Solid State Technology
Volume: 63 Issue: 6
Publication Year: 2020

Cyber War: A New Paradigm Of War

Dr. Shikha Dimri[1] , Akanksha Singh[2]

"The supreme art of war is to subdue the enemy without fighting."[3]

The world is speaking of cyber warfare today with enhanced capabilities of computer systems and networks. The annual Worldwide Cyber Threats report by the Director of National Intelligence identifies politically motivated actors as a growing reason for cyber attacks [4]. It goes on to identify not just political but some threat vectors from smaller non-state bodies as well. Amassed both by state and non-state actors, cyber weapons have known to be used at multiple instances across the globe [5]. Cyber warfare remains a popular phenomenon that still needs robust conceptualization efforts to be better explained in context. While there is a common understanding about traditional segments of war among scholars, say, submarine warfare or chemical warfare, developing such a consensus on cyber warfare does not seem plausible, at least in short term.[6]

Due to technology capacitation over the last few decades, every country processes and stores information digitally, be it government secrets, military strategies or citizens' data. This has given birth to a long felt need for cyber-intelligent defences and the protection of high assurance computer systems. In pursuance of this goal, countries like USA and China have begun to tap on their

[1] Associate Professor, University of Petroleum & Energy Studies (UPES) Dept. of Law, Science and Technology, School of Law. Knowledge Acres, Kandoli Dehradun, Uttarakhand, India Email : shikha@ddn.upes.ac.in

[2] Assistant Professor, Senior Scale, University of Petroleum & Energy Studies (UPES)Dept. of Law, Science and Technology, School of Law. Knowledge Acres, Kandoli Dehradun, Uttarakhand, India. Email: akanksha.singh@ddn.upes.ac.in

[3] Sun Tsu from "The Art of War" Believed to have lived between 770 and 476 B.C

[4] International Committee of the Red Cross, JUS IN BELLO - JUS AD BELLUM | INTERNATIONAL COMMITTEE OF THE RED CROSS, https://www.icrc.org/en/war-and-law/ihl-other-legal-regmies/jus-in-bello-jus-ad-bellum (last visited Nov 12, 2020).

[5] Dimitar Kostadinov, *Jus in Cyber Bello: How the Law of Armed Conflict Regulates Cyber Attacks*, INFO SEC INSTITUTE, 2014, http://resources.infosecinstitute.com/jus-cyber-bello-law-armed-conflict-regulates-cyber-attacks-part/#gref (last visited Jul 22, 2020).

[6] Syed, Rubab, et al. CYBER WARFARE. Sustainable Development Policy Institute, 2019, pp. 4–5, Cyber Security: Where Does Pakistan Stand?, www.jstor.org/stable/resrep24376.7. (last visited 12 Nov. 2020.

countries' digital capabilities to ensure readiness. Some even envisage a state-sponsored cyber war in the coming times. Computer technologies have undoubtedly reached a point where a nation state's military resources have the capability to cause injury and fight a war through the cyberspace. The adaptation of technology has become so pervasive and integrated with traditional technology that we are now in the era when weapons are not just guided, tracked and targeted by computers but computers have become weapons themselves. [7]

The threat landscape has only widened with technology taking the center stage of all critical services being provided to citizens. As dependence on computer systems is increasing, a huge portion of the cyber-attacks are being targeted at networks like military and strategy resources. Not just that, even with the participation of both the public and private sector parties in essential services such as distribution and generation of power, healthcare and transport etc., the lines between government, civil, and industrial systems are becoming increasingly blurred which is expanding the bounds of vulnerabilities. Undoubtedly, when one infrastructure element is attacked, it is capable of bringing down an entire country within a little fraction of time. Due to this, there has been exponential increase in cyber-attacks both state sponsored and non-state. Some might comprehend temporary shutdown of government websites and services as modes of cyber warfare but to the affected nation, it is sometimes even short of nuisance. The real threats: what started with Stuxnet back in 2009 as an attack against one nuclear facility has reached the shape of WannaCry in 2017 which infects millions of systems in a few seconds.[8] Needless to say,cyber technologies have evolved much faster than the legal frameworks that govern them. The highly destructive scenarios and potential use of cyberwarfare techniques underscore the need for an unambiguous classification of possibilities and a standard of conduct for cyberwarfare which may be universally accepted.

