'CYBERWAR' – OBSCURE DOMAIN OF INTERNATIONAL LAW

by

Priyanka Vaidyanath

ABSTRACT

In the world of computers, security to individuals and to nation states seems dicey. The borderless transactions between people and the ease of sharing thoughts, emotions, goods and services has no doubt led to a world of comfort. It seems imperative to look into whether such ease of transactions and comfort at the feet of people is worthy enough to compromise data and security. When it comes to security of individuals, there are International and National treaties and legislations respectively. Budapest Convention, General Data Protection Regulation, The Clarifying Lawful Overseas Use of Data Act, etc. Though there are a few laws to deal with cyber crime and individuals no law can be seen with regard to 'cyberwar'.

Introduction

The advancement of technology has been both a boon and a bane. The use of 'cyber' domain by people has made security a volatile concept with increasing threat. Cyber-attack not only poses a threat to individuals, but to nation states as well. Cyber-attack has the ability to cause consequential risk to the nation states threatening the national security and critical infrastructure of a country. Experts are debating over the fact, whether to consider the application of International Humanitarian Law (IHL) to cyber-attacks in the context of 'conflict' situation[1]. IHL does not apply to any other cases of cyber-attack but only to those launched with the intention to spur an armed conflict or applies in cases of cyberwar during an armed conflict. Thereby the presence of a 'conflict' becomes a precursor for application of International Humanitarian Law. It is worthwhile to contemplate that mere inclusion of 'war' in the nomenclature does not entail the application of International Humanitarian Law at all times.

'Cyberwar' and International Humanitarian Law

The issue of cyber-attack to be treated as an armed attack[2] needs to comply with few factors such as: the cyber-attack is to be intended to cause an effect that is equivalent to death or injury, to incapacitate critical infrastructure, that is: transportation, e-commerce, water and electric supply so on. This interpretation of cyber-attack to be treated as armed attack is said to attract the application of international humanitarian law only if occurred during an armed conflict. Cyber-attacks which cause equal amount of destruction as in case of a conventional conflict shall be governed by the rules of IHL. The categorization of international armed conflict[3] and non-international armed conflict[4] is based on the factors as elucidated in the Geneva Convention 1949. Cyber conflict between two states would entail a conflict to be an international armed conflict and the conflict where just one party is a state, is considered as a non-international armed conflict. For a cyber-attack to qualify as non-international armed conflict[5] it needs to be repeated over certain period of time from a different territory. Similar to that of a conventional war, the principles of international humanitarian law applies to cyberwar as well. Principle of distinction[6] mandates that civilian objects and military objects shall be distinguished, but whether the civilian data (Password, Identity online) qualifies as a civilian object or whether the states infrastructure qualifies as a civilian object needs

[1] Icrc.org. 2012. [online] Available at: <https://www.icrc.org/en/doc/assets/files/2013/130621-cyberwarfare-q-and-a-eng.pdf> [Accessed 27 January 2022].
[2] Melzer, N., 2011. [online] Unidir.org. Available at: <https://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf> [Accessed 10 December 2021].
[3] Geneva Convention 1949 Common art 2
[4] Geneva Convention 1949 Common art 3
[5] *Supra*, note 2
[6] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, art 57

clarification. Likewise, the principle of proportionality mandates that the incidental damage on the civilian should not exceed the anticipated military advantage[7]. Anticipating the civilian damage online is tougher[8] since it can either disrupt a service like health services or may disrupt some social media interaction.

Defining and understanding 'Cyberwar'

Cyberwar is defined as use of computer technology to disrupt the activities of a state more specifically attacking the information system for strategic or military purpose[9]. Like many of the recent technological advances that lack a concrete *legal definition* from an authority (Eg Artificial intelligence), cyber war falls under such pretext of lacking a substantial definition. Scholars such as Eun, Abmann[10] believe that, interpreting cyberwar to the existing definition of war serves no good, but the definition of war should meet the changing situations. The advocates of humanitarian law are concerned with disruption of services such as health care system[11] which are all digitalized in todays' era which lack sufficient protection to guard from cyberattacks. What actions constitute 'cyberwar' is yet another point which needs clarity to attract the application of IHL. The DDoS attack in 1990's[12] were treated as a hostile act but which is common today in terms of cyberattack.

