CYBER WARFARE: A DISCERNABLE BATTLEFIELD

Written by ***Shashwat Tandon***

Advocate, Kanpur Nagar District Court, Kanpur

ABSTRACT

The internet has indubitably become an indispensable part of our lives. It facilitates almost everything from a thing as casual and innocuous as social media to something as serious and important as defense of a country. With time this importance has been realized by various states and international organization with their focus shifting to sophistication of their cyber security.

Nations have been waging war against each other since their inception in the wake to further some national agenda. Initially the methods of war were limited to weapons only, however with passage of time and growing utility of the internet, the cyberspace has also become an equally effective medium. Intrusion with Iran's nuclear programme, alleged cyber-attacks by China on U.S systems to steal sensitive information are some examples of how the internet has be used to create a war like situation .such activities in the cyberspace are colloquially termed as 'Cyber Warfare, which generally involve actions by a state or international organization aimed to attack and damage computer networks of other states. These attacks may be directed towards financial institutions, infrastructure and other areas of national importance. However not all such activities can be termed as cyber warfare although they may contain the characteristics of the same, hence it is pertinent to distinguish between warfare and non-warfare activities. The pace at which threats may multiply in cyberspace is beyond any guess work and it not being a conventional war its intricacies obviously differ. This research paper aims to discuss the scope of cyber warfare, recent examples of such warfare in. The international arena, the principles and other legal framework governing it and the new laws being developed to regulate and minimize it.

INTRODUCTION

Computers and the internet have become an indispensable part of our lives today. Almost half of an average person's life who has access to such facilities is spent using the same. While the advantages of these resources are infinite, they do not exist without some cons. In the recent time the Internet has proved itself as a new front for waging war. The scenario has changed drastically Vis a Vis the use of computer systems in warfare. The resources that were initially meant to track and control the weapons have now themselves become weapons. Unlike the conventional weapons of warfare have witnessed gradual sophistication over the years, the tools of cyber warfare have developed at an unimaginable pace, more than what was required to draft a legal framework to regulate the same. This is not to be understood that the cyberspace is without some framework to stop the same, but the existence of the same has hardly been able to reduce the frequency of these attacks. Chances are that at a time when an ordinary man is carrying out his daily chores, a cyber-attack is being planned and executed in the same or some other part of the world. Therefore, it is imperative that the states recognize the threat that such cyber-attack pose to their security and work together to bring about a legal framework to regulate and prevent such warfare. To understand the intricacies of cyber warfare it is imperative to understand the legal framework in place, the emergence of the art and the tools and method involved and used to execute such an attack.

WHAT IS CYBER WARFARE?

The term cyber warfare is hard to define as there exists myriad definitions and explanations for the same due to the lack of a universally accepted definition. Several attempts have been made over the decades but all in vain. A very casual attempt to define it may lead to the conclusion that it is a situation where two or more states use cyberspace and the operations in it to intrude in each other's business, be it of any type which should not in the ordinary course be tampered with. However, this in no way presents the true picture of the term in question. Such warfare is not limited to state actors but involves several non-state actors as well. Anonymous and the Hezbollah are few such examples of non-state actors who were recently involved in cyber warfare. While it would not be fair to include every actor involved in a petty cybercrime like activity like spamming etc. As perpetrator of a cyber-attack, it is also true that it would not be

prudent to reject an activity solely based on the size of the organization as even an individual is equally capable of initiating cyber warfare.

While such a cyber-attack has most of the characteristics of conventional war, to equate it with the same shall not be appropriate while looking for an appropriate definition for the same. Differentiating it from every common tactically motivated web attack and giving due consideration to capability to cause serious threat to state's security is also important. Having due regard to the factors listed above the most suitable definition would be "*Cyber war is an extension of policy by actions taken in cyber space by state or nonstarter actors that either constitute a serious threat to a nation's security or are conducted in response to a perceived threat against a nation's security*[i]*".*

TO WHAT EXTENT ARE THE LAWS OF WAR APPLICABLE TO CYBER WARFARE?

To primary step in attributing the law of war to any cyber-attack is to check the appropriateness of their applicability to the given scenario. The Geneva Convention of 1949, the additional protocols, the Hague Convention of 1907 and relevant customary international laws make constitute the laws governing wars. There laws are only applicable when the existence of an armed conflict has been established and the rules of *jus in bellum (*situations in which war can be waged) *and jus in Bello (*means and methods of war) duly apply.