The Internet has infused all indispensable layers of our lives; the way we watch, the way we talk and entertain ourselves is all governed by the Internet[9]. This has opened gates for Ransomware type of Cyber Weapons like WannaCry and Petya globally because everyone ranging from deep pocketed firms to a broke restaurant server were victims. This is not just with the target victims but also with the target devices of Cyber Attacks: they range from smart power and gas utilities of the state to the IOT devices that citizens use, meaning that orchestrating a nationwide shutdown via cyber weapons is seemingly possible. Recent reports and claims suggest involvement of a nation-state in orchestrating such an attack.[10]

---

[7] Smith, Troy E. "Cyber Warfare: A Misrepresentation of the True Cyber Threat." American Intelligence Journal, vol. 31, no. 1, 2013, pp. 82–85. JSTOR, www.jstor.org/stable/26202046. (last visited 2 Nov. 2020.)

[8] https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet(last visited 5 Nov 2020)

[9] *Id.*

[10] DAVID P. FIDLER, WEAPONS UNDER INTERNATIONAL HUMAN RIGHTS LAW (Stuart Casey Maslen ed., 2014).

One of the challenge that the law has faced since the beginning of the 20th century has been to adapt with the changes in technology. The cyberspace has been more challenging. There have been attempts at reaching a convention about using Information Systems in Armed Conflicts [11] and a treaty for the Cyber Space [12].

Cyber Weapon: Definition, Description and Analysis

The leading reference to Cyber Weapons is always indexed in the infamous Tallinn Manual which addresses the question of what constitutes a cyber weapon [13]. It indicates that cyber weapons are tools of cyber warfare which are by design or use capable of causing either injury, damage, death or destruction, thereby matching the criterion of a cyber operation to be an attack [14]. It has also been said to be a malware that irreversibly neutralizes centres of gravity in cyber-dependent economic, military, and political systems and infrastructure [15] hitch is not on point technically because then one could be looking at anything that can cause disruption per se. A layman definition of the word however, would be a weapon used to execute or launch a cyber attack. The usage of Cyber weapons may be classified into three broad categories:

1. Civil usage of a Cyber Weapon

a) Offensive: targeted defamation or trolling leading to any civil contravention or an action in tort, use of cyber weapons for information warfare domestically and exploiting any known/new capability to effect digital trespass and cause damage.

b) Defensive: Removing strains of cyber weapons causing Information Warfare. Remotely activated jammers, DDOS tools activated by government agencies to ban or restrict the websites during law & order situations

---

[11] Karine Bannelier-Christakis, *Marco Roscini, Cyber Operations and the Use of Force in International Law*, 21 J. CONFL. SECUR. LAW 367–368 (2016), https://academic.oup.com/jcsl/article-lookup/doi/10.1093/jcsl/krw003.(last visited on 10 Nov 2020)

[12] MICHAEL N. SCHMITT, TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (Michael N. Schmitt ed., First ed. 2013).

[13] David E. Hoffman, *The New Virology*, 185 WASHINGTONPOST.NEWSWEEK INTERACTIVE, LLC, 2017, at 77–80, http://www.jstor.org/stable/41231621.(last visited on 1 Nov 2020)

[14] Stefano Mele, *Cyber-weapons: legal and strategic aspects*, 2 IST. ITAL. DI STUD. STRATEG. 8 (2013).

