

REGIONAL CONSULTATION OF LATIN AMERICAN STATES

9–10 NOVEMBER 2021

**INTERNATIONAL HUMANITARIAN LAW
AND CYBER OPERATIONS DURING
ARMED CONFLICTS**



RELACIONES EXTERIORES
SECRETARÍA DE RELACIONES EXTERIORES



ICRC

REGIONAL CONSULTATION OF LATIN AMERICAN STATES

9–10 NOVEMBER 2021

INTERNATIONAL HUMANITARIAN LAW AND CYBER OPERATIONS DURING ARMED CONFLICTS

Report prepared by Kubo Mačák, Legal Adviser, ICRC.

Citation: ICRC, *Regional Consultation of Latin American States, 9–10 November 2021, International Humanitarian Law and Cyber Operations During Armed Conflicts*, ICRC, Geneva, June 2022.

CONTENTS

Executive summary3

Introduction..... 4

Session 1: Technical overview of cyber operations during armed conflicts 4

Session 2: Applicability of IHL to cyber operations during armed conflicts.....5

Session 3: Cyber operations and the notion of ‘attack’ under IHL..... 6

Session 4: The protection afforded to civilian electronic data under IHL7

Session 5: The military use of cyberspace and the effect on its civilian character8

Session 6: Limits on the conduct of information or psychological operations during
armed conflicts 10

Session 7: National positions.....11

Session 8: Multilateral engagement 13

Annex 1: List of participating states 15

Annex 2: Background paper..... 16

Annex 3: Scenarios for discussion26

Annex 4: Agenda29

EXECUTIVE SUMMARY

The government of Mexico and the International Committee of the Red Cross (ICRC) jointly organized – on 9 and 10 November 2021 – a regional consultation of Latin American states on international humanitarian law (IHL) and cyber operations during armed conflicts. The aim of the event was to facilitate dialogue among states in the region, with a view to developing common understandings on how international law applies to the use of information and communication technologies during armed conflicts. These are the main takeaways from the event:

IHL LAYS DOWN LIMITS FOR CYBER OPERATIONS DURING ARMED CONFLICTS AND SHOULD BE INTERPRETED IN LIGHT OF THE EVOLVING TECHNOLOGIES OF WARFARE

- There was a general consensus among participating states that IHL applies to cyber operations during armed conflicts. Participants underscored that recalling IHL applicability by no means legitimizes or encourages conflict.
- Because malicious cyber operations may result in devastating humanitarian consequences, states should be prudent in developing legal interpretations, in order not to reduce the protections available under the law.
- The meaning of legal terms is not static. These terms have to be reinterpreted constantly in order for the law to remain effective. In particular, the interpretation of generic legal terms should be done in light of evolving circumstances, such as the digitalization of societies and the development of new means and methods of warfare.

CLARIFICATION OF KEY IHL NOTIONS IS NEEDED

- States should develop their legal views in order to clarify the notion of ‘attack’ under IHL in the cyber context. In particular, clarity is needed on the duration and nature of the loss of functionality that a cyber operation must cause to qualify as an attack.
- When considering incidental civilian harm resulting from cyber operations that qualify as attacks under IHL, all direct and indirect harm needs to be taken into account, including the loss of civilian data caused by those operations.
- Cyber operations against civilian data may bring about serious consequences for civilians, which should be addressed by IHL. States should prevent the creation of legal loopholes that might seem to permit cyber operations that cause such consequences.
- More clarity is needed on the legal implications of the use of cyberspace for military purposes, given the predominantly civilian character of cyberspace.
- Information operations may bring about serious humanitarian consequences and thus deserve close attention. If conducted during an armed conflict and with a nexus to that conflict, information operations must comply with the applicable rules of IHL.

SUGGESTIONS FOR THE WAY FORWARD

- States should be encouraged to develop national positions on the application of international law in cyberspace. Such positions are complementary to ongoing multilateral processes, and enable more focused discussions on how exactly international law, including IHL, applies in the cyber context.
- All states should take part in multilateral processes – such as the new UN-mandated open-ended working group (OEWG) on “security of and in the use of information and communications technologies” – in order to contribute to and maintain those processes’ transparency and inclusivity.

INTRODUCTION

The government of Mexico and the International Committee of the Red Cross (ICRC) jointly organized – on 9 and 10 November 2021 – a regional consultation of Latin American states on international humanitarian law (IHL) and cyber operations during armed conflicts. The aim of the event was to facilitate dialogue among Latin American states on IHL and cyber operations, with a view to developing common understandings on how international law applies to the use of information and communication technologies (ICTs) during armed conflicts.

The objective of this report is to provide an account of the exchanges among experts that took place during the consultation. The report does not purport to reflect the positions of either the government of Mexico or the ICRC on these issues. While the various points made in the discussion summarized here are not attributed to the participants who made them, a list of participating states is provided (Annex 1). An earlier draft of the present report was submitted to participants for comments.

The report also includes a detailed background paper and a set of hypothetical scenarios, which were prepared by the organizers and used to inform the discussions (Annexes 2–3) and the agenda of the meeting (Annex 4).

SESSION 1: TECHNICAL OVERVIEW OF CYBER OPERATIONS DURING ARMED CONFLICTS

Moderator: Salvador Tinajero Esquivel, Coordinator of Public International Law, Ministry of Foreign Affairs of Mexico

Expert presentation: Mauro Vignati, Adviser on Digital Technologies of Warfare, ICRC

The framing presentation discussed the technical aspects of cyber operations during armed conflicts. In this respect, military cyber operations can be broken down into two main types.

Event-based operations, which include all instances in which the target is directly and in real time attacked by compromising its software/infrastructure. For example, a distributed denial of service (DDoS) attack is an event-based operation without network access, in which the attacker weaponizes a botnet – i.e. a series of infected computers – to bring down a web server, and thus disrupt the services that server provides. There are also event-based operations with network access, such as deployment of ransomware, which have been used to freeze critical civilian infrastructure.

Presence-based operations, which include all network intrusions, in which the attackers trawl compromised networks until targets are located, assessed, and weaponized for later activation. Examples include operations that merely extract information from the target network, but also more complex disruptive operations, such as the use of so-called ‘wipers’. Presence-based operations have been used to attack energy facilities and have led to power outages in countries affected by armed conflicts.

The ICRC is also engaged in the search for concrete technical measures to operationalize in cyberspace the protection afforded by IHL. In particular, it is currently leading a project on the **digital emblem** that aims to examine technical ways to digitally identify infrastructure and data belonging to especially protected entities that are entitled to use the distinctive emblems (i.e. the red cross, red crescent and red crystal) in the physical world.¹

¹ For more information, see Tilman Rodenhäuser *et al*, ‘[Signaling legal protection in a digitalizing world: a new era for the distinctive emblems?](#)’ *Humanitarian Law & Policy Blog*, 16 September 2021.

It was noted that cyber operations represented an innovative and effective form of hybrid warfare, the use of which allows states and other actors to deny their involvement in belligerent conduct. The need for effective tools to trace such operations back to their source was underscored by participants (the so-called ‘**attribution problem**’).

SESSION 2: APPLICABILITY OF IHL TO CYBER OPERATIONS DURING ARMED CONFLICTS

Moderator: Oscar Macías, Legal Adviser, Ministry of Foreign Affairs of Mexico

Expert presentation: Kubo Mačák, Legal Adviser, ICRC

The starting point of the framing presentation² was that although the **applicability of international law** in general has been the subject of a general consensus since at least 2013³ – and reaffirmed in the Organization of American States (OAS) context by the OAS’s General Assembly in 2020⁴ – there have also been some debates over whether and to what degree this consensus also extends to IHL.

