Criminalize cyberattacks causing financial or infrastructure damage.

3. National Cyber Security Policy (2013)

i. Focuses on securing critical infrastructure (e.g., banking, energy, transportation) and building cyber defence capabilities.

ii. Mandates the creation of the **National Critical Information Infrastructure Protection Centre (NCIIPC)** to protect systems like power grids and defense networks.

4. Unlawful Activities (Prevention) Act (UAPA), 1967

i. **Section 15:** Defines "terrorist acts," which include cyberattacks intended to threaten India's security or economic stability.

ii. Used to prosecute state-sponsored hackers or groups involved in cyber warfare.

5. Defence Cyber Agency (DCA)

i. A tri-service agency under the Ministry of Defence (established in 2018) to counter cyber threats targeting military systems and critical infrastructure.

ii. Works with the **National Technical Research Organization (NTRO)** for cyber intelligence.

6. CERT-In (Indian Computer Emergency Response Team)

i. Mandated under **Section 70B of the IT Act** to handle cybersecurity incidents, issue alerts and coordinate responses to large-scale cyberattacks (e.g., ransomware, APTs).

7. Draft Digital Personal Data Protection Act (2023)

i. Aims to secure sensitive data from breaches (e.g., citizen data leaks used in hybrid warfare).

8. International Cooperation

i. India collaborates with global agencies like **INTERPOL** and **ITU** to counter cross-border cyber warfare.

ii. Bilateral agreements with countries like the U.S. (Cyber Relationship Framework, 2016) to share threat intelligence.

Attribution and Accountability Challenges in Cyber Warfare (Case laws)-

1. The Problem of Anonymity

One of the most significant challenges in addressing cyber warfare is the difficulty in attributing cyber-attacks to specific actors. Cyber attackers often operate anonymously, using sophisticated techniques to conceal their identities and locations. This makes it difficult for victim states to respond effectively, as they may not know who to hold accountable. One of the most significant challenges in cyber warfare is attributing attacks to specific actors. The lack of clear evidence and the ability of malicious actors to obfuscate their identities complicate the enforcement of legal norms.

Several cases illustrate this dilemma: [6] [7]

1. **Case: The Estonian Cyber Attacks (2007)**

   The 2007 cyber-attacks on Estonia, which targeted government, financial and media websites, highlight the challenges of attribution in cyber warfare. Although the attacks were widely believed to have been orchestrated by Russian state actors, definitive proof was difficult to obtain. The Estonian government sought assistance from NATO, but the lack of clear attribution made it difficult to invoke collective defense mechanisms under Article 5 of the NATO Treaty.

2. **Case: The Sony Pictures Hack (2014)**

   The 2014 hack of Sony Pictures, which was attributed to North Korean state actors, further illustrates the challenges of attribution. The film 'The Interview ' was based on an interview with the North Korean Leader Kim Jong Un in which the leader was said to be wrongly portrayed. The U.S. government imposed sanctions on North Korea in response to the attack, but the attribution was based on circumstantial

[6] Schmitt, M. N. (Ed.). (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge University Press, page [28]
[7] Shrikar Ventrapragada, https://blog.ipleaders.in/need-know-cyber-warfare/, (last visited on March 13, 2025).

evidence and intelligence rather than definitive proof. This raises questions about the legal standards required for attributing cyber-attacks to state actors.

3. **Case: The 2016 U.S. Presidential Election interference:**

Investigations highlighted Russia's involvement in cyber activities aimed at influencing the election. A report on the presidential Elections by special counsel Robert Mueller concluded that Russia was involved in influencing the US Presidential election, 2016. The Mueller report found that Russia made use of social media to disrupt the political situation in U.S., using a 'information malware' Despite consensus among intelligence agencies regarding the attribution legal consequences remain elusive.

4. **Case : The NotPetya Attack:**

This cyber incident, attributed to Russian state-sponsored actors, inflicted widespread damage on both Ukrainian and global systems. However, establishing liability under international law has proven challenging.

5. **Case: DDOs Attack on Ukraine, 2014:**

The propaganda by the Russian Government by conducting a DDoS attack that destroyed the internet services in Ukraine, which led to Russian rebels, taking control of Crimea, a city in Ukraine.

6. **Case: China's hack into US Telecom system, 2014:**

China's alleged recent breach of the innermost workings of the US Telecommunications system reached far deeper into the President office and hackers were able to listen in on Telephone conversations and read Text messages,even held by well connected Americans, including their President Donald Trump and Vice President JD Vance. The hack is assumed to be engineered by a group linked to Chinese intelligence that

has been named as 'Salt Typhoon' by Microsoft ,whose cyber security Team had discovered the act.