[15] Louise Arimatsu, *A treaty for governing cyber-weapons: Potential benefits and practical limitations*, (2012).

c) Dual: Software's used for network administration and monitoring tools or DDOS tools, snooping tools, Botnet

2. Criminal usage of a Cyber Weapon

a) Offensive: Trojan horses; e-mail bombs; denial-of-service tools; exploit scripts and programs that take advantage of vulnerabilities such as buffer overflows to gain access; root kits with Trojan system utilities, backdoors, and system log cleaners to cover tracks; and copyright crackers. Using known/unknown tools/capabilities for corporate espionage, data theft, phishing or defamation of any person in government or state controlled organization. Compromising UAVs, Auto Drive Vehicles, Medical Devices etc. to effect attacks like ransomware.

b) Defensive: software tools used for tracing of origin of any particular cyber attack incidence. Anti-piracy software or tools used to prevent data theft.

c) Dual: Botnet, Firewalls developed by various corporate and states for a restrictive usage. Every device attached to Internet.

3. Military usage of a Cyber Weapon

a) Offensive: targeted cyber weapons or tools like worm, Electro Magnetic Pulse missile (CHAMP) etc, Drones, DDoS Attacks, Zero Day vulnerability Exploits.

b) Defensive: Activating Anti DDOS attack tools, remotely activated jammers, DDOS tools activated by government agencies to ban or restrict the websites during war times.

c) Dual: Botnet, Vulnerability tools detectors, password crackers, etc.

International Warfare and Law Principles

One might feel that there must be many laws governing this unconventional dimension of warfare but truth be told, there are not many. When one refers to international warfare peace and resilience, they are essentially referring to the UN Charter of 1945[16] which lays down the resolution of withholding from use of force and limits the use only in cases of self defense. Since the World War II, it has been clear that the entire world stands in unison against any future war of the nature that happened back then. One of the products of this thought is the UN Charter of 1945 and particularly Articles 51 and 2(4). Although the provisions in question are in force and widely in use, it has not

[16] UNITED NATIONS, CHARTER OF THE UNITED NATIONS (1945).

prevented nations from practically developing and using nuclear, biological or cyber weapons. Article 2(4) of the UN Charter of 1945 states as under[17]:

"All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."

When one refers to the provisions of Article 2(4) of the Charter[18], Article 51 is naturally read in harmony. It states as under:

"Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security."

It is clear through this provision that the only single exception to the rule of Article 2(4) is Article 51 when a state is allowed the right of self-defense in case of an armed conflict. This reading does not clear the concept of "use of force", however, the author substantiates the initial research on cyber weapons to conclusively state that in order to qualify a conflict as "armed" usage of weaponry is paramount. As a researcher has put it,

"cyber attacks have the potential to reach out from cyberspace into the physical dimension, causing giant electrical generators to shred themselves, trains to derail, high-tension power-transmission lines to burn, gas pipelines to explode, aircraft to crash, weapons to malfunction, funds to disappear and enemy units to walk into ambushes."[19]

State Responsibility and Accreditation to an Attack

The next question that comes to mind naturally is that should a state be held responsible for activities of its actors, hackers? On the point of state agents, it is clear that an attack is attributable to the state..

[17] *Id.*

[18] UNITED NATIONS, CHARTER OF THE UNITED NATIONS (1945).

[19] Jason D Jolley, *Article 2 (4) and Cyber Warfare : How do Old Rules Control the Brave New World ?*, 2 INT. LAW RES. 1–16 (2013).

Article 4 [20] suggests that 'when state organ conducts an act, it is considered to be an act that state internationally. NSA is one example but many nations have started developing their own cyber cells, units, cyber military institutions etc. that perform activities ranging from defense to intelligence.' In some cases, these activities are outsourced to private entities which brings this question to the front. Although this tracing might seem like a bit of a challenge but in many cases, it has been found that in fact it is possible to trace states.

What happens when non-state actors are involved? On this point, Article 51 is firstly silent whether a state can actually use self defense against a non-state actor. Now, these non-state actors could be hacker groups, hacktivists or private citizens motivated by certain ideologies and in possession of sufficient skillset to develop/use cyber weapons to cause an attack.

Cyber Jus in Bello and Jus Ad Bellum

Two separate bodies of law can apply to such usage of cyber weapons: *jus ad bellum* and *jus in bello*. *Jus in Bello* is a Latin term that means "law in waging war." It is known also as international humanitarian law (IHL) [21] and the law of armed conflict (LOAC). IHL is aimed at minimizing unnecessary harm during a war using established rules to prevent certain type of use of weapons.