It is also important to distinguish the **two main aspects of the applicability of IHL**: one relates to the question whether IHL governs cyber operations that complement existing kinetic or physical military operations during ongoing armed conflicts, and the other to the question whether cyber operations by themselves – without kinetic operations – can be regulated by IHL.

Finally, the question of IHL’s applicability is at times linked to **concerns about the militarization of cyberspace or about the legitimization of cyber warfare**. However, for many states – and also for the ICRC – affirming the applicability of IHL does not legitimize cyber warfare, just as it does not legitimize any other form of warfare. In fact, IHL imposes important limitations on the militarization of cyberspace.⁵

All the participants who took the floor during the discussion affirmed the view that **IHL applies to cyber operations during armed conflict**. It was noted that a 2021 consensus report of the UN Group of Governmental Experts (GGE) – in a historical first for UN-based processes – expressly referred to IHL in the cyber context.⁶ It was also noted that accepting the applicability of IHL to cyber operations in armed conflicts does not make cyber operations more legitimate, and that IHL provides humanitarian protection for civilians and protects critical civilian infrastructure.

Establishing the origins of a cyber operation is often difficult (the so-called ‘**attribution problem**’), which may have implications for the applicable body of law. For example, if the author of a cyber operation is unknown, that may impede the ability of the targeted state to establish a link between that operation and an ongoing armed conflict, and thus to determine whether IHL would apply to any response that the state might consider.

² For more information, see section 3 of the background document (Annex 2).

³ UN General Assembly, ‘Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security’, UN Doc. A/68/98, 24 June 2013, para. 19; UN General Assembly, ‘Developments in the field of information and telecommunications in the context of international security’, UN Doc. A/RES/68/243, 27 December 2013.

⁴ OAS, ‘International Law’, AG/RES. 2959 (L–O/20), 21 October 2020.

⁵ See ICRC, ‘International Humanitarian Law and Cyber Operations during Armed Conflicts – ICRC position paper’, November 2019, pp. 4–5.

⁶ UN General Assembly, ‘Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security’, UN Doc. A/76/135, 14 July 2021, para. 71(f).

Moreover, the question was raised whether the **development of cyber weapons** that would be illegal under IHL could be prevented beforehand, in peacetime. It was noted in this regard that the obligation to conduct legal reviews of new means and methods of warfare applied in peacetime.⁷ When states study, develop, or adopt new means/methods of warfare, they need to assess whether these means/methods can be used in a lawful manner.

This obligation applies equally to cyber weapons, means and methods of warfare – setting aside, for the moment, the question whether cyber capabilities qualify as weapons. Weapons that would be unlawful in all circumstances must not be developed in the first place. The development of cyber tools that would, for example, self-propagate, and cause harm indiscriminately to military and civilian objects, is prohibited.

Finally, the discussion turned to the applicability of international law following the **first use of cyber capabilities by states for hostile purposes**. In this regard, distinction must be made between two relevant branches of international law. Under the law on the use of force (*jus ad bellum*), if the cyber operation qualifies as an armed attack, the victim state may respond by using force in self-defence;⁸ but if it does not reach that level, the victim state may resort only to non-forcible proportionate countermeasures.⁹

The question of the applicability of IHL (*jus in bello*) is distinct and must be assessed under that body of law. If the effect of the operation is equivalent to a classic kinetic operation, it is generally accepted among experts that it would amount to an international armed conflict. Therefore, that first operation and the response by the victim state would have to comply with IHL, regardless of their legality under *jus ad bellum*.

SESSION 3: CYBER OPERATIONS AND THE NOTION OF ‘ATTACK’ UNDER IHL

Moderator: Daniel Cahen, Head of the Legal Department for Mexico and Central America, ICRC

Expert presentation: Kubo Mačák, Legal Adviser, ICRC

The framing presentation¹⁰ noted that the **definition of ‘attack’** is of central importance for the application of IHL because most rules on the conduct of hostilities apply only to attacks. It is widely accepted that in the cyber context, the notion of ‘attack’ includes cyber operations that may be expected to cause death or injury to persons, or destruction or damage to objects. However, views are divided on whether operations that lead to a **loss of functionality** of the target system amount to an attack under IHL.

Some states take the narrower view that only operations that cause **death, injury, or physical damage** can be considered an attack. Others – and the ICRC as well – are of the opinion that cyber operations that **disable their targets** also constitute an attack, irrespective of whether the object is disabled through physical destruction or in some other way. The difference between these views also underscores the importance of understanding which protections IHL affords with respect to those **cyber operations that do not qualify as ‘attacks’**.

⁷ Art. 36 of the 1977 First Additional Protocol.

⁸ Art. 51 of the 1945 United Nations Charter.

⁹ Arts 50–53 of the 2001 International Law Commission’s Articles on Responsibility of States for Internationally Wrongful Acts.

¹⁰ For more information, see section 4.1 of the background document (Annex 2).

During the discussion, it was noted that although peaceful uses of technology have many benefits, the use of advanced technology may also have **devastating humanitarian consequences**. This includes the use of cyber operations for military purposes, particularly if they affect critical civilian infrastructure. Examples that are particularly concerning include cyber operations affecting the health and financial sectors.

Against that background, it is **important to clarify the notion of ‘attack’ in the cyber context**. The risk that the use of cyber capabilities may have grave humanitarian consequences necessitates prudence in developing interpretations that may affect the scope of the protection available under the law. It was noted that the “most appalling” cyber operations would be prohibited under the relevant rules, irrespective of whether they would qualify as ‘attacks’ or not. For instance, cyber operations targeting hospitals during armed conflicts are prohibited by the IHL obligation to respect and protect medical facilities.

The related concept of **loss of functionality** needs additional attention. There is a spectrum of views on the type of effects that a cyber operation might have, in terms of loss of functionality, for it to be regarded as an attack. Some consider that it would have to cause systems to stop functioning permanently; others include operations that make such systems operate improperly until they are repaired; and yet others consider that merely slowing systems down suffices for an operation to qualify as an ‘attack’.

It was suggested that it would be useful to have **specific scenarios** – such as those in the annex to the background document – that would further illustrate the spectrum of the various forms of loss of functionality. It was noted in response that the Cyber Law Toolkit project (co-led by the ICRC) provides such scenarios concerning a range of legal issues.¹¹ These include the question of the classification of military cyber operations as ‘attacks’ under IHL, and other aspects of the application of IHL in the cyber context.¹²

SESSION 4: THE PROTECTION AFFORDED TO CIVILIAN ELECTRONIC DATA UNDER IHL

Moderator: Kubo Mačák, Legal Adviser, ICRC

Expert presentation: Romina Soledad Morello, Regional Legal Adviser, ICRC

The starting point of the framing presentation¹³ was that IHL prohibits direct attacks on civilian objects. A **key question was whether electronic data qualified as ‘objects’**; if they did not, the prohibition would not apply to cyber operations targeting civilian data. This issue can be illustrated by a practical scenario.¹⁴ In this scenario, state A conducts a cyber operation against digital civilian records concerning social benefits and taxation held by state B. The operation results in the deletion of all of this data.

States have taken a **variety of views** on this issue. Some do not regard data as an object under IHL. Other states are of the opinion that the protection of civilian objects does extend to civilian data. There is also a middle view, which considers only civilian content data (as opposed to operational data) to be protected by these rules. When applied to the scenario, under the first view, the illustrative operation would not be covered by the prohibition against direct attacks on civilian objects. However, under the two other views, it would be regarded as a violation of that prohibition. While the law remains unsettled, the ICRC takes the position that when paper files and documents are replaced by digital files in the form of data, that should not decrease the protection that IHL affords them.¹⁵

¹¹ See [Cyber Law Toolkit](#).

