CYBER WARFARE AND INTERNATIONAL LAW: EXPLORING LEGAL COMPLEXITIES IN THE DIGITAL ERA

Author-GAUTAM PATNI
KIRIT P. MEHTA SCHOOL OF LAW, NMIMS MUMBAI
gautampatni5@gmail.com

ABSTRACT

Over the past two to three decades, the term 'cyberwarfare' has gained significant prominence. Given its increasing prevalence, it is crucial for internet users to understand cyberwarfare, its potential to significantly affect their lives, past incidents that serve as precedents, and the valuable lessons that can be drawn for the future. Cyber warfare refers to use of digital attacks by state or non-state actors by exploiting vulnerabilities in digital systems. This can be done to spread misinformation, use military technologies to harm civilians, achieve political, economic, and military advantage, maliciously obtain data which shall breach their privacy. Cyber warfare is not much different from traditional warfare, the international laws of war apply to both, for instance cutting of electricity of a hospital which leads to civilian death is no different from dropping of a bomb. Though, there are instances where cyberwarfare can be exclusively used to achieve any other political or economic objective. Experts often argue whether cyberwarfare would be an alternative to traditional warfare due to its low cost, remote connectivity, and largescale destructions.

This paper aims to inculcate an understanding of cyberwarfare, its types, motive behind such attacks, analysis of documented cyber incidents, use of cyberwarfare strategies and its impact on critical infrastructure and society, the study also aims to explore whether cyberattacks can be classified as "use of force" under Article 2(4) of the UN Charter and whether states have a right to invoke self-defence to such attacks. The role of international organizations in addressing cyberwarfare and to what extent are international laws regarding cyberwarfare effective. The paper emphasizes the importance of enhancing cybersecurity measures and fostering global cooperation to mitigate risks. This paper is based on qualitative research, it conducts an analysis of case studies. The sources cited are secondary, they comprise of articles, laws, and relevant judicial precedent. Readers are requested to immerse themselves and make opinions. Views are personal.

KEYWORDS – cyberwarfare, cyberattack, warfare, digital, military, etc.

RESEARCH OBJECTIVES –

- Understanding of the term cyberwarfare, its types, and motives behind such attacks
- Brief analysis of documented cyber attacks
- Whether cyberattacks can be classified as "use of force" under Article 2(4) of the UN Charter and whether states have a right to invoke self-defense to such attacks.
- Position of States in addressing Cyberwarfare

RESEARCH METHODOLOGY –

In this research, a secondary research methodology has been employed to gather facts, explore the topic of Cyberwarfare. Peer-reviewed publications, online papers, and official reports that provided in-depth studies of the topic is used as qualitative data. Use of blogs, official government sites have been put into use. Official data from UN, authentic articles and blogs have been used to analyze and delve into the study of the topic. Review of international laws, treaties, and policy documents related to cyberwarfare has been conducted to ensure systematic study of the subject. Statistical report regarding the frequency of cyberattacks has been used to understand the global phenomenon. Qualitative data for the purpose of examining real-world instances of cyberwarfare, such as state-sponsored attacks and geopolitical cyber conflicts has been done for comparative study of the subject.

UNDERSTANDING CYBERWARFARE: TYPES AND MOTIVES OF CYBERATTACKS

As the world becomes more digitally interconnected, the vulnerability of critical infrastructure to cyberattacks has increased, making cyberwarfare a significant aspect of modern geopolitical tussle. Cyberwarfare can be characterized as use of digital technology for disrupting the computer system of another individual or government by any state or non-state actor. This can include hacking, spreading malware, or spreading false information[1]. Unlike traditional warfare, which uses physical force, cyberwarfare targets digital infrastructure like power grids, communication systems, and military networks. With more and more systems relying on the internet, cyberattacks have become a key part of modern conflicts. Nations and groups can now launch hidden attacks that may disrupt economies, governments, or security. Over the past 20 years, nearly 20% of reported cyber incidents targeted the global financial sector, resulting in $12 billion in losses for financial firms, according to the IMF's Global Financial Stability Report. Since 2020 alone, losses have totalled about $2.5 billion. The IMF report notes that banks are frequent targets, and actual losses are likely much higher when factoring in indirect costs and reputational damage[2].