The qualifications however, require an armed conflict for *Jus in bello to apply*. This implies that *Jus in bello* will apply only after a war is entered into. The fact remains that the world has not seen a formal or cold cyber war where nation states have opted in, so there is no consensus. But the researcher foresees a strong possibility that it might be the case very soon that nation states use cyber weapons instead of kinetic weapons. At the global level, first the clarification needs to be on the point as to what constitutes a cyber war. Only then can one dwell into *Jus in bello.*

International Law stipulates that there are four basic considerations for *Jus in bello* to apply: Necessity, distinction, perfidy and neutrality. Article 52(2) of Addnl Protocol to Geneva Convention lays down that a military attack is lawful only "against those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction offers a definite military advantage." In order to use force on their own accord, it is hence, crucial for a state to keep a record of what the state knew of a computer network or resource to defend its actions once questioned globally. Though the last decade or so has seen increased number of attacks targeted at critical infrastructure yet there has been no use of the concept of *Jus ad bellum* because no cases have been taken to an International legal forum as such. Although the principle is about

[20] UNITED NATIONS, CHARTER OF THE UNITED NATIONS (1945).

[21] Rex Hughes, *A treaty for cyberspace*, 86 INT. AFF. 523–541 (2010).

deciding when responsive force is allowed in war, it gives little knowledge about legality of a cyber war and when an attack constitutes war enough to resort to responsive force [22].

Another reason for this is that treaties that govern this principle of law are age old legislations. Deducing and replicating them in the cyber space is rarely possible. *Jus in bellum* rules guide a nation's decision as to whether an incident justifies engaging in armed conflict or triggers the provisions of the United Nations Charter of 1945.

Questions, however arise about whether these principles of IHL would apply to the cyber space. Though there has been no formal recognition of the fact yet there is an implied usage by the ICJ of the Martens Clause in the Hague Convention IV of 1907 [23] as was seen in case of legality of threat of usage of Nuclear Weapons. This usage extends the scope of IHL to situations beyond the conventions as per the dictates of human conscience [24]. It is also to be noted that when a nation is to use force in self defense, it must essentially attribute the attack to another state. There has been some legal research on the point of application of traditional law to the cyber space. In the infamous International Court of Justice case titled *Nicaragua*[25], it was held that "the prohibition on use of force is part of the customary international law and also Article 2(4) of the UN Charter. It has been observed that humanitarian law would apply to cyber operations between states when there is either declaration of war or cyber operations in context of an already existing conflict with or without the concomitant occurrence of kinetic hostilities." [26]. The ICJ also said in this case that an armed attack would be judged by a scale and effects test which could mean that an armed attack even if done by irregular forces would be termed as armed attack if carried out by regular military personnel. International law in its essence provides for instances when a state is permitted to use force against another state. Foremost is self-defense in response to an armed attack. This is by the power of customary international law and Article 51 of the United Nation's Charter. To qualify a cyber attack as an armed attack, there have to be weapons and hence, recognition of cyber weapons is paramount.

---

[22] Stephen Moore, *Cyber Attacks and the Beginnings of an International Cyber Treaty*, 39 NORTH CAROLINA J. INT. LAW COMMER. REGUL. 223–257 (2013), https://extranet.cranfield.ac.uk/eds/detail/,DanaInfo=eds.b.ebscohost.com+detail?vid=1&sid=f2d5d5be-1348-4908-b651-e4d14a415678@sessionmgr111&hid=103&bdata=JnNpdGU9ZWRzLWxpdmU=#AN=92606783&db=bth.(last visited 8 Nov 2020)

[23]https://www.icrc.org/en/doc/resources/documents/article/other/57jnhy.htm(last visited 8 Nov 2020)

[24] *Id.*

[25] 1986 I.C.J. 14

[26] Kallberg, Jan. "Strategic Cyberwar Theory - A Foundation for Designing Decisive Strategic Cyber Operations." *The Cyber Defense Review*, vol. 1, no. 1, 2016, pp. 113–128. *JSTOR*, www.jstor.org/stable/26267302. (last visited on 1 Nov. 2020.