¹² See *ibid.*, ‘[Category: International humanitarian law](#)’.

¹³ For more information, see section 4.2 of the background document (Annex 2).

¹⁴ For the full scenario, see Annex 3, scenario 2.

¹⁵ See ICRC, ‘International Humanitarian Law and Cyber Operations during Armed Conflicts – ICRC position paper’, November 2019, p. 8.

During the discussion, most participants took the view that **the hypothetical cyber operation would be prohibited by IHL**, but it was noted that the specific legal reasons for arriving at that conclusion may differ. An overarching concern shared during the meeting was that cyber operations did not occur in a legal vacuum, and that states should therefore prevent the creation of legal loopholes that would seem to permit cyber operations with significant humanitarian consequences. It was noted that cyber operations against civilian data may indeed lead to serious consequences for civilians, which should thus be considered akin to physical harm.

There was also broad agreement that **the interpretation of generic legal terms – like the word ‘object’ – should be done in light of evolving circumstances**, an approach supported by international jurisprudence.¹⁶ It was underscored that because this was a constantly evolving area of state interaction, states’ positions also continued, and will continue, to evolve. In other words, the meaning of legal terms is not conserved in time and needs to be constantly reinterpreted in order for the law to remain effective.

In addition, it was highlighted that in many **domestic jurisdictions in Latin America**, electronic data are considered to be a legal object despite their not being tangible in nature. Moreover, the equally authentic Spanish version of the relevant IHL rules uses the term ‘bienes’, the meaning of which is closer to ‘goods’ or ‘property’, which may exist in both tangible and intangible forms. Reflecting these regional perspectives may provide further support to the view according to which data qualify as an object under IHL.

Some attention was also given to **the ‘middle’ position, according to which only content data – but not operational data – are subject to protection under the principle of distinction**. It was queried whether civilian operational data would be sufficiently protected under this view. It was noted in this regard that tampering with operational data would necessarily affect the functionality of the device or system concerned. Accordingly, if one took the broader view on the notion of attack (see above), then at least certain cyber operations that affected operational data in civilian devices or systems would be covered by the prohibition of direct attacks on civilian objects. This issue highlighted how the questions discussed in the individual sessions were interconnected.

SESSION 5: THE MILITARY USE OF CYBERSPACE AND THE EFFECT ON ITS CIVILIAN CHARACTER

Moderator: Salvador Tinajero Esquivel, Coordinator of Public International Law, Ministry of Foreign Affairs of Mexico

Expert presentation: Laurent Gisel, Head of the Arms and Conduct of Hostilities Unit, ICRC

In the framing presentation,¹⁷ it was noted that it was traditionally understood that a civilian object that was used simultaneously for both civilian and military purposes may become a military objective when its use for military purposes was such that it fulfilled the definition of a military objective (such objects are sometimes referred to as **‘dual-use objects’**). A wide interpretation of this rule in the cyber context could lead to the conclusion that many objects forming part of cyberspace infrastructure would constitute military objectives and would therefore not be protected against attack, whether cyber or kinetic. This would be a matter of serious concern because of the ever-increasing civilian reliance on cyberspace.

IHL contains several important safeguards in this regard. To begin with, **the analysis of when a civilian object becomes a military objective cannot be done for cyberspace in general**. Instead, belligerents must identify which computers, nodes, routers or networks might have become military objectives. In this respect,

¹⁶ See ICJ, *Legal Consequences for States of the Continued Presence of South Africa in Namibia (South West Africa) notwithstanding Security Council Resolution 276 (1970)*, Advisory Opinion, 1971, para. 53; ICJ, *Dispute regarding Navigational and Related Rights (Costa Rica v Nicaragua)*, Judgment, 2009, para. 66.

¹⁷ For more information, see section 4.3 of the background document (Annex 2).

parts of the network, specific computers, or other hardware that can be separated from a network or system as a whole need to be analysed individually. The means and methods used must enable directing the attack at the specific military objective, and all feasible precautions must be taken to avoid or at least minimize incidental harm to the remaining civilian objects or parts of the network.

Moreover, **cyberspace is designed with a high level of redundancy**, which means that one of its characteristics is the ability to immediately re-route data traffic. This inbuilt resilience needs to be considered when assessing whether the target's destruction or neutralization would offer a definite military advantage, as required by the definition of 'military objective'. If this is not the case, the object will remain civilian and cannot be attacked. In addition, all attacks are governed by the prohibition against indiscriminate attacks and the rules of proportionality and precautions in attack. Stopping or impairing the civilian use of an object in violation of one of these rules would render the attack unlawful despite the fact that the object had become a military objective.

The discussion revolved around **a hypothetical scenario** during an international armed conflict.¹⁸ In the scenario, one state engaged in the conflict is using several servers located in a large commercial data centre on its own territory. The servers in question are used only for military purposes by that state; however, the data centre also contains many other servers used exclusively by civilians. The enemy state launches a cyber operation that shuts down the entire data centre's cooling system, thus overheating and damaging all the servers within it.

The facts of the scenario raised two separate legal questions. First, **at what level must the attacking state assess whether the target of its operation has become a military objective?** A number of participants took the view that the state may target only the servers used for military purposes. It was agreed during the discussion that this would be the most protective interpretation. However, some participants took the position that if it was not feasible technically to target only the military servers, then the attack may also be directed at the cooling system at the data centre. The reasoning behind this view was that the cooling system was also an object used for military purposes – i.e. to keep the military servers operational – and thus possibly qualified as a military objective on its own.

Second, **what needs to be considered in terms of incidental civilian harm in relation to the principle of proportionality?** None of the participants considered that the assessment would be limited only to direct physical damage (such as fire damage caused by the cooling-system malfunction). Rather, it was noted that all direct and indirect harm would have to be considered, including the loss of civilian data caused by the operation, and the resulting indirect effects (also referred to as 'reverberating effects'). For example, if the data stored in the centre were being used for educational purposes and their loss would foreseeably halt the functioning of a school, that should also be considered a relevant form of incidental civilian harm when assessing the attack in question.

A related problem is the **difficulty of distinguishing between civilian objects and military objectives in cyberspace**. This difficulty is exacerbated by the use of technologies such as cloud storage: the client pays for a storage solution without necessarily knowing where exactly their data will be located, and whether it will be sharing storage space with other civilian or military data sets. It was noted that because of such challenges, whenever data are 'mixed', they should be regarded as civilian in nature, in order to ensure protection. It was queried, however, whether this would mean that storing a small amount of civilian data on a military server would immunize that server, and the military data sets it holds, from attack.

Another approach – more in line with the existing rules of IHL, it was suggested – would be to consider whether the military data sets in question (provided that they qualify as a military objective) could be targeted directly. If doing so was not feasible, then the server that stored both types of data could also be considered as a military objective on account of its dual use (i.e. it was also being used for military purposes).

¹⁸ For the full scenario, see Annex 3, scenario 3.

However, if the server becomes a military objective, that does not automatically mean that it can be attacked. For the attack to be lawful, additional rules must be observed, in particular the principles of precautions and proportionality, taking into account the incidental civilian harm that would foreseeably result from the attack.

Specifically with respect to precautions, it was noted that **IHL mandates that belligerents take all feasible precautions in the choice of means and methods of warfare to avoid or at least minimize incidental civilian harm.** Provided that the choice of a cyber operation instead of a kinetic one is feasible, and provided also that it causes less harm – in the specific circumstances – the principle of precaution requires that the cyber operation be given preference. The obligation to take all feasible precautions is technologically neutral: it also applies to means and methods relying on new technologies. Whether this is feasible in a specific instance depends on the circumstances at the time, including humanitarian and military considerations.