---

[1] Alexander S. Gillis, *Cyberwarfare*, Tech target, https://www.techtarget.com/searchsecurity/definition/cyberwarfare

[2] Johnny wood, *global financial stability at risk due to cyber threats, IMF warns. Here's what to know,* world economic forum, May 15,2024,

These attacks can cause damage to critical services, steal important data, or influence public opinion. According to experts' cyberwarfare can be more catastrophic and dynamic, it can have huge consequences for a nation. Cyberwarfare can be characterized as an emerging technology weapon[3] similar to biological and chemical weapon. During World War II and the years immediately following, nuclear and biological weapons were considered groundbreaking advancements in military technology, fundamentally changing the nature of warfare. Similarly, in today's world, cyberweapons—tools used to carry out computer network attacks (CNA)—are emerging as the latest technological innovation in warfare. These weapons have the potential to disrupt critical systems, highlighting the evolving landscape of conflict and defence strategies.

Cyberwarfare raises important issues about international laws and the rules of conflict, as it affects both military and civilian targets. The increasing use of technology in everyday life makes cyberwarfare a powerful tool, but also a risky one for global stability. Let's look back at some of the prominent CNA attacks that happened between 2007-2012 –

- Estonia, 2007, which targeted government and commercial website and the attack was suspected to be sponsored by Russia.
- Syrian air defence, September 2007 which targeted military system and led to degradation of air defence capabilities, the attack was suspected to be done by state of Israel.
- Georgia, July,2008 which affected government and civilian website and suspected to be done by Russia.
- Saudi amarco, a state-owned commercial enterprise which led to large scale destruction of data and led to physical disruption of oil production. This was suspected to be done by Iran.
- Stuxnet, 2009-2010, a computer worm that targeted physical destruction of Iranian nuclear programme. The attack was supposed to be carried by United states.

These five CNA-style attacks offer insight into the development of international norms in cyberwarfare. There are three key points:

1. Many of the attacks were used to sabotage military targets of enemy countries like US using worms to sabotage Iran's nuclear facilities, Russia attacking Syrian air defence, Iran attacking Saudi based MNC Amarco, the list does not end here. There are numerous other such examples.

---

https://www.weforum.org/stories/2024/05/financial-sector-cyber-attack-threat-imf-cybersecurity/

[3] Brian M. Mazanec, *why international order in cyberspace is not inevitable,* vol 9, No. 2 , SSQ, 78, 79-80, (2015)

2. When attacks were limited to military targets, they were likely carried out by Western nations like the U.S. and Israel. This suggests that different nations may follow competing or more lenient norms in cyberwarfare, reflecting a competitive phase in norm development.
3. Cyberwarfare experience is still minimal. No deaths or injuries have been reported from cyberattacks, and physical damage has been limited, though it has affected strategically important targets like Iranian nuclear programme.

These CNA based attacks happened roughly a decade ago, in last some years we have seen how these attacks have evolved and used in military conflicts for instance the pager attacks suspected to be done by Israel, destructive computer network attacks by Russia on Ukraine. Data breaches of Indian users on dark web and several other instances. These incidents shall be discussed in depth in this paper.

TYPES OF CYBER-ATTACKS –

With the rapid advancement of technology, cyberattacks have evolved in both complexity and frequency, posing significant threats to individuals, organizations, and governments. These malicious activities exploit vulnerabilities in digital systems to compromise data, disrupt services, and undermine privacy. As reliance on digital infrastructure is increasing, there is a dire need to address the growing threat of cyberwarfare for ensuring global security and stability. Some of the attacks employed by cyber-criminals are –

a) DOS AND DDOS attacks –

A Denial-of-Service (DoS) attack floods a system with fake traffic, causing it to slow down or crash, making it unavailable to legitimate users. A Distributed Denial-of-Service (DDoS) attack is similar but uses multiple compromised machines to amplify the attack.

