e-ISSN 2582-4570

CYBER WARFARE AND THE PRINCIPLE OF DISTINCTION UNDER INTERNATIONAL HUMANITARIAN LAW: SOME CRITICAL REFLECTIONS

Dr. Santosh K. Upadhyay[*]

ABSTRACT

Cyber warfare is one of the emerging realities of the current age. It is termed, by many, as a fifth domain of warfare after land, water, air and space. The cyber space is mostly man-made and provides many unique opportunities to the hostile parties to achieve desired results even without involving any kinetic force. It is the space where anonymity is the rule and to find a causal link of any effect is a bit difficult in comparison to other natural mediums. This medium seriously compromises the principle of distinction that is one of the cardinal principles International Humanitarian Law. The article analyses the application of the principles of distinction in respect of definitions of combatants and military objectives in the contexts of cyber warfare. It concludes that there are many situations during cyber warfare that may compromise the scrupulous application of the principle of distinction.There is a need to develop legal thinking in respect of these grey areas and one aspect of such thinking may be that cyber warfare should not be considered as a means and methods of warfare but as a separate weapon. This may herald new approaches to regulate cyber warfare.

I. Introduction

The computer and internet technology provide immense opportunities to human civilizations. Both states and private actors are now heavily relying on this technology in regulation and smooth functioning of almost all of their activities. Atomic reactors, electricity grids, air, rail and metro traffic controls, banking systems, essential and life-saving facilities at the hospitals are the major examples of use of computer and internet technology. The modern human civilizations have become much accustomed to the computer technology that any disturbance or manipulation in it may be of catastrophic outcome.

Thus, for the states to use the cyber mediums to conduct military operations against the computer systems of adversaries during armed conflict is very attractive option. The bottom

[*] Assistant Professor (Senior Scale), Law Centre II, Faculty of Law, University of Delhi

line of all the uses of computer technology is the flow of data from one computer system to another in a manner designed by human agents. Computer networks programs developed by human agency facilitate this design of flow of data and the stipulated results. The nexus between the human agents and the particular design and result, though, may be remote but it is *sine qua non*. A specific computer programming may use many intermediate automatic steps before bringing the final desired outcome but the initial design by human being is essential. The causation link may be remote or difficult to ascertain but it always exists. A large-scale worldwide physical infrastructure like satellites, routers, undersea cables etc. provide necessary support to this designed data transfer. Thus, any activity in cyber space is the result of human induced designed data transfer from one computer system/s to another computer system/s with howsoever-intermediate steps and facilitated by worldwide infrastructures.

Further, any military operations through cyber medium involve three important factors. First, the human agents operating the data transfer – it includes the persons who are instrumental in inserting or operating the specific computer program into the system. The technicians that are part of the development of such program does not *ipso facto* becomes part of any warfare activities in cyber realm. It does not seem that time has ripen to discuss the stockpiling and production of computer programs into the disarmament debate. The second important factor is the designed data transfer i.e. the program itself. The designed program and the intermediate steps used by it and its spread over other system/s are all the important factors in the cyber realm. The third important factor is the infrastructures that support such data transfer. They include the routers, sea cables, satellites, computer systems etc.

The term 'cyber warfare' is indeed the term of art and its various definitions cover primarily two criteria. First, that it is warfare conducted in the cyber space using programming based on computer network systems. In more simple term, it is the 'warfare conducted in cyberspace through cyber means and methods'.[1]Thus, to kill or capture the persons involved in cyber warfare or to damage or destroy cyber infrastructure by the kinetic force are not the subject matter of cyber warfare. It, however, does not preclude the discussions about who are the persons involved in cyber warfare or to ascertain how the infrastructure supporting the cyber warfare become the military objective.

[1] Nils Melzer, 'Cyber Warfare and International Law' *UNIDIR Resources* 4 (2011), *available at*: https://unidir.org/sites/default/files/publication/pdfs/cyberwarfare-and-international-law-382.pdf(last accessed on 23 August 2023) .

