CYBER OPERATIONS DURING ARMED CONFLICTS

Author: Simran Singh, B.B.A.,LL.B(Hons.), Lawyer

ABSTRACT

There has been a rapid development of technology in the past few decades. Individuals, societies and even States have become increasingly dependent on information technology and the internet. The more the technology develops and the more we become dependent on it, the more vulnerable the civilians as well as the States are to cyber-attacks and cyber security incidents. Cyberspace has eliminated traditional geographic boundaries. States, organizations and individuals are today linked by vast, interconnected networks to disseminate information and data at a rapid rate. Everyday activities – from banking and sharing musings through blogs or email, to controlling systems and infrastructure – occur through digital networks in interconnected infrastructure. There can be terrible consequences of such cyber operations ranging from attacks on civilian transportation system like air traffic control, nuclear power plants, dams, electrical supplies and oil pipelines. Along with the extensive utilization and uptake of cyber operations, there comes a great risk to these linked systems and networks, and the data contained therein, may become the target of intentional malicious acts by States and non-State actors. Originally, the principles of International Humanitarian Law have been applied to and developed in such a way so as to be applicable in a "physical warfare" which takes place on land, sea, air or outer space but now with the rapid development of technology cyberspace has become the fifth domain of warfare. Cyber operations in the context of an armed conflict are regulated by well-established norms of IHL. Therefore, the challenge lies not in determining whether the law applies, but rather in determining how, specifically, the law applies to cyber operations.

INTRODUCTION

There has been a rapid development of technology in the past few decades. Individuals, societies and even States have become increasingly dependent on information technology and the internet. The more the technology develops and the more we become dependent on it, the more vulnerable the civilians as well as the States are to cyber-attacks and cyber security incidents. Cyberspace has eliminated traditional geographic boundaries. States, organizations

and individuals are today linked by vast, interconnected networks to disseminate information and data at a rapid rate. Everyday activities – from banking and sharing musings through blogs or email, to controlling systems and infrastructure – occur through digital networks in interconnected infrastructure. There can be terrible consequences of such cyber operations ranging from attacks on civilian transportation system like air traffic control, nuclear power plants, dams, electrical supplies and oil pipelines. Along with the extensive utilization and uptake of cyber operations, there comes a great risk to these linked systems and networks, and the data contained therein, may become the target of intentional malicious acts by States and non-State actors. Originally, the principles of International Humanitarian Law have been applied to and developed in such a way so as to be applicable in a "physical warfare" which takes place on land, sea, air or outer space but now with the rapid development of technology cyberspace has become the fifth domain of warfare. It is not surprising that cyberspace has become a new frontier for attack given the ease and global uptake of cyber connectivity.[1]Experts estimate that approximately 140 countries have developed, or are developing, a capability to wage cyber war. Some countries, like the United States, have established major military organizations focused on cyberspace and operations.[2]

Experts have widely accepted that IHL applies to cyber operations undertaken in the context of an armed conflict. Stated differently, cyber operations in the context of an armed conflict are regulated by well-established norms of IHL. Therefore, the challenge lies not in determining whether the law applies, but rather in determining how, specifically, the law applies to cyber operations. Digital means and methods of warfare executed in both the virtual and real world pose novel issues with respect to IHL.[3] Under IHL, the classification of an armed conflict is the first step in determining the rights and obligations incumbent on the parties to that conflict. IHL recognizes two types of armed conflicts: international and non-international. In an international armed conflict, the full corpus of IHL applies. By contrast, in a non-international armed conflict, a more limited portion of IHL applies. Finally, in other kinds of situations of violence which does not amount to an armed conflict, such as sporadic violence, riots, or crime, IHL just simply does not apply.

[1] Wallace & Jacobs, conflict classification and cyber operations: gaps, ambiguities and fault lines, Penn Law: Legal Scholarship Repository, 643, 647 (2019).
[2] Kevin Coleman, Coleman: The Cyber Arms Race Has Begun, CSO (Nov. 9, 2020, 8.10 P.M), http://www.csoonline.com/article/2122353/criticalinfrastructure/coleman--the-cyber-arms-race-has-begun.html. [3] Gary d. Solis, the law of armed conflict: international humanitarian law in war, 21 (2016).