Unlike other cyberattacks that steal data or gain control, DoS and DDoS attacks aim solely to disrupt a system's functionality. While attackers don't typically profit from stealing information, they may cause financial harm to businesses, especially if hired by competitors to disrupt operations.

b) MAN IN THE MIDDLE ATTACK (MITM)

A Man-in-the-Middle (MITM) attack occurs when an attacker secretly intercepts and monitors the communication between two parties, such as individuals or computers. The attacker places themselves between the two, without either party knowing.During a MITM attack, both parties believe they are communicating normally, but the attacker may alter or steal the message before it reaches its intended recipient.

c) PHISHING ATTACKS

A phishing attack occurs when an attacker sends fake emails that appear to come from trusted sources to steal sensitive information. The attacker uses a link

to a fraudulent website, tricking the target into downloading malware or revealing private details. The target may not realize they've been compromised, allowing the attacker to target others in the same organization.

d) RANSOMWARE

Ransomware is malware that locks a victim's system until a ransom is paid. The attacker provides instructions for regaining control once payment is made. The malware is often downloaded through a website or email attachment, exploiting security flaws to encrypt files. It can also impact multiple systems or a central server, disrupting business operations.

e) DNS SPOOFING

DNS spoofing redirects traffic to a fake site, where victims may unknowingly enter sensitive info for the attacker to exploit. It can also damage a competitor's reputation. The attacker impersonates a legitimate site to carry out malicious actions.

f) TROJAN HORSE

A Trojan horse attack hides malicious software in a harmless program. When run, it opens a backdoor for hackers to access the system. The term comes from the Greek myth where soldiers hid in a wooden horse to attack Troy, similar to how users unknowingly allow threats by accepting seemingly safe apps.

g) MALWARE ATTACK

Malware is a term for harmful software that affects a computer by altering its functions, damaging data, or spying on the user or network traffic. It can either spread to other devices or stay on its host device, causing damage locally. Malware includes MITM, phishing, ransomware, Trojan horses, XSS attacks etc[4].

MOTIVES BEHIND SUCH ATTACKS –

After months of war between Russia and Ukraine, both sides initiated a series of cyberattacks on each other's government, banking, and other sites. Few of such attacks are mentioned herein Cybersecurity firm ESET identified a new data-wiping software that has infected hundreds of computers in Ukraine, in what officials describe as part of an escalating wave of cyberattacks. The malware, which appears to have been in development for months, was installed on numerous machines across the country. Symantec, another cybersecurity firm investigating the incident, confirmed that the infections have also spread to

---

[4] Fortinet, https://www.fortinet.com/resources/cyberglossary/cyber-warfare, (last visited 18/12/24)

Latvia and Lithuania. While the source of the attack remains unclear, suspicion is focused on Russia, given its history of similar cyberattacks on Ukraine and other nations. Russia has denied any involvement.

The United States and the United Kingdom attributed recent DDoS attacks on Ukrainian banking and government websites to Russian military hackers. On December 20, Ukraine's Deputy Prime Minister, Olha Stefanishyna, reported that a Russian cyberattack on state registries temporarily disrupted services holding vital citizen data, including records of births, deaths, and property ownership.[5] Ukraine responded by forming an "IT army," Vice Prime Minister Mykhailo Fedorov announced. Reuters revealed that Ukraine had enlisted its hacker community to defend infrastructure and conduct cyber espionage. Fedorov tweeted about a Telegram channel listing 31 key Russian entities, including Gazprom, Lukoil, and government sites, and noted, "There were tasks for everyone, and the fight on the cyber front continued[6]." Kremlin.ru, the Kremlin's official website, was reportedly taken offline in a DDoS attack.

- After analysing these events, we can assume that there has been a breach of military and civilian data. This is usually done to monitor any adverse activities using cyberworms or any other malware. Stuxnet was a famous cyberworm reportedly created by the U.S. and Israel to disrupt Iran's nuclear program. Most cyberpower operations, including Stuxnet, operate within specific tactical boundaries. While Stuxnet is often credited with the destruction of 1,000 Iranian centrifuges at the Natanz enrichment facility, this outcome was an indirect result of the malware. Stuxnet created the conditions that led to the damage but did not cause the destruction directly[7].