The second criteria restricts it to only those activities that can be the subject matter of International Humanitarian Law (IHL). Thus, as per one definition "cyber warfare" only refers to the small subset of cyber-attacks that do constitute armed attacks or that occur in the context of an ongoing armed conflict.[2]CordulaDroege, defines 'cyber warfare' as 'means and methods of warfare that consists of cyber operations amounting to or conducted in the context of an armed conflict within the meaning of IHL only'.[3] Thus, the term 'cyber warfare' includes only those cyber means and methods of warfare that are conducted in the context of an ongoing armed conflict in the sense of IHL. It does not include cyber criminality or cyber terrorism where IHL does not involve.[4]Going in the same vein, the term 'cyber warfare' for the purposes of this paper, includes the cyber operations conducted in the context of an ongoing armed conflict in the sense of IHL. It does not entertain any discussion on whether a particular cyber operation constitutes a use of force or threat to use of force.

Thispaper first discusses the specificity of cyber world and the reason for their proneness to serve as one of the prominent mediums of warfare. In the next part, it analyses the meaning of the term 'attack' and its possible interpretationswhen transposed to the realities of the cyber warfare. After this, it discusses the principle of distinction in respect of cyber warfare in little detail. This discussion has been undertaken in respect of requirements of being considered as combatants during cyber warfare so as to enjoy combatant privileges and immunities and the understanding about military objectives in respect of cyber world. The last section discusses the conclusion and notes down some suggestions.

II. Specificity of Cyber Space

Cyberspace is a 'globally interconnected network of digital information and communication infrastructures, including the internet, telecommunications networks, computer systems and the information resident therein'.[5]It has been created by human beings and in contrast to the other mediums of warfare like land, air, sea and space that are governed by the law of nature, the cyber space is governed by law of human technology. Whereas in natural mediums, the challenge is to discover the law of nature to ascertain cause and effect relationship but in

[2] Oona A Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue & Julia Spiegel, 'The Law of Cyber Attack' 100 (4) *California Law Review* 821 (2012).
[3] Cordula Droege, 'Get Off My Cloud: Cyber Warfare, International Law and the Protection of Civilians' 94 (886) *International Review of the Red Cross* 538 (2012).
[4] *Supra* note 1at 21.
[5] *Id.* at 4.

cyber mediums that isresult of inventions, the expertise over invented rules are always subjected to new inventions.

Thus, the cyber space is the space where both the framework as well as the rules are developed by human intellect. It is easier to establish cause-effect relationship in natural mediums like land, sea, air and space than that of cyber space. Hence anonymity is the rule than exception in cyber space and the concrete information about source of any activity is always not easy to ascertain. Moreover, the physical infrastructures like cables, satellites etc. through which the cyber operations are carried are used simultaneously by many actors at a time. Hence, it will be difficult to classify the nature of the use of these infrastructures at any given time.

This uniqueness of the cyber space and the inherent challenges therein are well describedin the following wordsof Nils Melzer:

> "[C]yberspace is the only domain which is entirely man-made. It is created, maintained, owned and operated collectively by public and private stakeholders across the globe and changes constantly in response to technological innovation. Cyberspace not being subject to geopolitical or natural boundaries, information and electronic payloads are deployed instantaneously between any point of origin and any destination connected through the electromagnetic spectrum. These travel in the form of multiple digitalized fragments through unpredictable routings before being reconstituted at their destination. While cyberspace is readily accessible to governments, non-state organizations, private enterprises and individuals alike, IP spoofing and the use of botnets, for example, make it easy to disguise the origin of an operation, thus rendering the reliable identification and attribution of cyber activities particularly difficult."[6]

The computer systems around the globe are most vulnerable to be attacked nowadays. The reasons for its vulnerabilities are many. First, it is very much cost effective and involves almost no kinetic efforts to get the desired results. Even without firing any shot and shedding away the life of a soldier, the enemy's capabilities to sustain war may be weakened to the desired result. Second, the complexity of the cyber operations makes it a desired target at anytime. The aggressor or attacker just needs to know only one or a few weak points in the