APPLICATION OF IHL TO CYBER OPERATIONS DURING ARMED CONFLICTS

The modern era of classification of conflicts began in the year 1949 with the adoption of the four Geneva Conventions. Earlier treaties governing hostilities had been silent as to the conditions under which they applied. They merely assumed the existence of a 'war'. When it comes to ICRC, there is no question that arises in respect of the application of IHL to, and therefore its limitations in cyber operations during armed conflict – just as it regulates the use of any other weapon, means and methods of warfare in an armed conflict, whether new or old. This holds true whether cyberspace is considered as a new domain of warfare similar to air, land, sea and outer space; a different type of domain because it is man-made while the former is natural; or not a domain as such.[4] States adopt the IHL treaties in order to regulate the present / on-going and future conflicts. There is always a presumption that IHL will apply to any kinds of warfare and hence, States have included such rules in IHL treaties that help in anticipating the development of new means and methods of warfare. For instance, if IHL could not be applied to future means and methods of warfare, then it would not be necessary to review their lawfulness under the existing IHL, as required by Article 36 of the 1977 First Additional Protocol; this exact conclusion has found strong support in the International Court of Justice's Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons: the Court has stated that the established principles and the rules of IHL applicable during an armed conflict apply 'to all forms of warfare and to all kinds of weapons', including 'those of the future', in the view of the ICRC, this finding applies to the use of cyber operations during armed conflicts.[5] States may also decide to impose additional limits to those found in existing law and develop complementary rules, in particular in order to strengthen the protection of civilians and civilian infrastructure against the effects of cyber operation. In cases not covered by existing rules of IHL, civilians and combatants remain protected by the socalled "Martens clause", meaning they remain under the protection and authority of the principles of international law derived from established custom, from the principles of humanity and from the dictates of public conscience.[6] It is important to underline that affirming the application of IHL to cyber operations during armed conflict does not legitimize cyber warfare or encourage the militarization of cyberspace. In fact, IHL imposes certain limits to the entire militarization

[4]ICRC, International Humanitarian Law and Cyber Operations during Armed Conflicts, 2019, https://www.icrc.org/en/download/file/108983/icrc_ihl-and-cyber-operations-during-armed-conflicts.pdf.
[5]*Id.*
[6] Art. 1(2) of Protocol Additional to the Geneva Conventions of 12 August 1949, , and relating to the Protection of Victims of International Armed Conflicts (AP I); paragraph 9 of the preamble to the 1899 Hague Convention (II); paragraph 8 of the preamble to the 1907 Hague Convention (IV).

of cyberspace by prohibiting the development of military cyber capabilities that would go against and violate IHL. Moreover, any use of force by States be it cyber or kinetic, will be governed by the Charter of the United Nations and the relevant rules of customary international law, particularly the prohibition against the use of force. International disputes must be settled by peaceful means, in cyberspace as in all other domains.[7]

NOTION OF "ATTACK"

States have the obligation of determining what constitutes an "attack" under IHL. The notion of "attack" under IHL relates to its rules on the conduct of hostilities in armed conflict and is distinct from the notion of "armed attack" under Article 51 of the UN Charter. In the past, an "attack"—whether with the muskets, mortars, field artillery, or air-to-surface missiles meant only a reasonably well-understood concept in warfare. The most fundamental component of any armed conflict is death, injury, damage, and destruction which are also the consequences of attacks. Under IHL there are certain principles – principle of distinction, proportionality and precaution which are applied to those military operations that fully qualify as "attacks", which is an effort to spare the civilians from the dangers of attacks. IHL defines an attack as "acts of violence against the adversary, whether in offence or in defence." - As under Article 49(1) of Additional Protocol I. This is a seemingly clear and broad definition. But when it comes to the cyber domain, the definition of attack tends to be unclear which gives rise to unique questions around what cyber activities classify as an "attack" and, by extension, do states have to comply with IHL.

Some operations are easier to define as "attacks" than others. It is widely accepted that cyber operations that are expected to cause death, injury or any kind of physical damage are considered as attacks under IHL. In the view of ICRC, this includes any foreseeable indirect (or reoccurring) effects of death, injury, or physical damage. For example, the death of patients in intensive-care units caused by a cyber operation on an electricity network that results in cutting off a hospital's electricity supply also constitutes an attack under IHL, if that operation occurs as part of an armed conflict.[8] in an armed conflict if an operation disables a computer or a computer network either through kinetic means or cyber means will easily constitute as an attack under IHL. An overly restrictive understanding of the notion of attack

[7] *Ibid* 4.

