POLICY BRIEF, MAY 2024

Lawfare in Cyberspace and International Law

Dr Faiza Ismail

IPRI Islamabad Policy Research Institute
Research | Innovation | Dialogue | Policy

NETT National Economic Think Tank

Chair, International Law

Executive Summary

Issue

Warfare is arguably somehow managed by International law. In Cyberspace, warfare exists without any recourse to law. Can international law afford tools for the global village to regulate warfare in the Cyberspaces of this world?

Recommendations

1- The warfare in cyberspaces of India and Pakistan should be regulated ideally by mutual negotiations between the two countries.
2- If this is not possible, International Law should be reformed to cover the warfare in cyberspaces of the two countries.
3- Broadly speaking, it is not just a matter of concern for India and Pakistan but powerful nations like the United States, China and Russia also need to regulate their hostilities in cyberspace.

Overview

War has always existed in the world. Generally speaking conflicts among nations which result in use of arms and hostilities are called armed conflicts. International armed conflict and its defence have been defined in the Geneva Conventions as well as the UN Charter. With the emergence of Cyberspace, warfare has entered into the digital world too. Over time, lawfare has also developed which refers to justification of war based on law. This policy brief is an examination of legal regimes that exist to justify warfare in Cyberspace. In this regard, author has conducted an analysis of lawfare in Cyberspaces of the US and Russia as well as India and Pakistan.

Analysis

I) Warfare

Lassa Francis Lawrence Oppenheim has defined war as a contention between two or more states to overpower each other and impose such rules on the defeated state(s) as the victor desires. There is no legal definition of war available in International Law. The Geneva Conventions of 1949 have defined the International Armed Conflict ('IAC'). Article 2 of the said Convention states IAC as, "all cases of declared war or of any other armed conflict which may arise between two or more of the High Contracting Parties, even if the state of war is not recognized by one of them." The said definition is there to determine whether a state has involved itself in the IAC on the pretext of self-defence or violated the sovereignty of another state.

Article 51 of the United Nations Charter of 1945 stipulates that nothing in the charter shall stop a state from using its right of self-defence provided that an armed attack has been launched against it. The United Nations Charter of 1945 does not provide any definition of war. However, Article 2 (4) of the United Nations Charter of 1945 requires that the states shall refrain from 'using threat or force against the territorial integrity or political independence of another state'. Thus, it is clear that the term encompasses the use of threat or force by one state against another state.

From the bare reading of the article, it is quite clear that the use of threat or force against the integrity and sovereignty of another state does not necessarily include the use of weapons of war or sending army personnel and mercenaries. The definition is broad enough to encompass the breach of sovereignty of another state using different

technical means including attacks on the cyberspace of another country. For instance, the hacking of websites of another state that contain sensitive data relating to the national security of that state. Therefore, such attacks or intrusions of the cyberspace of a country violate the sovereignty of another state. Attacks in cyberspace of a state can therefore be referred to as the use of force or warfare in cyberspace.

II Warfare in Cyberspace

Given the digital sphere of the 21st century, the states have continuously been engaging in warfare in cyberspace. Information warfare is the use of different technical instruments by a country or a group to get ahead of its adversaries. They make propaganda, spread misinformation, and fake news to cause intangible damage and harm the adversary's reputation. Sometimes, they use information warfare to intrude on the adversary's important computer data system, like military controls, causing real damage. This kind of warfare relies on fancy tech, like hacking tools, to mess things up for their rivals and gain an edge.

There are two types of warfare in cyberspace i.e. information warfare and digital warfare. Information warfare is defined as the use of electronic devices to influence and disrupt the enemy's decisions to get a competitive advantage while defending your information to stay ahead. Information warfare and digital warfare might appear similar, but they are quite different. Information warfare has been around for ages using information itself as a weapon. It includes things like spreading lies through media and social networks or disrupting important computer systems. Digital warfare, on the other hand, is newer and focuses specifically on using the internet and computers to gain an advantage. It involves attacks like hacking or using viruses on important computer systems. While information warfare is broader, including lots of tactics and tools, digital warfare is a smaller part of it, but it is become really important in today's world because of our reliance on technology.