SESSION 6: LIMITS ON THE CONDUCT OF INFORMATION OR PSYCHOLOGICAL OPERATIONS DURING ARMED CONFLICTS

Moderator: Paola Burgos Zechinelli, Legal Adviser, ICRC

Expert presentation: Talita Dias, Research Fellow, Jesus College and Oxford Institute for Ethics, Law and Armed Conflict, University of Oxford

The opening presentation¹⁹ noted that the term ‘**information operations**’ referred to a broad category of conduct that was understood to include “any coordinated or individual deployment of digital resources for cognitive purposes to change or reinforce attitudes or behaviour of the targeted audience”.²⁰ Examples include misinformation, disinformation, hate speech, or propaganda. Information operations are not unlawful per se under IHL and they have been a constant feature of armed conflicts.

However, there are **specific IHL rules** that cover different aspects and/or results of such operations in the context of armed conflict. They include:

- a. the **obligation to respect and protect certain categories of specially protected persons (such as medical, religious and humanitarian personnel)**: this obligation applies at all times and irrespective of the type of operation – physical or digital. Accordingly, it protects these persons against harm as well as against disruption, irrespective of the purpose of the operation against them.
- b. the **obligation to respect and ensure respect for IHL**: any encouragement to violate IHL would be inconsistent with the duty to respect IHL. The duty to ensure respect for IHL encompasses the duty to prevent and redress IHL violations, which – as an obligation of conduct – must be assessed by reference to the standard of due diligence. Accordingly, its application depends on criteria such as the state’s capacity to act and its actual or constructive knowledge of the underlying IHL violations.
- c. **obligations to direct military operations only against military personnel and to take constant care to spare civilians in the conduct of military operations**: whether these duties cover information operations depends, first, on whether the notion of ‘military operations’ covers a broader range of conduct than just ‘attacks’ and second, on whether a given information operation falls within that range of conduct.

¹⁹ For more information, see section 4.4 of the background document (Annex 2).

²⁰ [The Oxford Statement on The Regulation of Information Operations and Activities](#), June 2021, preamble.

- d. **the prohibition of directing attacks against civilians:** the application of this rule depends on whether information operations may qualify as ‘attacks’ under IHL. In this respect, some states have expressed the view that certain operations may so qualify. However, it may be difficult to square that position with the generally accepted requirement that a cyber operation amounts to an ‘attack’ only if it is ‘reasonably expected’ to cause death, injury, or damage.²¹ This is because before an information operation results in such effects, another actor needs to decide to cause violence on the basis of the information received, thus breaking the causal chain. A possible exception may be where the violent harm occurs without the addressee having the ability or opportunity to make such a decision: for example, where a party to the conflict spreads disinformation falsely describing as ‘safe’ those routes that in fact lead through minefields, resulting in civilian deaths – which could be seen as bringing the operation within the scope of ‘attack’ as understood under IHL.

During the discussion, there was a general consensus that **information operations may have serious humanitarian consequences**, and thus deserve close attention. In particular, many non-state armed groups and criminals engage in the spread of disinformation to further their aims. People can be misled by misinformation, but they often play – whether unwittingly or not – an important role in its spread on social media. Information operations are also used to specifically victimize various groups defined by ethnic, religious, or political criteria.

Some attention was given to the question of the law applicable to **information operations occurring outside of situations of armed conflict**. In these cases, the relevant legal frameworks would include international human rights law (IHRL), international criminal law, and the domestic law of the states affected – but not IHL, which applies only during armed conflict. While it is conceivable that some kinds of cyber operation could trigger the application of IHL (see session 2 above), it is difficult to envisage a situation where an information operation alone would do so.

However, **once an armed conflict – whether international or non-international in nature – is under way, all information operations with a nexus to that conflict must comply with the applicable rules of IHL**. In this regard, the prohibition against operations targeting health facilities must be considered. It was noted that cyber operations against health facilities are covered by the relevant rules, and in some cases, may amount to war crimes. Finally, the prohibition of threats of violence aimed at terrorizing the civilian population was highlighted as another legal constraint on information operations during armed conflict.²²

SESSION 7: NATIONAL POSITIONS

Moderator: Alfredo Uriel Pérez Manríquez, Legal Adviser, Ministry of Foreign Affairs of Mexico

Expert presentations:

- Cláudio Leopoldino, Head of the Division for Disarmament and Sensitive Technologies, Ministry of Foreign Affairs of Brazil
- Maitê de Souza Schmitz, First Secretary, Permanent Mission of Brazil to the United Nations
- Maria Tolppa, Legal Adviser, Ministry of Foreign Affairs of the Republic of Estonia

Mr Leopoldino opened the session by placing the question of national positions on the application of international law in the **contemporary international context**. In 2017, the United Nations (UN) Group of Governmental Experts (GGE) did not reach a consensus, in part owing to a deadlock on the politically fraught question of the applicability of international law, including IHL. In light of this, the mandate of the next GGE (2019–2021)

²¹ See e.g. Michael N. Schmitt and Liis Vihul (eds), *Tallinn Manual 2.0 on International Law Applicable to Cyber Operations*, 2nd ed., Cambridge University Press, Cambridge, 2017, rule 92.

²² See Jean-Marie Henckaerts and Louise Doswald-Beck (eds), *Customary International Humanitarian Law*, Vol. 1: Rules, Cambridge University Press, Cambridge, 2005, rule 2.

included an invitation to states to submit their national positions on the applicability of international law.²³

However, some members of that GGE resisted the inclusion of such positions in the official GGE report, on the grounds that doing so would constitute a formal recognition of their validity by the UN General Assembly. Others took the view that inclusion of the positions, as an annex to the report, was mandated by the resolution establishing the GGE. In the end, the GGE agreed on a compromise solution to make “an official compendium ... of voluntary national contributions” available on the website of the UN Office of Disarmament Affairs.²⁴

This compendium²⁵ represents a wealth of views – from 15 states in all – that Latin American states could take into account when they elaborate their national positions. In this regard, it should be noted that the 2021 OEWG report recommended to states that they submit their views, on a voluntary basis, on how international law applied to the use of ICTs in the context of international security.²⁶ In Brazil’s view, the new OEWG would benefit greatly from new contributions by Latin American states.

Ms de Souza Schmitz continued by elaborating on **Brazil’s national position**.²⁷ For Brazil, the starting point was that cyber operations do not occur in a legal vacuum. In their use of ICTs, states must comply with international law, including the United Nations Charter, IHRL and IHL. At the same time, for the sake of clarity and legal certainty, it might be necessary to further develop some legal norms.

Brazil’s national position covers the key issues of international relevance, which were identified through the discussions in the GGE, the relevant reports of the OAS’s Inter-American Juridical Committee, and an analysis of the existing national positions and views expressed in expert and multilateral forums. These issues include sovereignty, non-intervention, use of force, state responsibility, and IHL.

As far as IHL in particular is concerned, Brazil’s view was that there was no doubt that IHL applies to states’ use of ICTs during armed conflict. The fact that a specific weapon had been invented after the development of IHL did not exempt it from regulation. The recognition that IHL applies to cyberspace does not in any way endorse the militarization of cyberspace or legitimize cyber warfare; it only ensures a minimum level of protection in the event of armed conflict.

Ms Tolppa delivered, from **Estonia’s perspective**, the final framing presentation in this session. She agreed that the last GGE report could be seen as a success, given the difficulties in discussing the applicability of international law in cyberspace. National positions played an increasingly important role in advancing global and regional discussions, and it was likely that they would serve a key role in the new iteration of the OEWG. It was commendable that states were starting to address difficult issues, such as sovereignty, due diligence, and countermeasures.