[8] ICRC, International humanitarian law and the challenges of contemporary armed conflicts, 2015

as only referring to operations that cause death, injury or physical damage would be difficult to reconcile with the object and purpose of IHL's rules on the conduct of hostilities.[9]

INTERNATIONAL ARMED (CYBER) CONFLICT

International armed conflicts must be both 'armed' and 'international'. The first criterion presents the quandary that cyber operations are not kinetic in nature and do not employ what would in common usage be considered as 'weapons'. At a first glance, a conflict consisting of only cyber operations would, therefore, not appear to be 'armed'. Such a conclusion would be incongruous, due to the fact that cyber operations can have highly destructive, even deadly, results. A State involved in an exchange of cyber attacks at this level would be very likely to characterize the situation as international armed conflict, much as it would if it fell victim of another State's non-kinetic bacteriological attack.

A fortiori, any cyber operation that amounts to an 'attack' in the terms of IHL, would qualify as armed. Article 49(1) of Additional Protocol I defines attacks as 'acts of violence against the adversary, whether in offence or defence'. Although cyber operations are not violent in themselves, they can nonetheless generate violent consequences. The extent in which they result in injury or death of persons or damage or destruction of property, they are attacks which satisfy the armed criterion of armed conflict. For instance, if a State was behind the 2010 'Stuxnet' attack against supervisory control and data acquisition (SCADA) systems upon which the power centrifuges at an Iranian nuclear power plant depended, it would meet this threshold because physical damage resulted.[10]But is there a possibility of a cyber operation by one State against another that does not cause any physical injury or damage still initiate an armed conflict? The ICRC has taken the position that a cyber operation that 'disables' an object is also an attack even though it does not cause any sort of physical damage. This is a reasonable extension of the notion of damage, at least to the extent repair (as distinct from merely reloading software) of the cyber infrastructure concerned is necessitated. Since the operation is an attack, it is also armed in qualification for armed conflict. That said, a de minimis standard should attach. In the same way where a soldier throwing a rock across the border does not propel the States concerned into international

[9] *Id.*

[10] K Dörmann, Applicability of Additional Protocols to Computer Network Attack, ICRC, (Nov. 10, 2020, 9:10 P.M.), http://www.icrc.org/web/eng/siteeng0.nsf/htmlall/68lg92?OpenDocument

armed conflict, it would not suffice, for example, to merely disable a single computer that performs non-essential functions. Beyond this, it is unclear where State practice will lead. In a situation where one State takes control of critical infrastructure in another State, conducts denial of service attacks against essential societal services, or begins deleting or changing data in a manner that severely disrupts another State's economy. As perceptively noted by the ICRC, '[i]t would appear that the answer to these questions will probably be determined in a definite manner only through future state practice'.[11]

In addition to being armed, cyber attacks must be of an 'international' nature in order to qualify as an international armed conflict. The term international denotes actions conducted by, or attributable to, a State. By the plain text of the provisions cited above, those conducted by a State's armed forces qualify. Although not mentioned in those provisions, it is beyond dispute that cyber attacks conducted by other organs of a State, such as intelligence or law enforcement agencies, also qualify.[12] It is sometimes questioned whether attribution to a State is required at all for qualification as an international armed conflict. In the *Targeted Killing* case, the Israeli Supreme Court argued that attribution is not necessary so long as the group in question operates transnationally, that is, the conflict 'crosses the borders of the state'.[13]In the cyber context, this situation is highly probable, for organized armed groups might well launch cyber attacks from relative safety abroad. The US Supreme Court took a contrary approach in *Hamdan*, where it found that the conflict with the Al-Qaeda terrorist organization was 'not of an international character' because it was not between States.[14]

NON-INTERNATIONAL ARMED (CYBER) CONFLICT

Common Article 3 to the Geneva Conventions defines non-international armed conflicts in the negative as those that are 'not of an international character'. The ICTY has further developed the notion of non-international conflict. The equivalent definition has been adopted by international tribunals and in the Statute of the International Criminal Court. Additional Protocol II also refers to a conflict between a State's armed forces 'and dissident armed forces or other organized armed groups'. Accordingly, two essential criteria

[11]Michael Schmitt, Classification of Cyber Conflict, Journal of Conflict and Security Law, 245, 260, 2012.
[12]*Ibid.*
[13]Public Committee against Torture in Israel *(n 3)* para 18.
[14]Hamdan v Rumsfeld (n 3) 2795–96.

apply for all non-international armed conflicts—participation by an organized armed group and a particular level of intensity.

