Open-ended Working Group on security of and in the use of information and communications technologies

Application of international humanitarian law to the use of information and communication technologies in situations of armed conflicts

Working Paper submitted by Brazil, Canada, Chile, Colombia, the Czech Republic, Estonia, Germany, the Netherlands, Mexico, the Republic of Korea, Senegal, Sweden and Switzerland

1 March 2024

1. Introduction

A growing number of States and non-State armed groups are developing Information and Communications Technologies (ICT) capabilities for military purposes. The use of ICTs in times of armed conflict has recently seen a significant increase. This development raises concerns as to the implementation of International Humanitarian Law (IHL) in such circumstances, and therefore calls for further discussions on how to concretely apply IHL to the use of ICTs in situations of armed conflicts.[1]

The Annual Progress Report (APR) 2023 recommended to "continue to engage in focused discussions at the OEWG on how international law applies in the use of ICTs drawing from topics from the non-exhaustive list" that included the "need for further study on how and when" the principles of international humanitarian law apply.[2]

We share the view that States need to engage in discussions on how IHL applies to ICT operations in situations of armed conflict, acknowledging the particularities of the digital domain. This will help to develop common understandings on how we can best protect civilians and civilian objects, as well as what actions are prohibited or required during armed conflicts.[3]

This Working Paper aims to contribute to such discussions as well as capacity-building initiatives, while recognizing that a number of aspects remain to be clarified and that a continued intergovernmental exchange at the multilateral level remains key in this regard.

2. Applicability of IHL

IHL applies to cyber operations executed in the context of and in relation to an international or non-international armed conflict.

IHL addresses the realities of armed conflicts without considering the reasons for or the legality of the recourse to the use of force. Applying IHL does not encourage or legitimise in any way the possible recourse to the use of force between States, in any situation or context, including in cyberspace.

As the International Court of Justice stated, the intrinsically humanitarian character of the established principles and rules of IHL "permeates the entire law of armed conflict and applies to all forms of warfare and to all kinds of weapons, those of the past, those of the present and those of the future".[4] This is notably the case as the purpose of IHL is to regulate the conduct of hostilities and to protect those who

[1] Statement delivered by Switzerland on behalf of a group of States on IHL 2022 (JST 2022); 2023 Report of the open-ended working group on security of and in the use of information and communications technologies 2021–2025 (APR 2023) §11; ICRC short paper (2023) When does international humanitarian law apply to the use of information and communications technologies? (ICRC Paper #1).

[2] APR 2023, §33; 2022 Report of the open-ended working group on security of and in the use of information and communications technologies 2021–2025 (APR 2022) §15(b)(ii).

[3] JST 2022.

[4] ICJ, Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion of 8 July 1996, §86.

are not, or no longer, taking part in hostilities, such as civilians or the wounded and sick, in particular by restricting the use of certain means and methods of warfare. IHL reduces risks and potential harm to both civilians and civilian objects as well as combatants in the context of an armed conflict.

This applies to cyber operations in the same way as for other forms of warfare. Existing IHL applies to and places important limits on cyber operations in the context of an armed conflict, particularly its fundamental principles of humanity necessity, proportionality and distinction.[5]

While in many cases it is clear how IHL applies to cyber operations in the context of an armed conflict, a number of issues remain to be clarified. This Working Paper serves as an opportunity to further discuss these issues.

3. Principles and rules of IHL governing the use of information and communications technologies during armed conflicts

3.1. Principles of military necessity and humanity[6]

The principles of military necessity and humanity underlie the whole body of IHL and find expression in other rules and principles, such as the principles of distinction, proportionality and precaution.

The principle of military necessity requires that only measures which are actually necessary to achieve a legitimate military purpose and which are not otherwise prohibited by IHL are taken. The only legitimate military purpose is to "weaken the military forces of the enemy".[7]

The principle of humanity seeks to limit and alleviate the suffering and destruction during armed conflicts. It aims to protect property as well as life and health of the population.[8]

A fundamental concern of IHL is to ensure that a balance is struck between military necessity and humanitarian considerations. Accordingly, military operations must be justified by military necessity and respect the principle of humanity. Unless specific rules or principles explicitly provide an exception, military necessity can never be cited as a reason for disregarding other rules and principles of IHL. A military advantage may not be sought by prohibited means.