[6] *Id.* at 5.

whole system and the desired result could be achieved easily. Commenting on the complexity of the cyber world and the chances of its exploitation, Jack Goldsmith, most vividly said that:

> "Most computers connected to the Internet are general purpose machines designed to perform multiple tasks. The operating-system software that manages these tasks, as well as the computer's relationship to the user, typically has tens of millions, and sometimes more than 100 million, lines of operating instructions, or code. It is practically impossible to identify and to analyse all the different ways these lines of code can interact or might fail to operate as expected. And when the operating-system software interfaces with computer processors, various software applications, web browsers and the endless and endlessly complex pieces of hardware and software that constitute the computer and telecommunications networks that make up the Internet, the potential for unforeseen mistakes or failures becomes unfathomably large."[7]

Third, the benefits that cyber medium gives to the attacker in respect of difficulty in identity and attribution. The cyber space is the space of anonymity that is always puzzled with the precise location from where the impugned cyber activity started. Fourth is the geographical ease to attack any part of the world from anywhere.[8]It provides the combatants to fight the war from the distance and the cyber attackers are mostly emotionally detached from the effects of their activities.[9]These are the primary reasons that make cyber medium now the most desired framework for combat purposes. This has prompted some of the scholars to term cyber space as fifth domain of warfare after land, water, air and space.[10]

The need that states must put in order a technically sound and reliable cyber security regime is now the most urgent task of the hour. However, the challenge to the cyber security during the time of war is more severe than that at the time of peace. The war permits the conduct of military operations against the cyber security of the adversary, provided it has become the military objective. However, the peacetime attacks against cyber security involve the issues related to wrongfulness, jurisdiction and evidence; the concerns of wartime attacks against cyber security are of different character. They mostly involve the determination of nature of

---

7 Jack Goldsmith, 'How Cyber Changes the Laws of War' 24(1) *EJIL*, 130 (2013)
8 *Id*. at 131.
9 Michael Grevais, 'Cyber Attacks and the Laws of War' 30(2) *Berkely Journal of International Law* 532 (2012).
10 *Supra* note 1 at 3.

military operations, extent of attack and analysis of outcome within the framework of IHL. Now the next sections would further elaborate some of these issues.

III. Attack in the Cyber Space

Before going further, it is pertinent to discuss the meaning of the term 'attack' in cyber space. The basic idea here is to analyse the notion of attack as it is in IHL and to see whether this definition can be useful to describe the activities in cyber space. It is also important for the reason that most of the protection of IHL are granted against attack.[11] It will further help one to understand what kinds of operations will come under the regulation of IHL.

Article 49 of the Additional Protocol I defines attack as "acts of violence, against the adversary, whether in offence or defense". The phrase 'acts of violence' has created much controversy in respect of the non-kinetic nature of the cyber-attacks. Cyber-attacks are basically the actions taken through the use of computer networks to disrupt, deny, degrade or destroy information in computers and computer networksand it also includes the damage to the computer network themselves.

However, it has not always been the case where only kinetic nature and inbuilt violence of the object has been considered as attack for the purposes of IHL. The example of chemical and biological weapons are very pertinent in this respect. These weapons are non-kinetic and free from inbuilt kinetic characterbutthere use has been recognized as attack for long because of their violent outcome. In a similar manner, the cyber-attacks could also be termed as attack by considering their outcome. However, this approach further raises two questions based on the probable outcome of the cyber-attacks. The outcome of the cyber-attacks may be sometimes violent and sometimes may not be violent. They may cause destruction, damage (violent effect) or they may only neutralize (non-violent outcome) the functions of some systems. Thus the issue emerges what kinds of outcome of cyber operations can be considered as attack. Primarily there are two kinds of approaches supporting each stands.