In another case though not related to any military operation, In October of 2023, the U.S.-based cybersecurity company Resecurity reported that the personal data of 815 million Indians—approximately 55% of the country's population—was being sold on the dark web. This information allegedly included sensitive details such as phone numbers, addresses, and passport data. A hacker known as "pwn001" was reportedly offering this vast database for $80,000. Adding to these concerns, in June 2023, there were reports of a data breach involving vaccinated Indians,

---

[5] Reuters, *Russia conducted mass cyberattack on Ukraine's state registries, deputy PM says,* Reuters, (25.12.24), https://www.reuters.com/technology/cybersecurity/russia-conducted-mass-cyber-attack-ukraines-state-registries-deputy-pm-says-2024-12-19/

[6] James Pearson, *Ukraine launches IT army, takes aim at Russian cyberspace.* Reuters,(25.12.24), https://www.reuters.com/world/europe/ukraine-launches-it-army-takes-aim-russian-cyberspace-2022-02-26/

[7] Lukas Milesvki, *Stuxnet and strategy a special cyber operation in cyberspace*?, issue 63, 4th quarter 2011, https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-63/jfq-63_64-69_Milevski.pdf?ver=Jy0SW9E8UBbatlrmrw-egQ%3D%3D

with personal information being leaked from the CoWIN app and website[8].

In another case from India, on November 23,2022, a cyberattack on All India Institute of Medical Sciences (AIIMS), disrupted systems, erasing outpatient and research data from primary and backup servers. Former National Cybersecurity Coordinator Pant revealed that the network, designed by doctors rather than professionals, had significant vulnerabilities that made it easy to breach. The incident highlighted flaws in cyber defences and prompted the government to draft a National Cybersecurity Response Framework (NCRF) to address such issues[9].

If this was not enough it was revealed in a Threat Intelligence Report reveals that BSNL suffered significant data breaches by hackers "kiberphant0m" and "Perell." In May 2024, "kiberphant0m" infiltrated BSNL's systems, exposing critical data, including IMSI numbers, SIM card details, HLR records, DP card data, and Solaris server snapshots.

This data was offered for $5,000 (~₹4.17 lakh) with samples to verify authenticity, available for purchase briefly from May 30 to 31, 2024. Earlier, in December 2023, "Perell" breached BSNL, leaking 32,000 lines of sensitive data on a dark web forum, including email addresses, billing details, contact numbers, and network records. The hacker claimed the total breach spanned 2.9 million lines, endangering customer privacy and financial security[10].

This proves that India needs a complete revamp of its cybersecurity infrastructure, just as the country has progressed considerably in the IT domain, we need to make sure that cyber security of the country is something which cant be compromised.

- All these cases agree on the fact that cyberwarfare can be used to sabotage another country's military developments, breach the data of civilians, monitor any adverse activities, disrupt the economy, lifestyle etc. There have been incidents like Ukrainian power gird attack which have impacted the lives of common civilians, even traditional warfare in 21st century is subjected to border areas, whereas a cyberattack can affect the lives of common people be it in any part of the state. State or non-state actors can disrupt the economy, affect lives of civilians, and get away with it. The dilemma about cyberwarfare is whether international organizations and laws can control such attacks and whether they can take actions

[8] Danny D'Cruze, *data breach of 81.5 crore Indians: hacker allegedly leaks Aadhar, Passport, personal details on dark web,* business today, October. 31, 2023

[9] Deeksha Bhardwaj, *AIIMS ransomware attack led to a new SOP on cyber breach: Ex- cybersecurity chief pant,* Hindustan Times, 2 July,23

[10] Ashwani Mishra, BSNL breached twice in a year: A deep dive into the state -owned telecom's cybersecurity woes, 63 Stats , 26 June,2024

against such attacks or whether state which gets attacked can take action or can it counter attack the state which perpetrates cyber-attack?

- It is also seen that countries also employ their cyber-criminals to hack into another countries system to show their strength in the field, and to warn the adverse country of consequences in the future. As seen in documented cyber incidents, states obtain sensitive information of citizens of rival states, monitor their activities. Many times, cyber warfare is also used for political propaganda, for instance Russia has employed cyber operations as a tool of political warfare, combining propaganda to divide societies and influence elections. These efforts have included campaigns to deface websites and depict Ukraine's supporters as Nazis. This campaign was followed by a bold attempt to undermine trust in U.S. democracy during the 2016 presidential election, though the extent of its impact remains a topic of debate[11].