7. **Case: AIIMS ransomware attack**

A ransomware attack on the servers of All India Institute of Medical Sciences (AIIMS), wreaked havoc on their systems causing critical Data breach of crores of Individuals and all the processes had to go manual. The attackers encrypted the existing data, and allegedly demanded Rs 200 crore as ransom.

8. **Case: Take It Down Act [8]**

The 'Take It Down Act' is a bill that makes it a federal crime to knowingly publish or threaten to publish non-consensual intimate imagery on online platforms, which includes "digital forgeries" created by AI. It explicitly includes realistic, computer-generated intimate images depicting identifiable individuals. The bill was introduced in the Senate by Sens. Ted Cruz, R-Texas, Amy Klobuchar and D-Minn and was unanimously passed the Senate, early this year. The proposed law would require penalties of up to three years behind bars for sharing nonconsensual intimate images involving minors, and two years in prison for images involving adults. Further, it would require penalties of up to two and a half years behind bars for threat offenses involving minors, and one and a half years in prison for threats that involve adults. The bill clarifies that consent to create an image does not equate to consent for its publication.

State Sovereignty and Cyber Warfare- [9]

1. The Principle of Sovereignty in Cyberspace:

The principle of state sovereignty, which is a cornerstone of international law,

[8] https://www.hindustantimes.com/world-news/us-news/what-is-take-it-down-act-melaniatrump-pushes-for-anti-revenge-porn-bill-on-capitol-hill-101741051931475.html
[9] Sharona Mann's, Legal challenges in the realm of cyber warfare, Page- [11]

is particularly relevant in the context of cyber warfare. A state's sovereignty extends to its cyber infrastructure and any unauthorized intrusion into that infrastructure may constitute a violation of sovereignty. However, the application of this principle in cyberspace is complicated by the interconnected nature of the internet and the difficulty in determining the origin of cyberattacks.

2. Case Law: The Iranian Nuclear Facility Attack (Stuxnet, 2010)

The Stuxnet worm, which was used to disrupt Iran's nuclear enrichment facilities, is often cited as an example of a cyber -attack that violated state sovereignty. Although the attack was widely believed to have been conducted by the United States and Israel, neither country officially acknowledged responsibility. This raises questions about the legal implications of covert cyber operations and the extent to which they violate the principle of sovereignty.

3. The Role of Non-State Actors

The involvement of non-state actors in cyber warfare further complicates the issue of state sovereignty. Non-state actors, such as hacktivist groups or cybercriminals, may operate across multiple jurisdictions, making it difficult for states to assert control over their cyber activities. This raises questions about the extent to which states are responsible for the actions of non-state actors operating within their territory.

State Responsibility and Cyber Warfare- [10]

State responsibility in the context of cyber warfare entails holding states accountable for actions conducted by non-state actors within their territory, especially if they fail to prevent these actors from launching attacks against other nations. The International Law Commission's Articles on State Responsibility provide a framework for understanding how states may be held liable for cyber operations-

[10] Sharona Mann's, Legal challenges in the realm of cyber warfare, Page- [20]

1. **Active Complicity:**

   If a state knowingly assists non-state actors in launching cyber attacks, it may be held criminally liable. The connection between states and cybercriminal organizations complicates legal actions, as seen with the alleged support of North Korea in various cyberattacks on financial institutions.

2. **Failure to Prevent Attacks:**

   States have a duty to prevent harmful acts emanating from their territory. This principle is evident in cases like the 2020 SolarWinds attack, which exploited vulnerabilities in software that affected numerous U.S. government agencies.

3. **Responses to Cyber Incidents:**

   States must navigate the legal frameworks that govern self-defense in cyberspace. The principle of proportionality must guide responses, as illustrated by the U.S. offensive cyber operations in response to Iranian cyber threats.

The Implications for International Security-

1. The Risk of Escalation

The lack of clear legal norms governing cyber warfare increases the risk of escalation. Without a clear understanding of what constitutes a "use of force" or an "armed attack" in cyberspace, states may be more likely to respond to cyber-attacks with military force, leading to a potential escalation of conflict.

2. The Role of International Organizations

International organizations such as the United Nations and NATO, have a role to play in addressing the legal challenges posed by cyber warfare. However, the effectiveness of these organizations is limited by the lack of consensus among member states on how to regulate cyber activities. For example, efforts to negotiate a cyber arms control treaty have been hampered by disagreements between major powers, such as the United States, China and Russia.