Michael N. Schmitt has advocated the position in 2002 that only such cyber operations could be termed as attack under IHL that necessarily have violent outcome.[12]He has stipulated that the principle of distinction contained in article 48 of the Additional Protocol I doesnot

[11] Additional Protocol I to the Geneva Convention of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I) of 8 June 1977. See articles, 12 (1), 41 (1), 44(3) 51 (2), 52 (1).

[12] Michael N. Schmitt 'Wired Warfare: Computer Network Attack and the Jus in Bello' 84(846) *International Review of the Red Cross* 377-378 (2002).

encompass all kinds of military operations and thus some kinds of military operations may remain outside from the scope of this principle, like psychological operations against civilians.He further stressed that article 48 only prohibits the attack on civilians and civilian objects and does not prohibit targeting them in any other manner that does not qualify as an attack.[13]

By establishing these points, he further defined attacks as the activity that must have violent consequences and thushe does not accept any cyber operations that do not have violent consequences as an attack. He was of the view that all other cyber operations are not prohibited and thus may be used without inviting any IHL inquiry. He further termed itpermissive approach probably in a sense that it permits all those cyber targeting that are not violent in consequences.

Knut Dorman propagated the second approach and advocated that not only the violent outcome but also any neutralization of the object would also be termed as attack under IHL.[14] He developed his argument onthe definition of military objectives contained in article 52(2) of Additional Protocol I. Military objective is one "whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage".[15]Knut Dorman pointed out that:

> "The fact that CNA does not lead to the destruction of the object attacked is irrelevant. In accordance with Art. 52(2) of AP I only those objects, which make an effective contribution to military action and whose total or partial destruction, capture or neutralization offers a definite military advantage, may be attacked. By referring not only to destruction or capture of the object but also to its neutralization the definition implies that it is irrelevant whether an object is disabled through destruction or in any other way."[16]

However, criticizing both the versions for falling short of satisfactory interpretation of the notion of attack in context of cyber operations, Nils Melzer advocated that thrust should be to ascertain whether the cyber operations constitute part of the hostilities within the meaning of

---

[13] *Id.* at 378.
[14] Knut Dormann, 'Applicability of the Additional Protocols to the Computer Network Attacks' (2004) 4, *available at*: https://www.icrc.org/en/doc/assets/files/other/applicabilityofihltocna.pdf(last visited on Aug. 23, 2023).
[15] *Supra* note 11, art. 52(2).
[16] *Supra* note 14 at 6.

IHL.[17] Any cyber operations if conducted in nexus with the armed conflict fall under the ambit of armed conflict irrespective of its nature to becharacterized as attack in standard IHL formulations. For this, he pointed out that the basic rule of distinction is formulated in terms of military operations and not in the term of attacks.

CordulaDroege,while supporting the point that other military operations that though may not strictly be termed as attack are not immune from IHL scrutiny, indicated thebasic problem with Melzer's theory that it fails to answer what would strictly be fall under the concept of hostilities.[18]Further, while elaborating on the concept of attack, she concluded that attack should also encompass such operations that disrupt the functioning of objects without physical damage or destruction, even if the disruption is temporary.

Rule 30 of Tallinn Manual defines cyber-attacks as "a cyberoperation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects".[19]The most of the experts at the Tallinn deliberations were also of the view that damage includes the loss of functionality if it requires the replacement of physical component.[20]Though there was disagreement also about the extent of repair,Michael N Schmitt while rewriting his view in 2014 observes that the "loss of functionality would include situations requiring reloading of the operating system or any software essential to operation, but would not include replacing data that was merely stored on the system."[21] Moving the debate further, CordulaDroege highlighted in the most succinct way the notion of loss of functionality and the related question in the following words:

> "However, not all cyber operations directed at disrupting of the functioning of infrastructure amount to attacks… the difference lies in the fact that in some cases it is the communication function of cyber space alone that is being targeted; in other cases, it is the functioning of the object beyond cyber space in the physical world. While interference with cyber systems that leads to disruption in the physical world

---

17 *Supra* note 1 at 27. He states that "the applicability of the restraints imposed by IHL on the conduct of hostilities to cyber operations depends not on whether the operations in question qualify as "attack" … but on whether they constitute part of the "hostilities" within the meaning of IHL."