Cyberwar can be waged through different kinds of cyber weapons[13] as similar to that of a cyber-crime such as virus, malwares to attack a system directly, hacking, cyber espionage, ransomware etc. These weapons are used to attack the governmental or military system with a political vendetta either in the form of destabilization, sabotage or data theft[14]. Destabilization is where the attackers attack critical government functioning that impact civilians such as power and water supply, banking, transportation. Sabotage is where the governmental communications, military database are blocked which is supported by conventional conflict and data theft includes stealing of sensitive governmental information.

[7] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, art 51(b)

[8] Hathaway, Oona A., et al. 2012, "The Law of Cyber-Attack." California Law Review, vol. 100, no. 4, California Law Review, Inc., pp. 817–85, Available at:<http://www.jstor.org/stable/23249823>. [Accessed 18 December 2021]

[9] Lexico Dictionaries | English. 2022. *CYBERWAR | Meaning & Definition for UK English | Lexico.com*. [online] Available at: <https://www.lexico.com/definition/cyberwar> [Accessed 27 January 2022].

[10] Yong-Soo Eun, Judith Sita Aßmann, August 2016, *Cyberwar: Taking Stock of Security and Warfare in the Digital* Age, *International Studies Perspectives*, Volume 17, Issue 3, Pages 343–360, Available at<https://doi.org/10.1111/insp.12073> [Accessed 21 December 2021]

[11]International Committee of the Red Cross. 2022. *Cyber Warfare: does International Humanitarian Law apply?*. [online] Available at: <https://www.icrc.org/en/document/cyber-warfare-and-international-humanitarian-law#:~:text=No.,repeatedly%20raised%20in%20intergovernmental%20discussions.> [Accessed 24 November 2022]

[12] Cameran Ashraf (2021) *Defining cyberwar: towards a definitional framework*, Defense & Security Analysis, 37:3, 274-294, DOI: 10.1080/14751798.2021.1959141 [Accessed 29 November 2022]

[13] Terrell, K., Rosencrance, F. and Kevin, H., 2022. *What is cyberwarfare?*. [online] SearchSecurity. Available at: <https://www.techtarget.com/searchsecurity/definition/cyberwarfare> [Accessed 9 December 2021].

[14] *id*

Not many cyber-attacks that disrupt the governmental functioning is known to the masses. Stuxnet the highly famous cyber-attack is the first instance that is referred while reading about cyberwar in the scholarly articles. Stuxnet[15] `a computer virus attacked the Iranian nuclear site in 2010 directed towards uranium rich centrifuge to burn down themselves. The virus is said to be launched by US and Israel as 'Operation Olympic Games'[16] in furtherance of preventing Iran to develop its nuclear weapon[17]. It's been 10 years since Stuxnet and the engineers responsible are unfound[18]. Yet another cyber-attack that made the news was the attack on Estonian government[19] in 2007. Wherein the attackers attacked the critical infrastructure such as telephone exchange, banks, newspapers which resulted in disruption of ambulance and emergence services as well. While the links to attack was not found. The cyber attack had a direct severe impact on the civilians.

While Stuxnet has made its to reach masses, many other significant incidents are unheard of. The Center for Strategic & International Studies has listed out cyber-attacks on governmental institutions in recent times whose revelations are shocking.

Sl No	Cyber incident targeting governmental functions	Month of attack
01.	Cyber-attack on the police and interior ministry database in Belarus	August 2021
02.	Cyber-attack on high profile prison in Iran exposing the inhuman treatment of prisoners	August 2021
03.	Spear-phishing attempt on Slovak government by espionage group linked to Russia	August 2021
04.	Cyberattack on Israel's government during 2019 – 2020 found to be done by Chinese agencies	August 2021
05.	Estonia faced data leak of 286438 ID photos from its government database	July 2021
06.	Japan 2020 Olympics experienced data breach of volunteers including their passwords	July 2021

[15] Mcafee.com. 2022. *What Is Stuxnet? | McAfee*. [online] Available at: <https://www.mcafee.com/enterprise/en-in/security-awareness/ransomware/what-is-stuxnet.html> [Accessed 17 November 2021]. l

[16] Warrick, J. and Nakashima, E., 2012. *Stuxnet was work of U.S. and Israeli experts, officials say*. [online] The Washington Post. Available at: <https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html?utm_term=.3283038083d7> [Accessed 22 December 2021].