BRIEF ANALYSIS OF CYBER ATTACKS –

1) 2015 Ukraine power grid attack –

On December 23, 2015, a cyberattack targeted the power grid in two western regions of Ukraine, causing power outages for about 230,000 people lasting 1 to 6 hours. The attack occurred during the ongoing Russo-Ukrainian War (2014–present) and was linked to a Russian hacker group called "Sandworm." This was the first known successful cyberattack on a power grid. On December 23, 2015, hackers used the BlackEnergy 3 malware to remotely breach the information systems of three Ukrainian energy distribution companies, disrupting electricity for consumers. The hardest hit was Prykarpattyaoblenergo, which services the Ivano-Frankivsk region. The attack shut down 30 substations (7 at 110 kV and 23 at 35 kV), leaving approximately 230,000 people without power for 1 to 6 hours. The attack on December 23, 2015, was meticulously planned, with networks and systems being compromised up to eight months in advance. Understanding this timeline is crucial for identifying effective methods to detect and prevent similar attacks in the future[12].

2) Data breach of Indian users

In October last year, the US-based cybersecurity firm Resecurity reported that the personal data of 815 million Indians—55% of the population—was available for sale on the dark web. This included sensitive information like phone numbers, addresses, and passport details. A hacker known as ‘pwn001’

[11] Grace B Mueller, Benjamin Jensen, *Cyber operations during Russo- Ukrainian war from strange patterns to alternative futures*, Center for strategic and International studies (CSIS), July 13, 2023

[12] Jean-Pierre Hauet, Patrice Bock, Robert Foley, Romain Françoise, *Ukrainian power grids cyberattack,* International society of automation, March,2017

was allegedly selling this data for $80,000[13]. Additionally, in June 2023, there was another alarming breach involving the CoWIN platform, where vaccination data, including information about VIPs and ordinary citizens, was leaked[14].

3) All India Institute of Medical Science Delhi (AIIMS) Ransomware attack

In late 2022, the All India Institute of Medical Sciences (AIIMS), Delhi, suffered a major ransomware attack that forced the institution to revert to manual operations. The attack targeted sensitive data, including patient records, research data, and administrative information, severely compromising patient confidentiality and disrupting critical healthcare services.

The LockBit ransomware gang allegedly demanded ₹200 crore (approximately $24.5 million) in cryptocurrency. The attack caused AIIMS's servers to remain down for six consecutive days, delaying medical care and endangering patient well-being.

This incident underscored the catastrophic impact of ransomware on healthcare organizations, where disruptions can directly jeopardize lives. Garnering widespread media attention, the AIIMS attack served as a wake-up call for global healthcare and government-run institutions, emphasizing the urgent need for robust cybersecurity measures[15].

4) Role of Cyberwarfare in Russia- Ukraine war –

Since Russia's 2022 invasion of Ukraine, cyberwarfare has intensified, with both sides using cyberattacks for propaganda, espionage, and disruption. Anonymous-affiliated groups, such as YourAnonSpider and NB65, targeted Russian networks, temporarily disabling platforms like RuTube and taking down TV servers. Anonymous also breached Russian institutions, including a major intelligence agency and UAV plans.

Russia-linked actors like the FSB, SVR, GRU, and groups such as GHOSTWRITER/UNC1151 have launched disinformation campaigns, espionage, and destructive attacks against Ukraine. Pro-Russia cybercrime groups, including Conti and Killnet, have executed DDoS attacks on critical infrastructure, such as Italy's Defense Ministry.

Ukraine has countered with a volunteer-based "IT Army" of over 400,000 individuals, defending networks and coordinating attacks, while Belarusian Cyber Partisans have also targeted Russian systems, albeit with limited impact.