Role of Nation in case of attack

One of the countermeasure to an attributed cyber attack is retorsion. A simple example could be denying access to the host country's servers or digital resources.[27]These are unfriendly yet perfectly legal ways in which an attack can be tackled. According to the International Law Commission's Rules on Responsibility of States for Internationally Wrongful Acts, a victim state first must call upon the aggressor state to cease and desist a cyber attack before using force for self defense. [28]In case the aggressor denies or does not comply, then the victim state can use active defense which is to include blocking access, counter attacks etc. This warning requirement may however be overlooked through the language of Art. 52 of the rules which states that "a victim state can take urgent countermeasures as may be necessary to preserve its rights." It is pertinent to mention here that in cases of cyber attacks, time is of the essence. An aggressor state may build resilience and immunization against attacks by the time warning requirements are met. The ICJ also allows emergency countermeasures to be taken and the victim state is given discretion to determine the extent and levels of countermeasures.[29]

Internet regulation as a resolve to combatting Cyber Warfare

One of the strategies to combat this challenge is the current model/mode of operation where all nations conduct business as usual and traditional laws need to be interpreted to solve issues of conflict. That clearly is not the solution, because it leads to conflicts that render dissimilar results not just in situations but legal actions as well. There have been infamous international conflicts like the Yahoo! vs LICRA[30] case that led the world to think what internet jurisdiction and regulation principles are. Even since then, after 15 years of the judgment, there are no laws clearly marking jurisdiction on the internet. Another issue is that of criminality of acts. An unending extradition fight of Lauri Love [31] proved how criminal justice is a far-fetched dream in offences committed on the internet in multiple jurisdictions. The Internet is not owned by anyone, it is a decentralized network

[27] https://www.csoonline.com/article/3237324/what-is-a-cyber-attack-recent-examples-show-disturbing-trends.html(visited on 10 Nov 2020)

[28] Pool, Phillip. "War of the Cyber World: The Law of Cyber Warfare." The International Lawyer, vol. 47, no. 2, 2013, pp. 299–323. JSTOR, www.jstor.org/stable/43923953. (visited on13 Nov. 2020.

[29] OMER YOUSIF ELAGAB, THE LEGALITY OF NON-FORCIBLE COUNTER-MEASURES IN INTERNATIONAL LAW (1988).

[30] 433 F.3d 1199 (9th Cir. 2006)

[31] Simon Parkin, *The long read Keyboard warrior: the British hacker fighting for his life*, THE GUARDIAN, 2017, https://www.theguardian.com/news/2017/sep/08/lauri-love-british-hacker-anonymous-extradition-us.(Last visited 1 Nov 2020)

right now with centers of operation across the world [32]. To put it into perspective, one can view the internet to be operated by international organizations that run its different functions. Bodies like Internet Engineering Task Force (IETF) and Internet Corporation for Assigned Names and Numbers (ICANN) run its different functions which in a way vests them with the responsibility of governance. However, that does not give them the ownership of the Internet which is why nation states have over the years begun to regulate the Internet.

Cyber Warfare: the most potent International Threat

Needless to highlight, every dimension of a citizen's life is impacted by digital technologies in one way or the other. Historically, computer programs have been known to effect crimes otherwise considered impossible. In one such case of United States vs Morris[33], a computer program sent across to thousands of internet users caused their devices to automatically shut-down [34]. From then to now, it is only imaginable the kind of systems that are in operation today and the kind of functions that they perform. From citizen essential services to military and nuclear capabilities of a country, all of them are connected through computer systems capable of disruption at a national level.How the world sees regulation.