Estonia published its first national position in 2019, in the form of a speech delivered by the nation’s president.²⁸ In 2021, it submitted a revised version of this speech, as part of the GGE compendium mentioned above.²⁹ The Estonian position covers a broad range of issues of international law, including sovereignty, non-intervention, use of force, due diligence, IHL, IHRL, state responsibility and attribution, peaceful

²³ UNGA Res. 73/266, ‘Advancing Responsible State Behaviour in Cyberspace in the Context of International Security’, UN Doc. A/RES/73/266, 2 January 2019, para. 3.

²⁴ UN General Assembly, ‘Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security’, UN Doc. A/76/135, 14 July 2021, para. 73.

²⁵ UN General Assembly, ‘Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution 73/266’, UN Doc. A/76/136, 13 July 2021 (GGE compendium).

²⁶ UN General Assembly, ‘Developments in the field of information and telecommunications in the context of international security’, UN Doc. A/75/816, 18 March 2021, para. 38.

²⁷ See GGE compendium, *supra* note 25, pp. 17–23.

²⁸ See ‘President Kaljulaid at CyCon 2019: Cyber attacks should not be easy weapon’, ERR News, 29 May 2019.

²⁹ See GGE compendium, *supra* note 25, pp. 23–30.

settlement of disputes, retorsion, countermeasures, and self-defence. Insofar as IHL is concerned, the Estonian position affirms that this body of law applies to all operations with a nexus to armed conflict, including cyber operations.

For Estonia, the main takeaway from the process of preparing these two positions – the original speech and the revised version – has been that a broader engagement is needed in order to fully understand what a state's obligations under international law are. The development of national positions thus needs to be a cross-ministerial exercise, and must include public authorities, and national security and law enforcement agencies. Diverse materials should be consulted, including civil society input and academic research; in this regard, the Cyber Law Toolkit project³⁰ had been particularly useful.

During the discussion, several participants reaffirmed their states' **commitment to the application of international law, including IHL and IHRL, in cyberspace**. It was noted in this respect that national positions issued by states complemented existing multilateral processes, including the OEWG and the GGE. In particular, by developing their national positions, states could move the focus from questions of the applicability of international law – which had dominated the discussions so far – to details on how exactly international law applies in the cyber context.

The **importance of implementing states' international obligations at the domestic level** was also emphasized. In this respect, states should continue to evolve their domestic legal orders in parallel with the development of their national positions and with the relevant international discussions. As one participant noted, “cyber operations constantly evolve”, and thus the law – both international and domestic – must keep pace with them.

SESSION 8: MULTILATERAL ENGAGEMENT

Moderator: Oscar Macías, Legal Adviser, Ministry of Foreign Affairs of Mexico

Expert presentations:

- Ambassador Burhan Gafoor, Permanent Representative of the Republic of Singapore to the United Nations and Chair of the Open-ended working group (OEWG) on security of and in the use of information and communications technologies
- Mariana Salazar Albornoz, Rapporteur for International Law Applicable to Cyberspace, Inter-American Juridical Committee of the Organization of American States

Ambassador Gafoor opened the session by highlighting that cyber security was seen as an urgent issue at the UN. No country could by itself protect cyberspace, or guarantee its cyber security on its own, which underscored the need for international cooperation. The creation of the first OEWG in 2018 was a key step forward in this respect, as it was the first time that all UN member states could participate in a multilateral discussion on ICTs and international security. He commended Latin American states for having been particularly active in these debates.

From his perspective as Chair of the OEWG, he said, the **key priorities for the present OEWG** included:

1. encouraging the inclusive participation of all states, regardless of whether they were large or small, or whether they had advanced cyber capabilities and knowledge or not.
2. using the previous work of the OEWG to build upon what had already been achieved, i.e. the existing framework of norms, rules, and principles.
3. using the new OEWG as a platform for action and implementation – including through gaining a better understanding of the capacities, structures, and institutions that states needed to implement measures already agreed at the international level.

³⁰ See [Cyber Law Toolkit](#).

4. engaging with stakeholders, including the private sector, think tanks, and NGOs: cyber security issues cannot be solved by governments on their own.
5. encouraging regional efforts and consultations, such as the present one: having countries talk with one another represented an important confidence-building measure, and was part of the OEWG's mandate.

Prof. Salazar continued the session by providing an update on the **work of the Inter-American Juridical Committee (IAJC) on the issue of international law applicable to cyberspace**: she currently serves as special rapporteur in this connection. The rapporteurship started in 2018, with the aim of improving transparency and identifying the relevant national views of Latin American states.

The IAJC sent out a questionnaire, containing several key questions on the application of international law to cyber operations, to all OAS member states.³¹ However, only 9 out of 35 states submitted their answers,³² which highlights the varying degrees of understanding among states in the region. It is thus important to strengthen skills, and advance understanding, with regard to technical and legal matters in this connection. Analysis of the questionnaires received showed that most states affirmed that international law applies to cyberspace; some emphasized the applicability of the law on the use of force, IHL, and IHRL. In relation to IHL, there was some divergence of opinion as to whether a cyber operation had to cause death or injury to be regarded as an 'attack'; some participants took the view that a loss of functionality was sufficient. In general, the results confirmed states' interest in the issue of the applicability of international law to cyberspace and the continued need to engage in dialogue and in building capacities among states.

During the discussion, participants highlighted **the need for all states to take part in multilateral processes** such as the new OEWG, in order to contribute to and maintain their democratic, transparent, and inclusive nature. Discussions should build on the work that had already been done, including the general consensus on the applicability of international law in the cyber context. The application of international law, including the UN Charter, in cyberspace was essential for the maintenance of international peace and security.

With regard to the next steps for the **IAJC**, Prof. Salazar explained that, as a result of the informal consultations held with the legal advisers to OAS member states' foreign ministries, the majority deem it preferable to engage in capacity building before soliciting additional views from states on these issues. Therefore, she said, a training session would be organized by the IAJC with the OAS's International Law Department during the first half of 2022, and as rapporteur, she would continue to participate in dialogue and consultations. Once states were ready for further substantive engagement, a new questionnaire may be issued, one that was likely to contain fewer technical and more practical questions than the first one.

³¹ Questionnaire on the Application of International Law within OAS Member States in the Cyber Context, Verbal Note OEA/2.2/14/19.

³² See OAS, 'Improving Transparency: International Law and State Cyber Operations - Fifth Report', CJI/doc. 615/20 rev.1, 7 August 2020, Annex B.

ANNEX 1: LIST OF PARTICIPATING STATES

- Argentina
- Bolivia
- Brazil
- Chile
- Colombia
- Costa Rica
- Ecuador
- Mexico
- Nicaragua
- Paraguay
- Peru
- Uruguay

ANNEX 2: BACKGROUND PAPER

The aim of the event is to facilitate a dialogue between states from Latin America on international humanitarian law (IHL) and cyber operations, with a view to developing common understandings on how international law applies to uses of information and communication technologies (ICTs) during armed conflicts. The purpose of this background document is to provide relevant material to support the discussions during the regional consultation event. It does not necessarily reflect the views or positions of the co-organizing institutions.

Discussions during the regional consultation will focus on selected issues around the specific challenges to the application of IHL in the context of cyber operations, with a view to hearing the position of the participating experts in relation to these challenges, identifying areas of convergence and exploring ways of moving forward to clarify and possibly develop the law as needed.

The discussions at the meeting will be run under the understanding that the opinions expressed will not be attributed to the meeting's participants, also known as the "Chatham House rule". A report summarizing the discussions will be prepared after the event and published by the co-organizing institutions. The report will include the list of participating countries, but the substance of the discussion will be reported without attribution.