---

[13] Danny D'Cruze, *data breach of 81.5 crore Indians: hacker allegedly leaks Aadhar, Passport, personal details on dark web,* business today, October. 31, 2023

[14] John Xavier, *explained / what does the alleged cowin data leak reveal? The Hindu, June 18. 2023*

[15] Cyber management alliance, https://www.cm-alliance.com/cybersecurity-blog/aiims-ransomware-attack, (last visited dec 26,2024)

Cyberwarfare used for state propaganda

Russian state-sponsored cyber actors have launched influence operations to support their war aims. In April 2022, the Canadian Security Establishment (CSE) exposed several disinformation campaigns:

- **April 6:** Russia falsely claimed the US was setting up biological labs in former Soviet countries and using Ukraine for testing.
- **April 13:** Russia spread disinformation about Canadian Forces committing war crimes in Ukraine, using doctored images.
- **April 25:** Russia deflected blame for atrocities by falsely accusing Ukraine of breaching Geneva conventions, causing dissent within its army[16].

WHETHER CYBERATTACKS CAN BE CLASSIFIED AS "USE OF FORCE" UNDER ARTICLE 2(4) OF THE UN CHARTER AND WHETHER STATES HAVE A RIGHT TO INVOKE SELF-DEFENSE TO SUCH ATTACKS?

Article 51 of the UN Charter establishes a State's right to self-defence in response to an "armed attack," but the definition of such an attack remains open to interpretation. To clarify the rule on self-defence and enhance **jus ad bellum**, more clarity is needed on what constitutes an armed attack in cyberspace. Policy norms could help define when cyber-attacks cross the threshold of an armed attack, guiding both States considering cyber-attacks and victim States responding to them[17].

Self-defense, as outlined in Article 51 of the UN Charter, is a legal exception to the prohibition of transboundary use of force under Article 2(4) of the UN Charter. It allows a State to use force in response to an armed attack. While international law lacks clear criteria for determining what constitutes an armed attack, other sources can offer additional guidance when analyzing whether cyber-attacks qualify as such.

The ICJ confirmed that Article 2(4) of the UN Charter applies to any use of force, regardless of the means. A cyber activity is considered a threat or use of force if its scale and effects are comparable to those of kinetic force. For example, cyber actions causing injury, death, or significant damage are unlawful uses of force. Even cyber activities causing non-physical damage can qualify as unlawful force. A cyber activity may be part of a broader kinetic operation, an independent act with physical effects, or one without physical effects.

---

[16] Canadian centre for cyber security, *cyber threat bulletin: cyber threat activity related to the Russian invasion of Ukraine,* https://www.cyber.gc.ca/sites/default/files/cyber-threat-activity-associated-russian-invasion-ukraine-e.pdf, (last visited dec 26,2024)

[17] Oorsprong, F., Ducheine, P. and Pijpers, P. (2023) 'Cyber-attacks and the right of self-defense: a case study of the Netherlands', *Policy Design and Practice*, 6(2), pp. 217–239. doi: 10.1080/25741292.2023.2179955.

The International Group of Experts unanimously agree that certain cyber operations can be "sufficiently grave" to qualify as an armed attack. This aligns with the ICJ's nuclear weapon's advisory opinion, which stated that "the choice of means of attack is immaterial to the issue of whether an operation qualifies as an armed attack."

Existing international law provides limited criteria to assess scale and effect. However, the IGE agreed that a cyber operation causing significant harm—such as serious injury or death to individuals, or substantial damage or destruction of property—meets the threshold of an armed attack.

POSITION OF STATES –

EUROPEAN UNION –

A State facing a cyber operation that amounts to an armed attack can invoke its self-defense rights under Article 51 of the UN Charter. To qualify as an armed attack, the cyber operation must have a scale and impact similar to a physical military attack, such as causing significant damage to property (including ICT systems) or harm to individuals. Any defensive response must adhere to the principles of necessity and proportionality.

When a State exercises self-defense, it can request support from other States. Collective self-defense can only occur at the victim State's request and must adhere to the same rules. Within the EU, Article 42(7) of the Treaty on European Union obligates Member States to assist a victim of armed aggression, in line with Article 51 of the UN Charter, while respecting each Member State's security policies and NATO commitments[18].

UNITED STATES OF AMERICA –

Under Article 51 of the UN Charter, a State has the right to self-defense if it faces a cyber activity that amounts to an actual or imminent armed attack. This applies whether the attacker is another State or a non-State actor. In response, the State does not need to use the same methods as the attacker. It can defend itself using cyber tools, traditional military force, or a combination of both, depending on the situation.