Although cyber warfare does not find a separate mention in the laws of war, that in no way means that it is out of is purview and can be initiated at ones will without any regulation or consequences. The laws of war were drafted at a time when cyber warfare as a means of war could not have been dreamt of even in one's wildest dreams. There are many other weapons or means of war that find no mention in the laws of war but even these are agreed to be covered by the laws of war by all state parties. These laws are generally drafted given a humanitarian characteristic and hence are applicable to types of warfare and weapons. In fact, all state parties have reached a consensus that some small lacunae shall not stand in the way of application of these laws where needed. Hence from the above discussions it is safe to conclude that while

drafting the law of wars the state parties were conscious of the fact that the laws do not cover all the means of war and the possibility of new weapons emerging in the future but wanted these laws to cover such means too. Also, a legal obligation exists under the laws of war for the state parties to check the legality of an invented weapon even if not mentioned in the laws. If this was not the case and the list of weapons was exhaustive then the drafting if such laws would have been rendered useless and obsolete. Further these laws have over time gained the status of a customary international rule and must be observed by each nation irrespective of the fact that they are not a party.

DOES CYBER WARFARE CONSTITUTE AN ARMED CONFLICT?

The question that needs to be answered before a cyber-attack can be termed as cyber warfare is whether it constitutes an armed conflict as defined by the laws of war under common article 2 of the Geneva Convention 1949[ii]. There is no uniform definition provided for an armed conflict in the convention itself however the ICRC commentary has given an interpretation to it which reads as "*any difference arising between two states and leading to the intervention of members of armed forces, even if one of the patties denies the existence of war. It makes no difference how long the conflict lasts, or how much slaughter takes place*[iii]*".* It is important to differentiate between the various types of war like attacks according to the warfare element present in them. While it is easy to classify conventional methods of attack of which cyber-attack in just one part, the classification of attacks which solely contain the element of a cyber-attack is particularly difficult. A number of tests have been proposed by jurists to determine if a single cyber-attack can constitute an armed conflict. One theory in support of this proposition states that it may constitute an armed conflict if there is *physical manifestation like explosion*[iv]. The only problem with this theory is that it is incomplete. Acts that have tendency to or are intended to terrorize civilian population in an area are strictly prohibited by the law of war. An attack would also include within its purview, neutralization of a target[v] hence the proposition that a physical manifestation is a pre requisite stands rejected.

The second test proposed in this regard is the *'intent and likely result'* and this is to be applied on case to case basis. The problem with this test is that it involves subjective judgement[vi]. So

if legality of an attack is not challenged in court of law, the attacking state party gets the discretion to define as to what constitutes an armed conflict hence opening up a possibility for abuse. However, this is not a new problem by any stretch of imagination. History shows that more often than not state parties have been reluctant to recognize a state of war, that is precisely the reason why formal declaration of war in not an essential requirement any more[vii].

Therefore, the most appropriate test to determine if a single cyber-attack could amount to an armed conflict would be one which looks at the motivation behind the war laws which is to minimize damage and suffering while not interfering with military efforts to succeed in the war[viii]. Therefore, a cyber-attack could be said to be an armed conflict if "*it causes or is intended to cause physical damage or human injury or spread terror among the civilian population, and the action is undertaken by a state or by other persons whose actions can be attributed to a state*[ix]*"*.

WHAT ARE THE RESTRICTIONS IMPOSED ON CYBER ATTACKS?

It only makes sense that if law of war is applicable to cyber-attacks, the applicability of restrictions that come with it could also not be denied.

The **fist restriction** is the compliance with the ***principle of distinction*** which is one of the most significant principle of humanitarian law. The provisions relating the same could be found in article 48[x] and article 51 of the Additional Protocol 1. The principle states that during the time of war a distinction has to be made between the civilian population and the combatants and only the combatants are to be attacked.

Only military combatants and objects used by them are legitimate targets[xi]. For the application of the general clause i.e. article 48 of the additional protocol it is necessary to differentiate between civilian and military objects. Whatever is the test that applies to a conventional military attack shall apply to a cyber-attack while deciding as to which objects can be attacked and which cannot. Concerns have been raised with respect to targets that are or can be used for both military and civilian purposes. In case of a cyber-attack the networks that are attacked are

of such dual use nature and hence the instances of abuse are quite common. However, this problem is not a new one and it existed even before something like cyber warfare existed.

Any sort of an indiscriminate attack[xii] is prohibited by article 51(4) of the additional protocol 1. To summarize it is an attack which does not follow or observe the principle of distinction. For instance, a virus programme that target civilian as well as military network can be termed as an indiscriminate attack. Hence any such attack is prohibited by article 51(4).