18 *Supra* note 3 at 555.

19 Michael N. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*106 (Cambridge University Press, Cambridge, 1st ed., 2013).

20 *Id.* at 108.

21 Michael N Schmitt, 'Rewired Warfare: Rethinking the Law of Cyber Attack' 96(893) *International Review of the Red Cross* 203 (2014).

constitutes attacks, the question of interference with communication systems such as email systems or the media is not entirely solved."[22]

Thus, now a days, there is wider agreement among the scholars that disruptions of functionality of some higher degree must also be termed as damage and thus comes under the IHL's inquiry if happened in nexus with the armed conflict. The current literature on the subject has moved forward from the original debate between Knut Dormann and Michael N Schmitt about the requirement of violent consequences of any cyber operation. However, there seem to be disagreement about the extent of damage of functionality and there are attempts to measure this threshold vis- a-vis the efforts that are necessary to restore back the original functionality.

Thus, what the functionality test does at last is to depend the applicability of IHL on the technical requirement that is needed to restore the original function. This may further cause problem with the development of new technologies because some technically sound countries may achieve functionality without doing something extraordinary and for some countries the restoration of functionality may take some arduous attempts. Given the nature of the cyber operations, it would also not be an easy task to precisely determine the efforts needed to restore functionality and to decide on this basis whether particular cyber operations would fall under IHL scanner or not.Thuseven the functionality is not immune from further problems of understanding.

IV. The Principle of Distinction in Cyber Space

The principle of distinction limits the options of attack for the parties to the conflict. It requires that only combatants and military objectives would be the target of any military operation and civilians and civilians objects must not be subject to attack. It is one of the manifestations of the basic principle of laws of armed conflict that any conflict must be conducted by limited means and the rights of the conflicting parties to adopt the means of injuring the enemy is not unlimited.[23] The International Court of Justice has termed it as one of the cardinal principle of IHL.[24]

---

22 *Supra* note 3 at 560-561.

23 Robert Kolb and Richard Hyde*An Introduction to the International Law of Armed Conflict,* 125 (Hart Publishing 2008)

24 *Legality of the Threat or Use of Nuclear Weapons (Advisory Opinion)*[1996] ICJ Rep. 226, para 78.

The principle of distinction, in its most precise and clear sense, has been stated under article 48 of the Additional Protocol I of 1977. It states that:

> "In order to ensure respect for and protection of the civilian population and civilian objects,the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives."[25]

The protocol further positively defines the terms 'combatants' and 'military objectives' and prescribes certain conditions to be fulfilled for being characterized as such. However, the terms 'civilians' and 'civilian objects' have been defined negatively and all those persons who are not combatants are termed as civilians and all those objects that are not military objectives are considered as civilian objects.

The basic idea behind the negative definitions of the terms 'civilian' and 'civilian objects' is to avoid any gap in the protection given by law.There should be only two categories and all those persons that are not combatants and all those objects that are not military objectives must be protected from military operations. In case of any doubt, the civilian nature of the individual or objectwould prevail.[26]

These definitions are immune from the methods of warfare and they must apply with all their sanctity in case of any cyber warfare. However, due to the unique nature of cyber warfare, the application of these principles needs a fresh insight in various factual situations. The paper now discusses these concepts in respect of cyber warfare.

Combatants in Cyber Warfare

The characterization of any person as combatant makes such individual immune from any liability for lawful violence committed by that person during armed conflict and it also entitlessuch person tothe status of prisoner of war if caught.Combatants have the right to participate in the hostilities and they are required to distinguish themselves from the civilian population during attack or while making preparation to the attack.[27]IHL providesmainly three categories of persons that may be termed as combatants.