In information warfare, various tactics are used to influence how people think about a rival country or group. Here's a simplified breakdown of the tactics used in information warfare:

1. Use of Media: Using news and social media to spread false or manipulated information about a rival country or group. This can shape how people feel and think about them.

2. Social Media: Platforms like Facebook and YouTube are used to spread information to a huge number of people quickly. Paid campaigns make information reach even more users. False information on social media can rile up emotions and cause chaos.

3. Cyberspace Intrusion: Hacking into important computer systems of a rival country to disrupt or steal information. Governments work hard to protect their systems from these attacks.

4. Data Theft: Stealing important information or funds from a rival. Sometimes, this is politically motivated, like the Cambridge Analytica scandal, where data from Facebook was used for political purposes.

5. Shaping Public Opinion: Spreading manipulated information among the masses to influence their thoughts and actions. This can happen through the media or by sending agents to a rival country. Like, before invading Iraq, the U.S. spread false information to make it seem like they were protecting Iraqi citizens, not just acting in their interest. This helped the U.S. invade Iraq without much resistance.

7. Terrorist Information Warfare: Terrorist groups, like the Taliban, use information warfare to shape narratives. For instance, they used civilian casualties from NATO air strikes to create a negative image of NATO forces, affecting their operations in Afghanistan.

These tactics show how information can be used as a powerful tool in conflicts between nations or groups, affecting public opinion, military actions, and political decisions. Moreover, information warfare has changed the conventional way of conflicts, moving battles to the internet and making wars more about manipulating information than direct physical force. The mechanism of information warfare is described below:

1. War without Physical Force: Information warfare has changed how wars are fought. It doesn't need traditional military force but still causes significant damage. For example, attacks on a country's computer systems can weaken its defence, making it hesitant to engage in war.

2. The Internet as the Battlefield: Instead of traditional battlegrounds, the internet is now where the fight happens. Attacks through social media damage reputations, steal data, and weaken security systems without direct physical confrontation.

3. Enhancing Military Actions: When used with conventional military force, information warfare makes military actions more effective. For instance, spreading false information before the Iraq invasion helped the U.S. take over without much trouble.

4. Part of Hybrid Warfare: Hybrid warfare combines different tactics including information warfare. Propaganda, fake news, and hacking are used to tarnish the reputation of adversaries and weaken their defences without solely relying on traditional military force.

III Lawfare

Lawfare is defined as using the law as a weapon in conflicts between countries or groups. It mentions how international laws and institutions like the UN and the International Court of Justice have become important in today's world. There are two sides to lawfare: defensive and offensive. Defensive lawfare is when a country or an entity takes advantage of laws to defend itself or gain an edge. For example, ISIS used civilians as human shields and exploited international laws that protect civilians during conflicts. Offensive lawfare, on the other hand, is using legal strategies to gain an advantage against an opponent. For instance, the denial of legal protection to terrorists in the sanctuaries. Some countries have also made laws that hold individuals or groups supporting terrorism accountable. For instance, Israel’s actions in Gaza can be defined as an offensive lawfare.

IV Lawfare in Cyberspace of the US and China and Russia

Some countries have started using lawfare to justify their actions of intruding into another state’s cyberspace. For instance, the US has changed its cybersecurity policy from defensive to offensive in order to deter adversaries, i.e., China and Russia. There have been constant attacks on US cyberspace, therefore, they have expounded upon a preemptive defence strategy. The Trump administration lowered the threshold necessary for a response to defend the critical infrastructure from a significant cyber incident (any attack that puts US national security at risk).[1]

In 2018, the Trump Administration passed the Countering America’s Adversaries Through Sanctions Act (CAATSA) 2018. The primary purpose of the Act was to put

[1] Geoffrey M. Goodale and others, ‘National Security Law’ 53 ABA/SIL YIR 439.