Recommendations-

1. Develop a Comprehensive Legal Framework

There is a need for a comprehensive legal framework to address the unique challenges posed by cyber warfare. This framework should include clear definitions of key terms, such as "use of force" and "armed attack," as well as mechanisms for attributing cyber-attacks to specific actors. It should also address the role of non-state actors and the implications for state sovereignty.

2. Strengthen International Cooperation

International cooperation is essential for addressing the legal challenges posed by cyber warfare. States should work together to develop norms and rules governing cyber activities and international organizations, such as the United Nations and NATO, should play a leading role in this process. This could include the establishment of an international cyber court to adjudicate disputes related to cyber warfare.

3. Enhance Attribution Capabilities

Improving the ability to attribute cyber-attacks to specific actors is critical for addressing the legal challenges posed by cyber warfare. This could involve the development of new technologies and techniques for tracking and identifying cyber attackers, as well as the establishment of international standards for attribution.

4. Promote Cyber Security Education and Awareness

Promoting cyber security education and awareness is essential for addressing the legal challenges posed by cyber warfare. This could involve the development of educational programs and training initiatives to raise awareness of the risks posed by cyber-attacks and the importance of cyber security.

Conclusion

In conclusion, Cyber warfare represents one of the most significant challenges to global security in the 21st century. The rise of cyberwarfare has presented significant challenges regarding the applicability of international humanitarian law for the protection of civilians. Not only do cyber-attacks represent a fundamentally different method of warfare, they come at a time when the laws of armed conflict are struggling to meet the challenges of greater than ever civilian participation in conflict, increased asymmetry and technological advance. The inadequacies of existing international law, the difficulties in attributing cyber attacks and the implications for state sovereignty all contribute to the complexity of this issue. While there have been some efforts to address these challenges, such as the Tallinn Manual, much more needs to be done to develop a comprehensive legal framework that can effectively regulate cyber warfare. International cooperation, enhanced attribution capabilities and increased cyber security education and awareness are all essential components of this effort. Only by addressing these challenges can the international community hope to mitigate the risks posed by cyber warfare and ensure the stability and security of the global digital infrastructure.

REFERENCES

1. L. Alford, Cyber warfare: A new doctrine and taxonomy, US Air Force,1640 accessed 25/05/14 (April 2001).

2. Cyber warfare: Issues and challenges, https://www.researchgate.net/publication/276248097 (last visited on March 13, 2025), Page No. 8

3. Shrikar Ventrapragada, https://blog.ipleaders.in/need-know-cyber-warfare/, (last visited on March 13, 2025).

4. Dr. Nils Melzer, Cyber warfare and International Law-2011

5. Schmitt, M. N. (Ed.). (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge University Press. Talinn Manual https://csef.ru/media/articles/3990/3990.pdf

6. Sharona Mann's, Legal challenges in the realm of cyber warfare

7. United Nations. (1945). Charter of the United Nations. Retrieved from https://www.un.org/en/charter-united-nations/

8. Sumanti Sen, Trump pushes for anti-revenge porn bill on Capitol Hill, https://www.hindustantimes.com/world-news/us-news/what-is-take-it-down-actmelania-trump-pushes-for-anti-revenge-porn-bill-on-capitol-hill101741051931475.html, (last visited on March 17, 2025).

9. Rid, T. (2012). *Cyber War Will Not Take Place*. Journal of Strategic Studies, 35(1), 5-32.

10. Lin, H. (2010). *Offensive Cyber Operations and the Use of Force*. Journal of National Security Law & Policy, 4(1), 63-86.

11. Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., & Spiegel, J. (2012). *The Law of Cyber-Attack*. California Law Review, 100(4), 817885.

12. Kello, L. (2013). *The Meaning of the Cyber Revolution: Perils to Theory and Statecraft*. International Security, 38(2), 7-40.

13. Brenner, S. W. (2009). *Cyber Threats: The Emerging Fault Lines of the Nation State*. Oxford University Press.

14. Goldsmith, J. (2013). *How Cyber Changes the Laws of War*. European Journal of International Law, 24(1), 129-137.

15. Jensen, E. T. (2013). *Cyber Attacks: Proportionality and Precautions in Attack*. International Law Studies, 89, 198-217.

16. Shackelford, S. J. (2014). *Managing Cyber Attacks in International Law, Business and Relations: In Search of Cyber Peace*. Cambridge University Press.

17. DR. M.S. Sharmila & Vishwa. B- 'An enquiry into the legal challenges of cyber warfare in international law' ; https://www.ijlra.com/paper-details.php?isuur=3266