[17]Sanger, D., 2012. *Obama Order Sped Up Wave of Cyberattacks Against Iran (Published 2012)*. [online] Nytimes.com. Available at: <https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html> [Accessed 4 January 2022].

[18] Fruhlinger, J., 2017. *What is Stuxnet, who created it and how does it work?*. [online] CSO Online. Available at: <https://www.csoonline.com/article/3218104/what-is-stuxnet-who-created-it-and-how-does-it-work.html> [Accessed 21 January 2022].

[19] Kelsey, Jeffrey T. G. "Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare." *Michigan Law Review*, vol. 106, no. 7, The Michigan Law Review Association, 2008, pp. 1427–51, Available at: <http://www.jstor.org/stable/40041623.> [Accessed 8 January 2022]

07.	Pegasus scam where governmental authorities and politicians phones been installed with surveillance software	July 2021
08.	Iran gathered sensitive information from the US Military personnel through Facebook by using phishing sites	July 2021

*Data directly collected from the CSIS website.

With the above seen incidents of cyber-attack on governmental institutions either from the groups within the country or from other lack egal regulation. If going by the above-mentioned definition of cyberwar then entire world all the countries right now at some point of time are constantly engaging in cyberwar. The cyber incidents mentioned above can be treated as a 'cyberwar' going by the definition of cyberwar. But none of those incidents have taken place during a armed conflict or has given rise to an armed conflict thus escaping the application of IHL.

While a cyber-attack during a conflict is to be ruled under IHL norms, leaves behind the attacks that are not in lieu of a conflict. Cyberattacks cause greater economic loss and as well attract international attention such as that of human rights activists which may affect the international politics. Here comes the legal vacuum of international law to regulate the cyber-attacks between states as well as a state and a non-state actor outside the ambit of armed conflict. Intersection of IHL principles and public international law to bring in state liability and responsibility is the need of the hour owing to the frequency and intensity of cyber-attacks on governmental institutions.

Can state responsibility be attributed easily?

It is not easy to track the cyber-attack and attribute the liability and responsibility to a state as seen in conventional conflicts. Article VIII[20] of responsibility of states for internationally wrongful acts 2001 attributes the responsibility to the state for the wrongdoing of its organs. Such organs of the state that are under the state 'control' entitles the responsibility over the state. The meaning of 'control' can be deduced from the Nicaragua[21] and Tadic case. Where the Nicaragua judgment lays out effective control when such organs are in display of power over the actors and in turn the actors are in 'complete dependence' over the state. While the Tadic[22] judgments speak about overall control i.e., when the state is in control of organizing, supporting and coordinating the group. Cyber-attacks are not easy to be traced and many of such attackers have escaped their identification. With such a case in hand, effective control seems redundant[23] since establishing the link between the state and actors seems out of hand. As well, cyber-attack may not be cause from a nations' government

[20] Article VIII of the International Law Commissions Draft Articles on the Responsibility of States for International Wrongful Acts 2001

[21] Nicaragua v. United States, 1986, p. 392

[22] Prosecutor v. Tadic, 1995, para. 70

[23] Scott J. Shackelford,State Responsibility For Cyber Attacks: Competing Standards For A Growing Problem 1, Conference on Cyber Conflict Proceedings 2010 C. Czosseck and K. Podins (Eds.) CCD COE Publications, 2010, Tallinn, Estonia.

but by an individual or a group from a country against another the acts of which may be unknown to the host state[24]. The problem with attribution of responsibility in case of a cyber-attack is to prove beyond reasonable doubt since collection of evidence is tedious and non-viable at times.

Conclusion

The events of cybercrime and cyber war known no boundaries or jurisdiction. There needs an international structure to be formulated with high level cyber defense mechanism that each country is to built with. An international treaty obligation over the state will automatically entail pro-active steps by the nation state to install a cyber defender to protect its citizen and itself with international or transnational cybercrime and cyber war.

[24] Barney Warf & Emily Fekete (2016) Relational geographies of cyberterrorism and cyberwar, Space and Polity, 20:2, 143-157, DOI: 10.1080/13562576.2015.1112113