sanctions on Russian politicians and oligarchs. The Act also placed sanctions on Russian persons identified in the indictments, especially those who were involved in the interference of 2016 presidential elections. The US Government also took action against Russia for its alleged involvement in the nerve-agent attack on Sergei and Yulia Skripal in the United Kingdom in 2018.[2]

Moreover, the US has passed certain Acts that have authorized the administration to surveil individuals and control the investments of non-US nationals in the country. Section 702 of the Foreign Intelligence Surveillance Act of 2017 permitted the FBI to collect emails, text messages, and phone calls of individuals not in the US who have been targeted for intelligence surveillance.[3] The said section of the Act was challenged in the case of *United States v Hasbajrami.* In the said case, the district court weighed in favour of surveillance. The court opined section 702 does not violate the Fourth Amendment of the US Constitution primarily because the said amendment does not apply to non-US persons. Additionally, the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA) controls the investments of non-US nationals in the country. It requires the Committee on Foreign Investment in the United States to be notified of any potential investments in US critical technology companies. FIRRMA applies to all foreign investors irrespective of their countries. Previously, it monitored the investments of the nationals from Russia, China and Venezuela only but now its scope has been broadened to include nationals of all countries.[4]

From the foregoing, it is clear that the US Government has adopted an offensive policy to deter cyber-attacks and also relies on diplomatic, legal and economic tools to achieve the aforesaid purpose. An example of the US's diplomatic effort to deter cyberattacks is the 2015 bilateral agreement to end China's cyber economic espionage; however, China continues to steal trade secrets. In the legal sphere, the Foreign Sovereign Immunities Act of 1976 confers some sort of protection in this

[2] Geoffrey M. Goodale and others, 'National Security Law' 53 ABA/SIL YIR 439.
[3] The Foreign Intelligence Surveillance Act 2017, s 702
''(a) AUTHORIZATION.—Notwithstanding any other provision of law, upon the issuance of an order by subsection (i)(3) or a determination under subsection (c)(2), the Attorney General and the Director of National Intelligence may authorize jointly, for a period of up to 1 year from the effective date of the authorization, the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information.
[4] Geoffrey M. Goodale and others, 'National Security Law' 53 ABA/SIL YIR 439

regard. The said Act was passed by Congress to obtain jurisdiction over a foreign state in the US courts. A US court could obtain jurisdiction only in case of three exceptions enumerated in the Act - commercial activity, torts or terrorism. On the pretext, the statute provides broad immunity to the foreign states and a US court is conferred jurisdiction only if the foreign states' conduct falls within the aforementioned three exceptions.[5]

However, the ambit of taking action against foreign states involved in cyber-attacks on individuals and companies in the US is narrow and there is a lack of clarity and consistency in its application.[6] An example of this unclarity and inconsistency is the reasoning of the Ninth Circuit in *WhatsApp v NSO Case*.[7] In this case, an Israeli security company developed a spyware named 'Pegasus' and sold it to foreign governments, which was later used to target and surveil WhatsApp accounts of human rights activists and journalists. NSO argued that it was entitled to derivative foreign sovereign immunity conferred by the 1976 Act. The Ninth Circuit dismissed the motion of NSO stating that it does not enjoy the foreign sovereign immunity deviating from the opinion of the Fourth Circuit in *Butters v Vance Int'l Inc.*[8] In the said case, the court granted immunity to a US firm hired by Saudi Arabia.

V Lawfare in Cyberspace of Pakistan and India

Cyberwarfare is prevalent in third-world countries as well and the 21st century has revolutionized conventional warfare by providing a new domain, i.e., digital space. Pakistan and India are prime examples of cyber warfare, i.e., disrupting the cyberspaces of each other for political, strategic, and military objectives. Both countries view invading each other's cyberspace as an essential defense and security strategy.[9]