This also applies to cyber operations during an armed conflict. Even if no specific rule of IHL governs a specific cyber operation, it must nevertheless respect both principles of military necessity and humanity. Moreover, in accordance with the Martens clause, in cases not covered by relevant IHL conventions or by other international agreements, the civilian population and combatants 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.[9]

3.2. Fundamental IHL rules and principles regulating the conduct of hostilities in or through cyberspace

IHL notably regulates the use of means and methods of warfare through general rules and principles – regulating conduct or prohibiting certain effects – which also apply to cyber capabilities. In cyberspace, as in any other domain, the right of parties to an armed conflict to choose methods or means of warfare is not unlimited.[10] Many of the rules and principles governing the conduct of hostilities are applicable in particular to cyber operations that amount to an attack within the meaning of IHL, i.e. acts of violence

---

[5] See Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, 2021, A/76/135, para 71(f), consensus GA resolution 76/19, noting that international humanitarian law applies only in situations of armed conflict and recalling the established international legal principles including, where applicable, the principles of humanity, necessity, proportionality and distinction that were noted in the 2015 report.

[6] 1868 St. Petersburg Declaration; 1907 Hague Regulation, Preamble; Martens Clause.

[7] 1868 St. Petersburg Declaration.

[8] 1868 St. Petersburg Declaration.

[9] Martens Clause; 1907 Hague Convention, preamble; 1977 Additional Protocol I (AP I), Art. 1.

[10] 1907 Hague Regulations, Art. 22; AP I, Art. 35.

against the adversary, whether in offence or defence. This encompasses at the very least cyber operations that are reasonably expected to cause, directly or indirectly, injury or death to persons, or physical damage or destruction to objects. However, the circumstances in which a loss of functionality could be considered an attack in the sense of IHL need to be further clarified, including thus discussions regarding the definition of a "cyber attack" in the sense of IHL. In a similar vein, the protection of civilian data and questions regarding cyber operations disrupting systems without causing physical harm – but nevertheless with potentially wide-ranging effects – remain challenges that require further clarification.

IHL considers some means and methods of warfare as inherently unlawful, notably if they:

- are of a nature to cause superfluous injury or unnecessary suffering;[11]
- cannot be directed at a specific military objective or limited in their effects as required by IHL and consequently are of a nature to strike military objectives and civilians or civilian objects without distinction;[12]
- are intended, or may be expected, to cause widespread, long-term and severe damage to the natural environment;[13] or
- are otherwise specifically prohibited by applicable treaty or customary international law.

The use of such means and methods of warfare is unlawful regardless of the manner in which they are employed. This also applies to cyber means and methods of warfare.

In addition to the principles of military necessity and humanity, in particular the principles of distinction, proportionality and precautions govern the conduct of hostilities and are also of fundamental importance when cyber means and methods of warfare are employed.

a) Distinction

The principle of distinction is one of the cornerstones of IHL and applies also to cyber attacks. The parties to the conflict shall direct their military operations only against military objectives. Thus, they must distinguish at all times between civilians and combatants, as well as between civilian objects and military objectives.[14] Cyber attacks may only be directed against combatants or military objectives. With regard to objects, "military objectives are limited to those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage".[15] In case of doubt civilian status must be presumed.[16] For the application of IHL in cyberspace, a challenge may arise from the fact that ICT infrastructure may be used for both civilian and military purposes. Military use can, in certain cases, render such an object into a military objective. In such cases, the above-mentioned criteria must be fulfilled and any attack would need to comply with all other relevant rules of IHL, in particular those relating to the principles of proportionality and precaution.