---

[25] *Supra* note 11, art. 48.
[26] *Id.*atart. 50 and art. 52(3)
[27] *Supra* note 11, art. 44(3)

First, the members of the armed forces of the parties to the conflict, other than medical personnel and chaplains,and the members of the militias or volunteer corps forming part of the armed forces. Second, themembers of other militias and volunteer corps could also be considered as combatants if they fulfill the requirements of – being under responsible command, carrying arms openly, fixed distinctive signs recognizable at distance. These three requirements are not specifically mentioned in respect of the first category of combatants only for the reason that the members of the armed forces and other volunteer corps forming part of such force are always supposed to follow these requirements. This becomes very specific by article 44(3) of the Additional Protocol Ithat requires that all the 'combatants are obliged to distinguish themselves from the civilian population while they are engaged in attack or a military operations preparatory to an attack.[28]Thus, the members of the armed forces are also required to follow these requirements if to be considered as lawful combatant under IHL.Even in case of guerrilla warfare where surprise attack is the norm, combatants are required always to carry arms openly during each military operation or preceding the launching of an attack in which he is to participate.

Third category is the category of *levee in masse*. According to this, the inhabitants of non-occupied territories who spontaneously take arms on the approach of the enemy are also considered as combatants provided they carry arms openly and respect the laws and customs of war.[29]

However, if one applies these requirements in context of cyber warfare, the following problematic areas may emerge. First, how the requirement of carrying arms openly should be understood? Nils Melzer has suggested that this requirement may be fulfilled "when the cyber operation are not conducted by feigning protected, non- combatant status within the meaning of the prohibition of perfidy"[30]. Talinn manual summarily neglects this requirement by observing that 'the requirement to carry arms openly has little application in the cyber context'.[31]

However, this requirement is the part of the basic principle of distinction. The requirement of carrying arms openly atleast during operations or during immediate preparation before attack

[28] *Id.*atart. 44(3).
[29] Geneva Convention Relative to the Treatment of Prisoners of War (Third Geneva Convention) of 12 August 1949, art. 4A (6).
[30] *Supra* note 1 at 34.
[31] *Supra* note 19 at 100.

helps the adversary locate the exact points of origin of violence so that counter attacks can avoid unnecessary civilian causalities. The insertion of this term has a definite purposive meaning and not a mere addition of figurative words. Thus, it does not seem proper to declare this requirement meaningless.

It is the duty of the combatant to distinguish itself from the civilian and carry arms openly. Primarily, it seems wrong to neutralize this requirement at the altar of convenience or technology. The basic philosophy of IHL that any new technology if it is to be used in the armed conflict must correspond itself to the requirement of IHL. The burden of adjustment lies towards the technology and not on the IHL. The debate may be on the mechanism of the applicability but it is not proper to reject summarily the applicability of any IHL requirement in respect of some technological advancement. The same sort of obligation has also been stated in article 36 of the Additional Protocol I in the following words:

> "In the study, development, acquisition or adoption of a new weapon, means or methods of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of International law applicable to the High Contracting Party."[32]

Thus, the requirement of carrying arms openly could be completed in the cyber world by designating a specific IP addresses from where the cyber attack is emanating and making all the computer systems that are participating in such military operations explicit on the cyber web. This argumentation may seem absurd and as observed by Dinniss[33]may amount to putting computers directly on the target by the adversary. If it is not possible in advance, atleast when the cyber-attack starts all the IP addresses from where it is emanating must be explicitly manifested. The camouflage use of any civilian computersfor launching an attack must be considered as human shield in the language of IHL.

---

[32] *Supra* note 11, art. 36.

[33] Heather Harrison Dinniss 'Participants in Conflict – Cyber Warriors, Patriotic Hackers and the Laws of War' in Dan Saxon (ed.) *International Humanitarian Law and the Changing Technology of War* 257 (MartinusNizhoff Publishers 2013). The author observes"requiring a computer to be marked as a military computer is tantamount to placing a target on any system to which it is connected. The internet is constantly searched or crawled by millions of software boat searching for military designated IP addresses would be able to find them in a matter of minutes. Once identified, the only way to effectively move the computer or system out of range is to disconnect it, a solution which is likely to disrupt its normal running or usefulness."