The Internet is perceived to everywhere but nowhere, still in fact, it is subject to geography after all in architecture, hence to law [35]. It may be a possibility in the distant future that the world actually does become a global village legally but the national and cultural values will always be different from place to place. From issues as small as communication and trade to as complex as capabilities of war are increasingly being governed by the mannerisms of the Internet. It is for that reason that Internet balkanization has become an urgent need. Another important facet is the realization of globalization. While actors on the internet feel that globalization is smoothing out the edges and ending conflicts leading to a government free and regulation-less internet, they fail to realize that the

[32] Jay Krasovec, *Cyberspace: The Final Frontier, for Regulation*, 31 AKRON LAW REV. 101 (1997), http://heinonline.org.ezproxy.library.wisc.edu/HOL/Page?handle=hein.journals/aklr31&id=109&div=&collection=journals%5Cnhttp://heinonline.org.ezproxy.library.wisc.edu/HOL/Page?handle=hein.journals/aklr31&div=9&collection=journals&set_as_cursor=8&men_tab=sr. (Last visited 5 Nov 2020)

[33] 928 F.2d 504 (2d Cir. 1991).

[34] https://opentextbc.ca/introductiontosociology2ndedition/chapter/chapter-8-media-and-technology/.(Last visited 1 Nov 2020)

[35] 2001, *The Internet's new borders*, THE ECONOMIST, .

power of nations protecting the way they are or the way they want to be is also dominant [36]. The internet/online/virtual border concept is not a new one.

The internet is in its native stages in terms of regulation [37] and possibly virtual borders would centralize it in a way so as to arguably remove its open access and democratic attributes. The challenge as has been identified by many researchers is identification of an environment that utilizes technological methods to respect rights of sovereign nations while upholding the unique nature of the Internet [38].

The nuances of a borderless empire not only pose a threat to the nation states but to the interested parties also. In a legal conflict, parties are clear, liabilities are clear too but discerning which nation has jurisdiction because of the communication poses another legal challenge [39] which a balkanized model can possibly solve. As the knot on data protection and again dissimilar laws tighten, corporates are becoming wary and confused by some law of some state that might strangle their operations [40].

A nation that limits/filters/blocks access to critical information and services offered by the state to only its individual citizens and not the internet is most certainly a safer one. Not just for protection of its own sovereignty but for the protection of users' privacy from foreign attacks. The next rationale to having a bordered/fenced cyber space is also rooted in the history of the world. When nations separated based on religion, belief systems, cultures etc. they essentially demarcated boundaries for themselves so that there could be peaceful lifestyles for all dismembered nations. The Internet's global dissemination happened without any international law, borders or processes [41] which means that there were no rules and still are none. In its initial years, everyone viewed internet as this global revolution to bring the world together until it was being slowly recognized and the researcher points again to the case of *Yahoo!* how cultural differences and belief systems do govern the internet.

---

[36] https://www.pewresearch.org/internet/2020/02/21/concerns-about-democracy-in-the-digital-age/(Last visited 2 Nov 2020

[37] *Id.*

[38] *Id.*

[39] Charles R Topping, *The Surf Is up , but Who Owns the Beach - Who Should Regulate Commerce on the Internet The Surf Is up , but Who Owns the Beach - Who Should Regulate*, 13 (2014).

[40] *Id.*

[41] *Id.*

Domestic Regulation

One might debate the remote application of domestic regulation against Cyber Warfare and regulation, that too, of the way the internet operates. To speak as a proponent of the above theory of balkanization as a resolve to cyber warfare, the author highlights the following points:

1. Regulation for protection against attacks
2. Regulation to respond to attacks
3. Regulation for protection against adverse law
4. Regulation for enforcement of domestic law

Regulation for protection against attacks

Making the same case for India as China, Russia and EU to some extent have made for themselves, when one operates as a domestic island of the internet with a one way communication channel to the rest of the world, it essentially shields itself from any neighboring attacks. Quintessentially, in the next decade, each digital economy will need to go back to the basics and start regulating the internet at its source of entry into geographical territories.

When some suggest that in fact the Internet is borderless, they are inherently forgetting that national sovereignty is underlined by the principle of territoriality which each nation wants to exercise today. When the subjects of Data Protection and Privacy are talked about on international forums today, one nation accepts privacy as fundamental, while the other doesn't. How does a country in such circumstances plan to execute national laws and principles and guarantee its citizens the basic fundamental rights, if any.