Indiscriminate cyber attacks are prohibited. This includes cyber attacks that are not directed at a specific military objective, that employ a method or means of combat which cannot be directed at a specific military objective; or those that employ a method or means of combat the effects of which cannot be limited as required by IHL.[17]

b) Proportionality

The principle of proportionality requires that parties, when attacking military objectives, evaluate whether an attack may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof which would be excessive in relation to the concrete and direct military advantage anticipated, and refrain from such prohibited attacks.[18]

---

[11] AP I, Arts. 35; CIHL Rule 70.
[12] AP I, Arts 51(4)(b) and (c); CIHL Rule 71.
[13] AP I, Arts. 35; CIHL Rule 45.
[14] It is to be noted that civilians are protected against attack, unless and for such time as they take a direct part in hostilities and that civilian objects are protected against attack, unless and for such time as they are military objectives. Attacking persons who are recognized as *hors de combat* is prohibited.
[15] AP I, Arts. 48, 51, 52; ICRC Study on Customary IHL (CIHL), Rules 1 and 7.
[16] AP I, Arts. 50, 52; CIHL Rules 6 and 10.
[17] AP I 51(4)(a)-(c); CIHL Rules 11 and 12.
[18] AP I, Art. 51(5)(b); CIHL Rule 14.

c) Precaution

The principle of precaution requires that parties take constant care in the conduct of military operations to spare the civilian population, civilians and civilian objects and take all feasible precautions in attack to avoid, and in any event to minimize, incidental loss of civilian life, injury to civilians and damage to civilian objects.[19] Precautionary measures apply to all phases of a military cyber operation, from its planning to the decision to go ahead with the operation, as well as during its execution, and must be taken independently of the question of proportionality. The obligation to take steps to avoid and in any event minimize incidental harm, as described, applies regardless of whether the expected incidental harm would otherwise be excessive in relation to the anticipated military advantage. In this sense, the risk of the harmful effects of cyber operations spreading or the potential damage that could be caused beyond the targeted objective must be assessed with a degree of reasonable foreseeability. In addition, those who plan or decide upon a cyber attack shall do everything feasible to verify that the objectives to be attacked are neither civilians nor civilian objects and are not subject to special protection but are military objectives and that it is not prohibited by IHL to attack them.[20]

3.3. Additional key rules and principles of IHL

Compliance with IHL when conducting cyber operations is not limited to the rules and principles governing the conduct of hostilities. Other specific rules and principles of IHL must be respected, including when conducting cyber operations that would not qualify as an “attack”. All of the relevant and applicable IHL obligations must be respected when resorting to cyber operations.

In particular, certain additional rules apply when cyber operations affect specially protected persons or objects, or other activities governed by IHL. Examples include medical, religious or humanitarian personnel and objects, which must be respected and protected in all circumstances.[21]

4. Measures to ensure respect for IHL

States and parties to an armed conflict must take measures to implement IHL, give orders and instructions to ensure observance of IHL and supervise their execution. Such measures are also important in relation to cyber operations that are conducted in the context of an armed conflict.[22]

Knowledge of the content of IHL, notably also by cyber operators, is an important measure to ensure compliance and to protect victims of armed conflict, such as the wounded and sick, and civilian infrastructure.

States and parties to a conflict are required, inter alia, to take measures to ensure that the development and use of means and methods of warfare fully comply with IHL. In accordance with their obligations under international law, States must determine, in the study, development, acquisition or adoption of a new weapon, means or method of warfare, whether its employment would, in some or all circumstances, be prohibited by international law applicable to them.[23]

While the legal review of cyber means and methods of warfare is important, the legal assessment of concrete or specific cyber operations is also relevant. This can include, for instance, to ensure that legal advisers are available when evaluating cyber operations.[24]

---

[19] AP I, Art. 57; CIHL Rule 15.

[20] AP I 57(2)(a)(ii); CIHL Rule 16.

[21] With regard to medical personnel and objects see GC I Art. 19, 24, 25, 35, 36; GC II Art. 22, 24, 25, 27, 36 – 39; GC III Art. 33; GC IV Art. 18 – 22; AP I Art. 8(d), 12, 15, 21 – 24, 26; AP II Art. 9; CIHL Rules 25, 27 – 30. With regard to humanitarian personnel and objects see GC IV Art. 23, Art. 59 - Art. 62; AP I Art. 70; CIHL 31, 32 and 55.

[22] GC I-IV, Art. 1, GC I, Art. 47, GC II, Art. 48, GC III, Art. 127, GC IV, Art.144; AP I, Arts. 1, 36, 80,83; CIHL Rules 139, 142, 143.

[23] GC I-IV, Art. 1, GC I, Art. 47, GC II, Art. 48, GC III, Art 127, GC IV, Art 144; AP I, Arts. 1, 36.

[24] AP I, Art. 82; CIHL Rule 141.