INTRODUCTION

The use of cyber operations during armed conflicts is, today, a reality. While only a few states have publicly acknowledged using such operations, an increasing number of states are developing military cyber capabilities, and their use is likely to increase in future. Just as any other means and methods of warfare, cyber operations have the potential to seriously affect civilian infrastructure and to result in human harm. They also raise a number of questions as to precisely how certain rules of IHL – which were drafted in a period predating the emergence of cyber operations as a means or method of warfare – apply to cyber operations.

In line with its mission and mandate, the International Committee of the Red Cross (ICRC) is primarily concerned with the protection that IHL affords against the humanitarian consequences of the use of means and methods of warfare during an armed conflict, including cyber operations when so used. Its positions on the challenges that these operations entail, including those that will be the focus of this regional consultation, have been presented in publicly available documents,¹ which form the basis for its engagement with states on this theme and which have informed the preparation of this document.

Mexico very much shares the need to reflect, as a regional block, on the humanitarian consequences of cyber operations. Our increasing dependency on technologies demands a clear legal framework to ensure responsible behaviour in cyberspace and protect civilians from harmful cyber operations. Yet, the nature of cyber operations represents a challenge when interpreting rules designed to regulate physical forms of violence. The present consultation represents a good opportunity to express our opinions concerning future regulations of cyber capabilities.

This background document will first briefly set the scene by defining the notion of cyber operations during armed conflicts and by presenting a summary of the current military use of cyber operations and their potential human cost (section 2). It then discusses the threshold question of whether IHL applies to cyber operations (section 3) and zooms in on four specific issues related to how IHL principles and rules apply to cyber operations during armed conflict (section 4). The document is also complemented by brief scenarios that will be used in the discussion (these are found in a separate Annex).

¹ See ICRC, [International humanitarian law and cyber operations during armed conflicts: ICRC position paper](#) (November 2019; hereafter *ICRC position paper*); see also Laurent Gisel, Tilman Rodenhäuser and Knut Dörmann, "Twenty years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts", *International Review of the Red Cross*, Vol. 102, No. 913, 2020, pp. 287–334.

CYBERSPACE AND CYBER OPERATIONS: SETTING THE SCENE

IHL does not contain a definition of cyber operations, cyber warfare or cyber war, and neither do other fields of international law. Various definitions of cyber operations have been used in military or other documents by certain states. Other states refer instead to information warfare or information war and define this notion in a manner that includes at least some aspects of what is often understood as cyber warfare. The ICRC understands cyber operations during armed conflict as “operations against a computer system or network, or another connected device, through a data stream, when used as means or method of warfare in the context of an armed conflict”.²

In the recent years, societies have become largely dependent on ICTs, a process only accelerated by the ongoing COVID-19 pandemic. While the benefits and opportunities of increased interconnectivity are countless, increased dependency also implies increased vulnerability. Whereas the emergent proliferation of cyber tools and their use as a means or method of warfare may offer belligerents the possibility of achieving their objectives without necessarily causing direct harm to civilians or physical damage to civilian infrastructure, the potential human cost of cyber operations must not be neglected. By means of cyber operations, processes controlled by computer systems can be triggered, altered, or otherwise manipulated with the potential to cause significant harmful effects for civilians.³ These risks are compounded by the interconnectivity that characterizes cyberspace, which means that whatever has an interface with the Internet can be affected by cyber operations conducted from anywhere in the world. A cyber operation against a specific system may have repercussions on various other systems, regardless of where those systems are located.

There is a real risk that cyber tools – either deliberately or by mistake – may cause large-scale and diverse effects on critical civilian infrastructures, such as essential industries, telecommunications, transport, governmental, and financial systems. Cyber operations conducted over recent years – primarily outside armed conflicts – have shown that malware can spread instantly around the globe and affect civilian infrastructure and the provision of essential services.⁴ As one cybersecurity expert put it recently, such military operations constitute a “humanitarian crisis in the making”.⁵

Cyber operations can harm infrastructure in at least two ways. First, they can affect the delivery of essential services to civilians, as has been shown with cyber operations against electrical grids and the health-care sector. Second, they can cause physical damage, as was the case with the Stuxnet attack against a nuclear enrichment facility in Iran in 2010, and an attack on a German steel mill in 2014.

Moreover, the characteristics of cyberspace raise specific concerns. For example, cyber operations entail a risk for escalation and related human harm for the simple reason that it may be difficult for the targeted party to know whether the attacker’s aim is intelligence collection or more harmful effects such as disrupting or destroying an asset. The target may thereby react with greater force than necessary out of anticipation of a worst-case scenario.

Cyber tools also proliferate in a unique manner. Once used, they can be repurposed or reengineered and thus widely used by actors other than the one that had developed or used them initially. A further concern is the difficulty to reliably attribute cyber operations, which hampers the identification of the authors of such operations and of holding them accountable, as well as the determination of the applicable legal framework.⁶

² *ICRC position paper*, supra note 1, p. 3 fn. 1.

³ See further ICRC, *The potential human cost of cyber operations* (May 2019).

⁴ Examples include the malware *CrashOverride*, the ransomware *WannaCry*, the wiper program *NotPetya*, and the malware *Triton*. *CrashOverride* affected the provision of electricity in Ukraine; *WannaCry* affected hospitals in several countries; *NotPetya* affected a very large number of businesses; *Triton* was aimed at disrupting industrial control systems, and was reportedly used in attacks against Saudi Arabian petrochemical plants. See further Laurent Gisel and Lukasz Olejnik, “*The Potential Human Cost of Cyber Operations: Starting the Conversation*”, *Humanitarian Law and Policy Blog*, 14 November 2018.

⁵ Sergio Caltagirone, “*Industrial Cyber Attacks: A Humanitarian Crisis in the Making*”, *Humanitarian Law and Policy Blog*, 3 December 2019.

⁶ See ICRC, *International humanitarian law and the challenges of contemporary armed conflicts* (2011), p. 37; Gisel, Rodenhäuser and Dörmann, supra note 1, pp. 309–310.

The perception that it will be easier to deny responsibility for such operations may also weaken the taboo against their use – and may make actors less scrupulous about using them in violation of international law.⁷

Overall, these concerns underscore the need to understand the potential harmful impact of cyber operations on the civilian population and, accordingly, the protections afforded to civilians and civilian infrastructure by the applicable international law.

APPLICABILITY OF IHL TO CYBER OPERATIONS DURING ARMED CONFLICTS

States have repeatedly reaffirmed that international law is applicable to the use of ICTs, most recently in this year's reports of the UN Open-Ended Working Group (OEWG)⁸ and the UN Group of Governmental Experts (GGE).⁹ The GGE report also expressly referred to IHL in the cyber context (a historical first for UN-based processes), noting that this branch of international law 'applies only in situations of armed conflict'.¹⁰

For the ICRC, there is no question that IHL applies to, and therefore limits, 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. In doing so, IHL seeks to minimize the humanitarian consequences of armed conflict whether caused by kinetic or cyber means. 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 are natural; or not a domain as such.¹¹

In line with this view, an increasing number of states and international organizations have publicly asserted that IHL applies to cyber operations during armed conflict.¹² At the same time, some states have expressed opposition to the militarization of cyberspace or a cyber arms race and have expressed concerns regarding a possible legitimization of the use of military cyber operations.¹³ While these are important considerations, they are not necessarily incompatible with the application of IHL to cyber operations during armed conflict.