Organized armed groups must be both 'organized' and 'armed'. Common Article 3 refers to 'parties to a conflict', a reference that serves as the source of the organization requirement. In considering this requirement, the ICTY has noted 'some degree of organisation by the parties will suffice to establish the existence of an armed conflict. This degree need not be the same as that required for establishing the responsibility of superiors for the acts of their subordinates within the organization, as no determination of individual criminal responsibility is intended under this provision of the Statute'. But the group must nevertheless be organized. Organization allows for acting in a coordinated manner, thereby generally heightening the capability to engage in violence. In military operations, such coordination typically involves mission planning, sharing intelligence and exercising control and command. In other words, the organizational criteria implies that the actions are best understood as those of a group and not its individual members. This structural requirement is fundamental, for structures that are absent, there is no identifiable enemy to treat as the other party to the conflict.[15] In contradistinction to international armed conflict, non-international armed conflict entails a certain degree of intensity. Riots, civil disturbances or isolated and sporadic acts of violence do not suffice; the hostilities must also be protracted. However, no bright-line intensity test exists, nor is there any clear standard for 'protracted' conflict. In the manner in which cyber campaigns are mounted, though cyber-attacks have to be frequent enough to be considered as related, they clearly need not have to be continuous. This is a high threshold that would preclude many cyber operations from sufficing the purpose of a non-international armed conflict. Even highly destructive cyber attacks would fail to qualify unless they occurred on a regular basis over time. They would instead be addressed within the criminal law paradigm and be governed internationally by human rights, not humanitarian, law.[16]

The ICRC's Interpretive Guidance on the Notion of Direct Participation in Hostilities addresses such situations; it contends that "organized armed groups operating within the broader context of an international armed conflict without belonging to a party to that conflict could still be regarded as parties to a separate non-international armed conflict". Some

[15]Prosecutor v Limaj (Judgment) ICTY-03-66-T (30 November 2005) para 89
[16]Prosecutor v Haradinaj (Judgment) ICTY-04-84-T (3 April 2008)

participants in the expert process that resulted in the Guidance rejected the ICRC's position on the basis that it would prove problematic in practice because it requires application of the law of both international and of non-international armed conflict in the same battlespace; in their view, it was more appropriate to ask whether an unambiguous nexus existed between the actions of the group in question and the international armed conflict, rather than any party thereto.[17] For instance, an organized armed group might conduct cyber attacks against an occupying force because of religious or political opposition to the occupants, not to expel them on behalf of the government. The requisite nexus between the group and the conflict would be their opposition to the occupation. In such a case, the conflict would remain entirely international irrespective of the lack of a relationship between the group and the occupied State. Additional Protocol II only applies when organized armed groups control territory. Since a group cannot control territory without physical presence, the instrument is generally thought to be inapplicable to cyber-only conflicts. It would accordingly only apply to cyber operations in those Additional Protocol II conflicts involving an organized armed group that controls territory and conducts such operations.

CONCLUSION

States have refrained from characterizing any cyber operations conducted outside the context of an on-going armed conflict as either international or non-international armed conflict. Be that as it may, cyber operations will in the future inevitably present difficult conflict classification challenges for States. With regard to international armed conflict, attribution of cyber operations conducted by non-State actors will likely prove even more problematic than the attribution to States of kinetic actions has been in the past. In the context of non-international armed conflict, qualification as an organized armed group will prove increasingly complex as the structures, means and prevalence of virtual organization grow and evolve. Perhaps most importantly, the approach taken in this article to the interpretation of the term 'armed' is, although presently reflecting *lexlata*, unlikely to survive. With States and non-State actors engaging in ever more destructive and disruptive cyber operations and societies becoming deeply dependent on the cyber infrastructure, State practice accompanied

[17] N Melzer, Interpretive Guidance on the Notion of Direct Participation under International Humanitarian Law (ICRC 2009) 24.

by *opiniojuris* can be expected to result in a lowering of the current threshold. The law of cyber-armed conflict is a work in progress and will remain so for the immediate future.