In exercising its inherent right of self-defense, a State may use force that is necessary and proportionate to respond to an actual or imminent armed attack, whether in the cyber context or any other. The use of force in self-defense must be necessary and proportionate to the threat. Before resorting to force, States should consider if passive or active cyber defenses below the threshold of force could neutralize the threat[19]

ISRAEL –

[18] Council of the European Union, Declaration on a common understanding of International Law In cyberspace, https://data.consilium.europa.eu/doc/document/ST-15833-2024-INIT/en/pdf, 18 nov,24.

[19] NATO Cooperative Cyber Defence Centre of excellence, United Nations General Assembly, 13 July,2021.

The prohibition on the "threat or use of force" in Article 2(4) of the UN Charter applies to cyberspace. A cyber operation causing physical damage, injury, or death can be considered a use of force, similar to kinetic attacks. Non-physical damage may also be considered, depending on future legal developments.

If a cyber operation constitutes an armed attack, the targeted State may exercise self-defense under Article 51 of the UN Charter, following the principles of necessity and proportionality. Self-defense against a cyber attack can involve either cyber or kinetic means[20].

SINGAPORE –

States must avoid using force against others' territorial integrity or political independence. Cyber operations can qualify as a use of force based on factors like origin, effects, and nature. Singapore asserts that a State's right to self-defense under the UN Charter applies to cyberspace. Malicious cyber activity causing significant harm can trigger self-defense, even without physical damage, if the disruption is severe[21].

CONCLUSION –

In conclusion, cyberwarfare is a growing threat to national security and global stability. As technology advances, strong cybersecurity and international cooperation are essential to tackle new risks. It is important to consider the ethical, legal, and political impacts when dealing with these challenges.

We have seen in the examples and case studies above how state and non-state actors have used cyberattacks to orchestrate attacks on other countries for various purposes, such as data breaches, espionage, propaganda, and computer network attacks (CNA) on military targets and equipment. States like Iran, Russia, the US, and Israel have used such tools against each other or in support of their allies. In contrast, while these states have advocated against the use of such tools, they have also repeatedly violated international law or the UN Charter.

To prevent cyberattacks, a state should strengthen its cybersecurity systems, create clear laws and regulations, and promote awareness. Investing in technologies like firewalls and encryption helps protect important sectors. Regular training for employees can reduce human errors, which are often exploited by attackers. States should also cooperate internationally, sharing threat information, and have a response plan in place to quickly handle any attacks. India has taken a positive step in addressing this concern, The Indian Government has taken significant steps to combat cybercrimes, including the establishment of the Indian Cyber Crime

---

[20] Roy Schondorf, *Israel's perspective on Key Legal and practical issues concerning the application of international law to cyber operations*, International law studies, https://digital-commons.usnwc.edu/ils/vol97/iss1/21/ .

[21] NATO Cooperative Cyber Defence Centre of excellence, United Nations General Assembly, 13 July,2021

Coordination Centre (14C) and the National Cyber Crime Reporting Portal (https://cybercrime.gov.in), which allows citizens to report cybercrimes directly. Additionally, the 'Citizen Financial Cyber Fraud Reporting and Management System' and a toll-free helpline (1930) have been launched to address financial frauds. The government has also implemented awareness campaigns, issued alerts, and provided training for law enforcement and judicial personnel to strengthen the overall response to cybercrimes[22].

Further the government has enacted the Digital Personal Data Protection Act,2023. The Digital Personal Data Protection Act, 2023 ensures individuals' rights to protect their personal data through principles like consent, data minimization, and security. It mandates strict controls on data transfers, including requirements for storing payment system data within India. The Act enforces accountability with penalties for breaches and non-compliance[23].

[22] Ministry of Electronics & IT, Safeguarding India's Digital Landscape – Key governments's Intiative to enhance cybersecurity awaraness, (https://pib.gov.in/PressReleasePage.aspx?PRID=2037115#:~:text=The%20Indian%20Government%20has%20established,for%20addressing%20digital%20threats%20comprehensively) 25 july,2024,

[23] Digital Personal Data Protection Act 2023.