[5] Adam L. Silow, 'Bubbles over Barriers: Amending the Foreign Sovereign Immunities Act for Cyber Accountability' (2022) 12 J Nat'l Sec L & Policy 659.
[6] Adam L. Silow, 'Bubbles over Barriers: Amending the Foreign Sovereign Immunities Act for Cyber Accountability' (2022) 12 J Nat'l Sec L & Policy 659.
[7] WhatsApp Inc. v. NSO Grp. Techs. Ltd., 17 F.4th 930, 933 (9th Cir. 2021).
[8] 225 F.3d 462,466 (4th Cir. 2000).
[9] Abu Hurrairah Abbasi and Saher Liaqat, 'Cyberwarfare is Shifting the Nature of Indo-Pak Conflict in South Asia' (2023) Islamabad Policy and Research Institute

In recent years, India has gained a competitive advantage over Pakistan by augmenting its defensive and offensive cyberwarfare capabilities. It has been working with Israel and the US and inculcating cutting-edge technologies to gain a competitive advantage in the region. There have been reports of India using the NSO's spyware named *'Pegasus'* to get access to the chats of important Pakistani officials. Notably, the surge in cyberattacks is always followed by various events such as terrorist attacks or instability at the Line of Control (LoC) thereby disrupting the peace in the region.[10]

Pakistan and India both need to work together and expound upon a framework for responsible behaviour in cyberspace to prevent the escalation of conflict in the region. Lastly, Pakistan needs to establish a robust cybersecurity culture to ensure data and privacy security by investing in cybersecurity infrastructure and enhancing cooperation with international partners, akin to what India is doing, to address threats to its cyberspace.[11]

VII Recommendations

This policy brief has identified the use of law to justify individuals' as well as countries' surveillance by the US. Often the lawfare in Cyberspace by the US against Russia and China particularly and the world generally has taken an offensive approach. Preemption has shaped lawfare in Cyberspace at a different level that has to be addressed. Warfare which exists in the Cyberspaces of India and Pakistan is not justified based on law. Warfare in the Cyberspace of India and Pakistan has to be regulated under International Law. Although International Law has not managed to regulate it between the US and Russia and China, experts in International Law need to work out a mechanism to regulate cruel war in the Cyberspace of the globe.

[10] Abu Hurrairah Abbasi and Saher Liaqat, 'Cyberwarfare is Shifting the Nature of Indo-Pak Conflict in South Asia' (2023) Islamabad Policy and Research Institute

[11] Abu Hurrairah Abbasi and Saher Liaqat, 'Cyberwarfare is Shifting the Nature of Indo-Pak Conflict in South Asia' (2023) Islamabad Policy and Research Institute

Recommendations and Action Matrix				
Legal Options for Government				
Recommendations	**Pathways to Solution**	**Implementation of Solution**	**Actors Responsible**	**Implementation Timelines**
There is a need for dialogue between India and Pakistan regarding mutual regulation of Cyberspace for warfare.	The foreign office needs to work with its Indian counterpart to begin a dialogue on this sensitive matter.	Bilateral treaty between India and Pakistan to ensure mutual cooperation in designing a mutual cyber security policy.	Ministry of Information Technology and Telecommunication, Ministry of Foreign Affairs (MoFA) and Ministry of Defence.	6 months to 1 year.
In Pakistan, we have National Cyber Security Policy 2021 which does not cover international cyber security issues. We need to integrate our Cyber Security laws with international Cyber laws.	Think Tanks can set up a team to study Cyber warfare threats which exist between India and Pakistan to identify crucial matters to address at the earliest.	Memorandum of Understanding among regulating authorities within Pakistan.	Security-related think tanks and authorities	3-6 months
The government of Pakistan needs to approach UNIDR to begin working on this project**.**	International law is in dire need of reform to address international cyber warfare. This has been particularly identified by the United Nations Institute for Disarmament Research (UNIDR). Pakistan needs to work with the UNIDR to specifically examine issues existing between the	Recommendations in collaboration with international entities interested in the regulation of cyber security matters.	Ministry of Foreign Affairs and Ministry of Defence.	1-3 years

	US, Russia, China and EU and draw comparisons between Pakistan and India. This should help us learn lessons and design more appropriate and international Cyber security policy.			