Then comes the million-dollar question of how regulation protects against attacks. For beginners, a balkanized and regulated internet space in a country will be able to filter and block all outside attacks at the very brink of their occurrence. Attacks will never manifest into big blunders. In sandboxed environments, researchers, security experts and governments will be able to decipher exploits and prevent them from entering the ecosystem of the intranet of a country in itself.

Assuming a Wannacry getting launched and the moment it enters the Indian Internet, it is detected to be a malware and then stopped. The nation knows exactly where the exploit has spread already and response mechanisms in furtherance to the same can be initiated accordingly. In addition, signatures may also be used to store and verify again on future occasions whether a new entrant in the local internet is a contaminant or not.

It is clear in the 21st century that the Internet is a combination of infrastructure and the ideologies associated with it.[42] It is therefore that this change has to perforate through national policy on the Internet along with change in the way architecture of the Internet is laid down. Russia for instance is termed as a master of using cyberspace to advance information agenda.[43] It is often accredited to the architecture and balkanized model of the internet that the country follows. As a matter of fact, Russia adopts a rather unconventional approach of encouraging private citizens to participate in cyber operations when in need of national interests, setting up a kind of cyber command.[44]

Regulation to respond to attacks

Regulation is also needed in order to respond to attacks. First, if there is no internet regulation, a country might not be able to even ward off or prevent imminent threats. An attack cripples an economy and most of the response strategy is rectifying what is lost. In order to be able to respond first, regulation to combat needs to be in place.

Then, to respond to cyber attacks, the balkanized model will act as the shield in warfare that will protect against counter attacks and crossfires. Policies need to be in place for justification as to attack methodologies and nature. Strategies of response need to be in place within any type of a regulation model. It is also necessary as has been seen through the research that there is mandatory disclosure or outreach to the U.N. in order to call for international peace. Countermeasures or self defense is not warranted primafacie[45], sufficient evidence needs to be in place before any action is taken. Regulation will also ensure that this evidence is gathered and present in prescribed or uniform formats if a sanction for waging war is needed.

Some suggestions might be at a tangent with the principle of international peace, however, experts continually suggest that the world is at a cyber war on the go, it is only that nobody is realizing it or talking about it because then they would have to stop. The objective of this dialogue is initiate a discussion about cyber weapons and state sponsored attacks against others.

Regulation for protection against adverse law

The case for protection against adverse law is rooted in the concept of international sanctions against a rogue state. While India will never grow out to be such a state but in order to assure protection,

[42] Gary D. Brown, *The Cyber Longbow & Other Information Strategies: U.S. National Security and Cyberspace*, 5 PENN STATE J. LAW INT. AFF. 1–28 (2017).

[43] *Id.*

[44] *Id.*

[45] https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf(last visited on 6 Nov 2020)

regulation is the answer. For starters, regulation will help prove through empirical evidence the throughput of attacks and their severity which is needed in law.

Government services and procurements for example in Germany are mandatorily to be stored in the German jurisdiction without fail. This will protect nations from litigation in matters that they get involved in as a result of a flaw in architectures of other states.[46]

Regulation for enforcement of domestic law

In cases of cyber attacks, cyber war or even otherwise, it is crucial for enforcement of domestic law that there is regulation to effect it. Today, one of the major problems that the country's law enforcement is facing is enforcement of domestic laws because regulation does not exist. Data is not localized, accessible or available to the law enforcement for investigation. Surveillance for national security on social media is almost not possible because the model of internet in India is such that data flowing in and out of the country is not regulated.

This leads to a situation of chaos and haywires wherein neither is proactive policing nor enforcement of the law possible. If regulation clubbed with a balkanized approach is applied, it will further the protection to domestic actors and also protect the interests of the domestic law enforcement agencies.