Every cyber-attack involves a certain degree of sophistication which a common soldier may not possess. So, the issue that arises is that whether the perpetrators of the cyber-attacks are to be treated as civilians or as combatants. To answer this question the definition of civilian as provided in the Geneva Convention of 1949 has to be analyzed. Although the convention does not define who a civilian is, it does describe we do not fall within the category of civilians. *." Combatants re quires the fulfillment of four criteria. The combatant has to be commanded by a person responsible for his subordinates, wear a distinctive sign visible at distance, carry his arms openly, and conduct operations in accordance with the laws and customs of war.50 a combatant is a legitimate target. A civilian on the other hand is protected from attack, "unless and for such time as he takes a direct part in hostilities*[xiii]*."* So, it could be safely said that a civilian attacking a computer resource in another state is directly involved in hostilities. Therefore, if cyber warfare is absolutely necessary during the time of war, the state should have their soldiers or combatants do it rather than its civilians whose status not clear in this regard. While these four requirements are solid in cases of conventional war crimes, there is a need to reevaluate them in the light of cyber-attack because in such cases there is no physical activities involved and the so-called combatants may be sitting a thousand miles away hence rendering the differentiation obsolete.

The second restriction is that of perfidy. Article 37(1) of additional protocol defines this restriction *as inviting the confidence of an adversary to lead him to believe that he is entitled to, or is obliged to accord, protection under the rules of international law applicable in armed conflict, with intent to betray that confidence*[xiv]*".* It is important to distinguish perfidy from ruse of war. Ruses may be defined as a war act carried out to mislead the opponent resulting in a reckless action by him but they do not instill any hope or confidence with respect to any

protection. An example of perfidy is sending an email or any electronic document pretending to be sent from a reputable source which in reality containing a logic bomb[xv]. The restriction with respect to a perfidious act is restricted to killing, injuring or capturing an adversary by carrying out such an act.

The third restriction is that of the principle of neutrality. A person or state is said to have acted in contravention of this principle when he uses the structure or network of some other country to attack a third nations computer networks. This principle is legitimized and can be found in the Hague convention and contains various rights and duties that are to be observed by neutral states as well as the nations at war. The existence and demarcation of territory is very important for a nation to exercise and determine the extent of its sovereignty. The principle of inviolability is absolute that a state is sovereign within its own borders. But the question that arises in this scenario is whether cyberspace is a part of territory and if yes then is the usage of the cyberspace of a third nation equivalent to breach of sovereignty. This issue arises because people involved in cyberwarfare TN to use or disguise themselves so as to pretend that the network being used to wage these attacks is of some other country. Article 2 of the fifth Hague convention prohibits troops and things carried by them to be moved across border to a neutral state which suggests that physical invasion is a pre-requisite which is not fulfilled when the internet network of a neutral country is used. The Hague convention is an old law which could not have inculcated or foreseen the cyberspace being used as a weapon to wage war and hence does not contain any provision regulating or prohibiting the same. However, the usage of the network of a third country cannot be blamed on that country as it is very difficult to detect as to when and for what purpose the network is being used. Also, the fifth Hague convention contains an exception for telecom which allows neutral states to give access to their networks to parties at war so long the granting of access is done impartially.

CYBER WARFARE AND PECULIAR PROBLEMS

The primary problem is proving the origin of an attack in cases of cyberwarfare. The thin line of difference between war crimes and ordinary crimes becomes hard to point out. The

intangibility of cyber-attacks makes it hard to deal with when compared to conventional military transactions.

The reason for this is that masking one's identity in a cyber transaction is extremely easy. There is also the threat of hacktivism which cannot be ignored. It is defined as "*computer hacking intended to communicate a social or political message, or to support the position of a political or ideological group*[xvi]. These hacktivists are highly trained people and though their intentions are noble and it is believed that they will not use their knowledge and resources to initiate a cyber war, the possibility of the same cannot be completely ruled out and nations need to be cautious and prepared in case such an occurrence presents itself as a challenge or threat. The biggest problem is that of establishing a link between the hacker and the state who employed him. This problem was eased to an extent after the Iran case in which the International court of Justice held that – "*actions of a state's citizen can be attributed to the government if the citizen acted on behalf of the state, having been charged by some competent organ of the state to carry out a specific operation*[xvii]*".* However, proving the extent of control can be an extremely tiring task.