In particular, asserting that IHL applies to cyber operations during armed conflict is not an encouragement to militarize cyberspace and should not be understood as legitimizing cyber-warfare.¹⁴ As underscored in the 2021 GGE report, 'recalling [IHL] principles by no means legitimizes or encourages conflict'.¹⁵ In fact, IHL imposes some limits to the militarization of cyberspace by prohibiting the development of military cyber capabilities that would violate IHL.¹⁶ Moreover, it must be noted that any use of force by states – cyber or

⁷ *ICRC position paper*, supra note 1, p. 8.

⁸ UNGA, *Open-ended working group on developments in the field of information and telecommunications in the context of international security: Final Substantive Report* (10 March 2021), para. 34.

⁹ UNGA, *Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security* (14 July 2021), para. 69.

¹⁰ Ibid. para. 71(f).

¹¹ ICRC, *International humanitarian law and the challenges of contemporary armed conflicts* (2015), p. 40; see also Michael N. Schmitt and Liis Vihul (eds), *Tallinn Manual 2.0 on International Law Applicable to Cyber Operations*, 2nd ed., Cambridge University Press, Cambridge, 2017 (hereafter *Tallinn Manual 2.0*), Rule 80.

¹² See e.g. *Council of the European Union, Council conclusions on the Commission and the High Representative of the European Union for Foreign Affairs and Security Policy joint communication on the Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, 25 June 2013, para. 6; NATO, *Wales Summit Declaration (Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales)*, 5 September 2014, para. 72.

¹³ See e.g. the submissions of China, Cuba, Iran, Nicaragua, or Russia on the initial pre-draft of the OEWG report, available at: www.un.org/disarmament/open-ended-working-group/.

¹⁴ *ICRC position paper*, supra note 1, pp. 4–5.

¹⁵ UNGA, *Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security* (14 July 2021), para. 71(f) in fine.

¹⁶ For example, IHL prohibits the development of cyber capabilities that would qualify as weapons and would be indiscriminate by nature or would be of a nature to cause superfluous injury or unnecessary suffering. See e.g. Jean-Marie Henckaerts and Louise Doswald-Beck (eds), *Customary International Humanitarian Law, Vol. 1: Rules*, Cambridge University Press, Cambridge, 2005 (hereafter *ICRC Customary Law Study*), Rules 70, 71.

kinetic – remains governed by the Charter of the United Nations and the relevant rules of customary international law, in particular, the prohibition against the use of force.¹⁷ International disputes must be settled by peaceful means,¹⁸ as recently reaffirmed in the cyber context by states in both the OEWG and the GGE processes.¹⁹

QUESTIONS TO CONSIDER

- Does the affirmation that international law applies to the use of ICTs cover all areas of international law, including IHL?
- Would affirming that IHL applies to cyber operations during armed conflicts risk militarizing cyberspace or legitimizing cyber warfare?
- Is it possible for states to acknowledge and address these concerns while at the same time affirming the applicability of IHL in cyberspace?

SPECIFIC CHALLENGES

While affirming that IHL applies to cyber operations in armed conflict is an essential first step to avoid or minimize the potential human suffering that cyber operations might cause, it is equally important for states to work towards common understandings of how IHL principles and rules apply to the specific nature of cyber operations. To that effect, participating states to the regional consultation are invited to exchange views on the following four challenges.

CYBER OPERATIONS AND THE NOTION OF “ATTACK” UNDER IHL

The question of whether or not an operation amounts to an “attack” as defined in IHL is essential for the application of many of the rules deriving from the principles of distinction, proportionality and precaution, which afford important protection to civilians and civilian objects.²⁰ Concretely, rules such as the prohibition on attacks against civilians and civilian objects, the prohibition on indiscriminate and disproportionate attacks, and the obligation to take all feasible precautions to avoid or at least reduce incidental harm to civilians and damage to civilian objects when carrying out an attack apply to those operations that qualify as “attacks” as defined in IHL. The question of how widely or narrowly the notion of “attack” is interpreted with regard to cyber operations is therefore essential for the applicability of these rules and the protection they afford to civilians and civilian infrastructure.

Article 49 of the 1977 Additional Protocol I defines attacks as “acts of violence against the adversary, whether in offence or in defence”. It is well established that the notion of violence in this definition can refer to either the means of warfare or their effects, meaning that an operation causing violent effects can be an attack even if the means used to cause those effects are not violent as such. For example, it is uncontroversial that the use of biological, chemical, or radiological agents during an armed conflict constitutes an attack under IHL, even though the attack does not involve physical force.²¹

¹⁷ UN Charter, Article 2(4).

¹⁸ UN Charter, Articles 2(3) and 33.

¹⁹ UNGA, *Open-ended working group on developments in the field of information and telecommunications in the context of international security: Final Substantive Report* (10 March 2021), para. 35; UNGA, *Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security* (14 July 2021), para. 70.

²⁰ The notion of attack under IHL, defined in Art. 49 of the 1977 First Additional Protocol, is different from and should not be confused with the notion of ‘armed attack’ under Art. 51 of the UN Charter, which belongs to the realm of *jus ad bellum*. To affirm that a specific cyber operation, or a type of cyber operations, amounts to an attack under IHL does not necessarily mean that it would qualify as an armed attack under the UN Charter.

²¹ Cordula Droegge, “Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians”, *International Review of the Red Cross*, Vol. 94, No. 886, 2012, p. 557.

It is also widely accepted that cyber operations expected to cause death, injury or physical damage constitute attacks under IHL.²² Some states have clarified that this includes harm due to the foreseeable direct and indirect (or reverberating) effects of an attack,²³ 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 – a view shared by the ICRC.²⁴

Beyond this, cyber operations that significantly disrupt essential services without necessarily causing physical damage constitute one of the most important risks that cyber operations raise for civilians. Diverging views exist, however, on whether a cyber operation that results in a loss of functionality without causing physical damage qualifies as an attack as defined in IHL.

In the ICRC's view, during an armed conflict an operation designed to disable a computer or a computer network can constitute an attack under IHL, whether the object is disabled through kinetic or cyber means. Indeed, if the notion of attack is interpreted as only referring to operations that cause death, injury or physical damage, a cyber operation that is directed at making a civilian network (such as electricity, banking, or communications) dysfunctional, or is expected to cause such effect incidentally, might not be covered by essential IHL rules protecting the civilian population and civilian objects. Such an overly restrictive understanding of the notion of attack would be difficult to reconcile with the object and purpose of the IHL rules on the conduct of hostilities.²⁵

Because cyber operations can significantly disrupt essential services without necessarily causing physical damage – such as those that would incapacitate banking or communications networks – this question constitutes one of the most critical debates for the protection of civilians against the effects of cyber operations. For the moment, opinions vary among the states that have taken public positions.²⁶

Finally, IHL remains relevant also to those cyber operations that do not qualify as “attacks”. On the one hand, some rules apply to a broader range of conduct described in IHL as “military operations”. This is the case, for example, with the obligation that “[i]n the conduct of military operations, constant care shall be taken

²² ICRC, *International humanitarian law and the challenges of contemporary armed conflicts* (2015), pp. 41–42; Tallinn Manual 2.0, supra note 9, Rule 92.

²³ See e.g. Denmark, *Military Manual on International Law Relevant to Danish Armed Forces in International Operations*, 2016, p. 677 (when discussing computer network attacks); Finland, *International law and cyberspace: Finland's national positions*, 2020, p. 7; New Zealand, *Manual of Armed Forces Law*, 2nd edition, 2017, Vol. 4, para. 8.10.22; Norway, *Manual i krigens folkerett*, 2013, para. 9.54; Switzerland, “Switzerland's position paper on the application of international law in cyberspace: Annex UN GGE 2019/2021”, May 27, 2021, p. 10; United States, “United States Submission to the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (2014–15)”, p. 6 and from a practical perspective Joint Publication 3–12 (R) ‘Cyberspace operations’, February 5, 2013, p. IV–4.