Conclusion- International Law and Cyber Peace

Sometimes, warfare has to be resorted to in order to promote cyber peace. In April 2016, U.S. Cyber Command was tasked with its first every warfare assignment against the ISIL to carry out combats to disrupt its line of control. Proponents of protection of law will at this point wish to intervene and say that International law has to essentially apply in this case of armed conflict also because the U.S. is definitely going to use capabilities. In order to protect civilian interests and other domestic infrastructure, some international law has to apply but the territory is unchartered. The legal principles on this point of analysis whether there is military necessity or when an attack becomes an act of war, have been previously discussed.

On the point of sovereignty of other states, remote operations through systems in other territory are not violative of any international law as long as there is sanction and no effect to that state's territory. This could be further debated that a counter attack against such an attack might be targeted at the intermediate state in such cases. Needless to say, the most challenging part in international law read with cyber peace is the problem of attribution. Technically, there has to be a lot of capacity building

[46] https://www.lexology.com/library/detail.aspx?g=ff94b8d9-e252-4c45-a432-b83789355c95(Last visited on 6 Nov 2020)

in the domain of cyber forensics, per se, in order to have the necessary skill set for attribution which is otherwise missing.

From a legal standpoint, customary international law is clear on the point of application of state responsibility in attributing acts. There are standards of analyzing whether state responsibility can be fixed based on the organs of a state test. The research has also established how even non-State actors can be considered to be acting under the state's supervision to call for self defense by the target state. It is also therefore suggested that committing acts through proxies will not protect states from liability or shield them from the law.

On the point of countermeasures against attacks, states may resort to retorsions as discussed earlier. An example could be diplomatic sanctions. These are essentially those actions that do not violate International law. A state may however take actions that are violative as well in response to malicious activity that poses exceptional circumstances but then the law, in order to validate the actions will require the state to establish the exceptionality.

In order to promote international cyber peace, it is necessary that there is a treaty and there are sanctions against military/armed usage of any cyber weapon. States will continue to feel that it is essential to have cyber capabilities because of law enforcement and other security reasons but the usage has to be controlled like that of biological or nuclear warfare. In conclusion, cyber space is a new territory but the law is in existence since decades. States are under the responsibility to identify existing legal frameworks or to develop their own if they want to survive attacks and live through this century. And the only way ahead is international cooperation and articulation of international standards and norms without which at one point of time, it would become highly difficult to control and monitor even citizen essential services in a State. The following suggestions are proposed: The state shall not engage in cyber-enabled theft of any other state's properties, confidential data or critical infrastructure data;
The state shall not use against another any cyber weapon that can cripple critical infrastructure or citizen essential services;
The state shall not undertake any countermeasures against cyber attacks unless attacks are attributed and must do so within the norms of international law without disrupting civilian networks; & the state shall cooperate in international investigations and other obligations from time to time.

REFERENCES

1. Choi, Seungho, et al. "Success Factors for Luxury e-commerce: Burberry's Digital Innovation Process." *International Journal of Information Systems Management Research and Development* (2014): 1-10.

2. Charles A. Ray, "Cyber war and Information Warfare: A Revolution in Military Affairs or Much Ado about Not Too Much?", National War College Report, 1997.

3. Carl von Clausewitz, *On War*, (edited and translated by Michael Howard and Peter Paret), Princeton University Press, 1989, p. 89.
4. Kumar, A. Senthil, and Easwaran Iyer. "An industrial IoT in engireering and manufacturing industries–benefits and challenges." *International Journal of Mechanical and Production Engineering Research and Dvelopment (IJMPERD)* 9.2 (2019): 151-160.

5. Rosenzweig, P. Cyber Warfare: How Conflicts in Cyberspace Are Challenging America and Changing the World; Praeger: Santa Barbara, CA, USA, 2013; pp. 15–73.

6. Roy, Bishnu Pada. "'Crossing Over'the (Blurred) Lines Among Reality, Virtuality, And Theatricality: A Cyberpsychoanalytical Study Of The Nether By Jennifer Haley." International Journal of English and Literature (IJEL) 7.5, Oct 2017, 47-56

7. Sun Tzu translated by Samuel B. Griffith, The Art of War. (Oxford University Press, 1963)