All the persons who are engaged in the cyber-attack must always bear the uniform or any distinctive signs. This is directly important in the cyber warfare that are fought in close proximity with the adversary but its importance also remains intact when the person operating the cyber warfare are sitting miles away from the battlefield. This will help the respective operators to distinguish themselves so that any attack in the form of physical violence against them distinguish between civilians and the respective combatants.

The idea behind this requirement is to show explicitly who the combatants are during any operation so that unnecessary causalities to the civilian population may be warded off. The requirement of being under the responsible commandmust be fulfilled and all the cyber combatants must be under responsible command. The private hackers and individual cyber patriots etc. must not be accorded the status of combatants unless they otherwise become eligible on some other grounds, like *levee en masse*.

The phenomenon of *levee en masse* indicates the general uprising of the population to resist the invading army from their territory. This is a people's uprising to take up cyber-attacks against the adversary in order to resist its progress. Though, in its classical application, it does not contemplate any sort of military operations deep inside the enemy territory but in the context of cyber warfare, it is not reasonable to curb the effects of such cyber operations only towards the approaching army. Though some authors seem to argue for application of this concept even in cases of non-physical invasion of the territory by the enemy[34] but this should be understood in the sense of physical invasion of the enemy because this is the basic condition on which its application depends. The majority of the experts in their deliberation over Tallinn manual also support this view.[35]

Military Objectives in Cyber Warfare

Article 52(2) of the Additional Protocol Idefines the term 'military objectives' as follows:

> "[M]ilitary objectives are limited to those objects which by their nature, location,purpose or use make an effective contribution to military action and whose

[34] *Supra* note 1 at 34. The author observes "indeed in cyber warfare, territory is neither invaded nor occupied, which may significantly prolong the period during which a *levee en masse* can operate".

[35] *Supra* note 19 at 103.

> total or partial destruction, capture or neutralization, in the circumstances ruling at the time,offers a definite military advantage."[36]

This definition lays down two conditions to be complied simultaneously for categorizing any attack as directed against military objectives. First, an attacked object must effectively be contributing to the military capacity of the adversary and second, the attack must offer a definite military advantage.There must be a close nexus between potential target and military action and the definition proposed that this nexus should be established in relation to the nature, location, purpose and use of the object.

These four yardsticks are the very source of conflict in the realm of cyber warfare. Tallinn Manual Rule 39 specifically states that "an object used for both civilian and military purposes- including computers, computer networks and cyber infrastructure – is a military objective". The most of the cyber infrastructure are the so-called 'dual use' infrastructure. Both civilians and military use the cyber infrastructure simultaneously and the cyber infrastructures are largely interconnectedworld wide. This rule makes all such infrastructure as military objective because they are dual use character.

Though in traditional warfare, it is easier to classify the exact nature and use of any infrastructure at any given point of time. However, itbecomes a difficult or complex task in respect of cyber infrastructure. At any given time of cyber-attack, the millions of civilian users are also active on cyber world using the same infrastructure. This multiplies the chances of unimaginable spillover of the effects of the cyber war to the civilians.There is a potential and real danger that any part of the cyber infrastructure could be targeted.[37] Depicting a very grim and hostile situation where the whole cyber infrastructure could be turned into military objective, CordulaDroege observed:

> "In a world in which a large part of civilian infrastructure, civilian communication, finance economy, and trade rely on international cyber infrastructure it becomes all too easy for parties to conflicts to destroy this infrastructure. There is no need to argue that a banking network is used for military action, or that an electrical grid is dual use. Disabling the major cables, nodes, routers, or satellites that these systems rely on will

[36] *Supra* note 11 atart. 52(2).
[37] *Supra* note 3 at 563.