Another issue with cyber-attacks is that more often than not the victim of the attack cannot be identified unlike in conventional was where causalities can easily be determined. The recent attack by the Chinese on the google system is a good example to understand this problem. Was this merely a criminal act or was it an act of war against the state. If the involvement of the Chinese government in the attack can be proved then it could be said that sovereignty of the other state has been hampered as googles headquarters are for the purpose of war a civilian and they cannot be the subject of an indiscriminate attack. Here a loss is not a physical one but an economic one. Article 49(1) of the additional protocol 1 contains the definition of attack which interpreted in anyway does not include economic loss hence it cannot in a legal sense be termed as an attack.

Non state actors are also a very big problem identifies with cyber-attacks. Cyber warfare offers easy and inexpensive opportunities to non-state actors to engage in the same. In the cyberspace the difficulties of conventional battlefield do not exist which allows them to target big players and achieve best efforts while applying minimal efforts. This is precisely the reason why

authors are demanding a new cyber warfare regime so as to reduce these easy opportunities available to the non-state actors. However, the problem is much bigger than cyber warfare when it comes to non-state actors the treatment of any action by them of such nature has no universally accepted framework.

CONCLUSION

Those who are against the introduction of a new cyber warfare treaty regime argue that such actions pose problems that are beyond a solution specially when it involves dual use object and non-state actors. The problem lies in dealing with cyberwarfare as a new aspect of warfare and finding answers for which there are no questions. A new treaty would be rendered completely futile without first determining the role and regulation of dual use objects. Also new treaty would not be applicable to non-state actors. There is no denying the fact that attributing the laws of war to cyber-attacks is quite a difficult task but these cyber-attacks when used for a noble purpose and by the military help in reducing capsulitis and avoiding the effect of war. One of the primary objectives of war is to reduce harm and suffering and more often than not cyber methods help achieve this objective. So as of now there is no need for a new regime for cyber warfare and the existing regime is suitable to deal with the existing situation if the same is done in accordance with the general principles and objectives of humanitarian law.

BIBLIOGRAPHY

1. Jason Andress and Steve Winterfeld, (*cyber warfare: techniques tactics and tools for security practioners), elseiver, 2011*
2. Catherine A Theohary, CyberWarfare and Cyber terrorism: in brief, https://fas.org/sgp/crs/natsec/R43955.pdf.
3. Nils Melzer, Cyberwarfare and International Law, http://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf
4. Karnika Seth, *computers Internet and new technology laws,* Lexis Nexis, ed. 2013

5. Paul Cornish, David Livingstone, Dave Clemente and Claire Yorke, A Chatham House Report on Cyber Warfare.
6. Martin C. Libicki, Cyberdeterrence and cyberwar, https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf

REFERENCES

[i] PAULO SHAKARIAN JANA SHAKARIAN ANDREW RUEF, Introduction to cyber warfare: a multidisciplinary approach.
[ii] "The present Convention shall apply to all cases of declared war or any other armed conflict [...]. The Convention shall also apply to all cases of total or partial occupation of the territory of a High Contracting Party [...].*29
[iii] ICRC Commentary, supra note 29, Article 2, para. 1, p. 20.
[iv] Louise Doswald-Beck, Some Thoughts on Computer Network Attack and the International Law of Armed Conflict, in Computer Netwo
[v] See Article 52 (2) of Additional Protocol I.
[vi] Emily Haslam, Information Warfare: Technological Changes and International Law, 5 J. Conflict & Sec. L. 157,167 (2000).
[vii] See Common Article 2 of the Geneva Conventions: "[...] the present Convention shall apply to all cases of declared war or of any other armed conflict which may arise between two or more of
[viii] Leslie C. Green, The contemporary law of armed conflict 348 (2nd ed. 2000).
[ix] Cyber Warfare Challenges for the Applicability of the Traditional Laws of War Regime, Jenny Döge, http://www.jstor.org/stable/25782613
[x] 39 Leslie C. Green, The contemporary law of armed conflict 348 (2nd ed. 2000). 40 Article 48 Additional Protocol I read: "In order to ensure respect for and protection of the civilian population and civilian objects, the Parties to the conflicts shall at all times distinguish between the civilian population and combatants and between civilian objects and militia
[xi] Article 52 (2) of Additional Protocol I
[xii] attacks that are not directed at a specific military objective, or (b) those which employ a method and means of combat which cannot be directed at a specific military objective, or (c) those which employ a method or means of
[xiii] Supra9
[xiv] See Article 37 (1) Additional Protocol I.
[xv] A logic bomb is a particular type of Trojan horse that activates only when a certain condition is met. Trojan Horses are code
[xvi] US-China Economic and Security Review Commission, Report on the Capability of the People's Republic of China to
[xvii] United States Diplomatic and Consular Staff in Tehran, Judgment, I. C. J. Reports 1980