almost always be justifiable by the fact that these routes are used to transmit military information and therefore qualify as military objectives."[38]

Though, Tallinn Manual rejects such possibility by terming it 'purely theoretical at the present time' but it accepts the possibility of limited attack against certain discrete segments of cyber infrastructure.[39] Considering the possibility that a computer programmecould beinjected through one or another route, primarily it seems, as argued by Droege, that all possible routes of military information will become military objective.[40]

But such possibility must also correspond to the requirement of proportionality and precaution. However, it seems impossible to realise that any such contingency would arise where the world-wide destruction of cyber infrastructure will be justified on the ground of proportionality and precaution. Any such possibility would also seriously compromise the principle of neutrality that commands from the warring parties that there adoption of means and mechanism of warfare must not do any harm to any third country or its inhabitants that are completely neutral to that warfare.It also challenges the prohibitions imposed against indiscriminate attack. It means one can not use such methods and means of warfare that cannot be directed at a specific military objective.[41]Such possible extent of cyber warfare would also come under these prohibitions.

Despite this remote possibility that whole cyber infrastructure can become military objective, the problematic dual use characteristics of cyber infrastructure always presents potent question of determination of its exact nature. The basic question how to define accurately and precisely the military objectives in cyber realm is still evasive to any concrete answer.

V. Conclusion and Suggestions

The threat to cyber security of any country through cyber means is now a reality. This threat multiplies at the time of armed conflict for the reason that armed conflicts permit the lawful use of force against the military objectives.IHL regulates the situation of armed conflict and this paper has attempted to understand the applicability of IHL to the situations of cyber warfare.

---

38 *Id.* at 564.
39 *Supra* note 19 at 136.
40 *Supra* note 3 at 564.
41 *Supra* note 11, art. 51 (4) (b).

Cyber warfare throws many challenges like understanding about cyber-attacks, principle of distinctions and proportionality etc. There are problematic areas where one gets perplexed about how to apply the established principles of IHL to the situations of cyber warfare. These areas may briefly be mentioned as requirement from combatant to distinguish themselves, need to carry arms openly during the hostility or preparation preceding thereof, determination of proportionality and determination of military objectives etc. There are problematic areas of application but it does not mean that IHL will not apply to the situation.

IHL as *lexspecialis* will always remain applicableduring the situations of armed conflict and any attack through cyber means that have nexus with the ongoing armed conflict will always be under the gaze of IHL. Even in the challenging situations, where the application of direct provision of IHL is not ensured because of definitional and technological issues, the protection under the Martens Clause will always remain applicable. In all those conditions where the direct applicability of IHL principles are in question, the Martens clause provides the protection to the individuals as per the notions of humanity and public conscience.

However, there is also a need to further develop international legal thinking to the gray areas of application of particular IHL norms to the situation of cyber warfare. There is no doubt that emphasizing too much on established IHL conventions and treaties may result in extending them too much to a new reality that may ensue the apprehension of encrypt incoherency in such extension. Cyber warfare is definitely a warfare through new mediums, through new methods and through new instruments. It is very difficult to say that when the Geneva Conventions and the Additional Protocols were being negotiated, the realities of the cyber warfare were even envisioned.Thus, there is a need to separately look at the specific IHL issues highlighted by cyber warfare.

Tallinn Manual is an attempt in this direction, but it also does not satisfactorily answer all the relevant issues.There is also an issue whether the cyber warfarecan be conducted as per the IHL principlesat all. It means whether it is inherently possible to conduct warfare through cyber means as per the strictures of IHL principles. This line of thought is important because if there are inherent impossibilities of the precise application of IHL principles, then it is better to consider cyber warfare not as a means and methods of warfare but as a weapon that may be subjected to prohibition or regulation under specific weapons' convention, particularly a new one.This area of study is quite new and still to find its own place in the

academic discourse. The abovementioned points are some important concerns that may further affect the development of this area and thus regulate the cyber warfare in better way.