²⁴ *ICRC position paper*, supra note 1, p. 7.

²⁵ Ibid. pp. 7–8; for more details, see Gisel, Rodenhäuser and Dörmann, supra note 1, pp. 312–316.

²⁶ States that subscribe to the broader view that includes loss of functionality under the notion of “attack” include e.g. Ecuador, Verbal Note 4–2 186/2019 from the Permanent Mission of Ecuador to the OAS (June 28, 2019), cited in OAS, *Improving Transparency: International Law and State Cyber Operations: Fifth Report*, OAS Doc. CJI/doc. 615/20 rev.1, 7 August 2020, para. 32; France, Ministry of the Armies, *International Law Applied to Operations in Cyberspace*, 2019, p. 13; Germany, *On the Application of International Law in Cyberspace Position Paper*, March 2021, p. 9; Guatemala, Note Of. 4VM.200–2019/GJL/lr/bm, from Mr. Gabriel Juárez Lucas, Fourth Vice Minister of the Interior Ministry of the Republic of Guatemala to Luis Toro Utillano, Technical Secretariat, Inter-American Juridical Committee (14 June 2019), cited in OAS, *Improving Transparency: International Law and State Cyber Operations: Fifth Report*, OAS Doc. CJI/doc. 615/20 rev.1, 7 August 2020, para. 32; Japan, Ministry of Foreign Affairs of Japan, *Basic Position of the Government of Japan on International Law Applicable to Cyber Operations*, 2021, p. 7; New Zealand, *The Application of International Law to State Activity in Cyberspace*, 1 December 2020, para. 25. States that take the narrower view that requires physical damage include e.g. Denmark, *Military Manual on International Law Relevant to Danish Armed Forces in International Operations*, 2016, pp. 290–291; Roy Schöndorf, ‘Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations’, *International Law Studies*, Vol. 97, 2021, pp. 395–406, at 400; Peru, Response Submitted by Peru to the Questionnaire on the Application of International Law in OAS Member States in the Cyber Context (June 2019), cited in OAS, *Improving Transparency: International Law and State Cyber Operations: Fifth Report*, OAS Doc. CJI/doc. 615/20 rev.1, 7 August 2020, para. 31.

to spare the civilian population, civilians and civilian objects”.²⁷ This obligation requires all those involved in military operations to continuously bear in mind the effects of military operations on the civilian population, civilians and civilian objects, to take steps to reduce such effects as much as possible, and to seek to avoid any unnecessary effects.²⁸ Its applicability to cyber operations has been reaffirmed by several states.²⁹

On the other hand, some rules of IHL afford specific protection to certain categories of persons and objects that goes beyond the protection against attacks. For example, IHL specifically makes it illegal “to attack, destroy, remove or render useless objects indispensable to the survival of the civilian population”.³⁰ The explicit mention of “rendering useless” must be understood as covering a broader range of operations that may impact these goods, beyond attacks or destruction.³¹ Accordingly, cyber operations that are designed, or can be expected, to disable indispensable objects such as drinking water installations are prohibited, irrespective of whether they qualify as attacks.

Please see scenario 1 in the Annex for a case study illustrating this topic.

QUESTIONS TO CONSIDER

- Is the harm due to the foreseeable direct and indirect (or reverberating) effects of a cyber operation relevant to identify whether this operation is governed by the rules on “attack” under IHL?
- Is the loss of functionality relevant to identify whether a cyber operation is governed by the rules on “attack” under IHL?
- What protection does IHL afford with respect to those cyber operations that do not qualify as “attacks” under IHL?

THE PROTECTION AFFORDED TO CIVILIAN ELECTRONIC DATA UNDER IHL

Essential civilian data – such as medical data, biometric data, social security data, tax records, bank accounts, companies’ client files or election lists and records – are an essential component of digitalized societies. Such data are key to the functioning of most aspects of civilian life, be it at individual or societal level. There is increasing concern about safeguarding such essential civilian data. Deleting or tampering with essential civilian data can quickly bring government services and private businesses to a complete standstill and such operations could therefore cause more harm to civilians than the destruction of physical objects.

With regard to data belonging to certain categories of objects that enjoy specific protection under IHL, the protective rules are comprehensive. In particular, the obligations to respect and protect medical facilities³² and humanitarian relief operations³³ must be understood as extending to medical data belonging to those facilities and data of humanitarian organizations that are essential for their operations.³⁴ Similarly, deleting

²⁷ AP I, Art. 57(1); ICRC Customary Law Study, *supra* note 13, Rule 15.

²⁸ See e.g. United Kingdom, Ministry of Defence, *The Joint Service Manual of the Law of Armed Conflict*, 2004, para. 5.32.1; *Tallinn Manual 2.0*, *supra* note 9, para. 4 of the commentary on Rule 114; Stefan Oeter, ‘Methods of Combat’, in Dieter Fleck, *The Handbook of International Humanitarian Law*, 4th edition, Oxford University Press, Oxford, 2021, p. 215; Noam Neuman, ‘A Precautionary Tale: The Theory and Practice of Precautions in Attack’, *Israel Yearbook on Human Rights*, Vol. 48, 2018, pp. 28–29.

²⁹ See e.g. Finland, International law and cyberspace: Finland’s national positions, 2020, p. 7; France, Ministry of the Armies, International Law Applied to Operations in Cyberspace, 2019, p. 15; Germany, On the Application of International Law in Cyberspace Position Paper, March 2021, p. 9.

³⁰ AP I, Art. 54(2); AP II, Art. 14; ICRC Customary Law Study, *supra* note 13, Rule 54.

³¹ Gisel, Rodenhäuser and Dörmann, *supra* note 1, p. 327.

³² See, for instance, Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, Art. 19; Convention (II) for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea, Art. 12; Convention (IV) relative to the Protection of Civilian Persons in Time of War, Art. 18; AP I, Art. 12; Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (AP II), Art. 11; ICRC Customary Law Study, *supra* note 13, Rules 25, 28, 29.

³³ See e.g. AP I, Arts 70(4), 71(2); ICRC Customary Law Study, *supra* note 13, Rules 31 and 32.

³⁴ See Gisel, Rodenhäuser and Dörmann, *supra* note 1, pp. 327–328.

or otherwise tampering with data in a manner that renders useless objects indispensable to the survival of the civilian population, such as drinking water installations and irrigation systems, is prohibited.³⁵

Still, it is important to clarify the extent to which civilian data are protected by the existing general rules on the conduct of hostilities. In particular, debate has arisen on whether data constitute objects as understood under IHL, in which case cyber operations against data (such as deleting them) would be notably governed by the principles of distinction, proportionality and precaution and the protection they afford to civilian objects.

Experts hold different views on whether data qualify as objects for the purposes of the IHL rules on the conduct of hostilities. One view, held by the majority of experts involved in the Tallinn Manual process, is that the ordinary meaning of the term “object” cannot be interpreted as including data because objects are material, visible and tangible.³⁶ Some states also subscribe to this view.³⁷

By contrast, others have argued that either all or some types of data should be considered as objects under IHL. One view, taken by several states, is that the protection of civilian objects extends to civilian data.³⁸ This implies that all data constitute objects for the purposes of IHL. This interpretation is supported by the “modern meaning” of the notion of objects in today’s society as well as by the object and purpose of the relevant IHL rules.³⁹ It is also consistent with the traditional understanding of the notion of “object” under IHL, which is broader than the ordinary meaning of the word and encompasses also locations and animals.⁴⁰ Another approach, thus far endorsed by one state, is to consider content data (such as financial or medical data) as protected under the principle of distinction, leaving to the side whether other types of data (in particular operational data, also referred to as code) formally qualify as objects or not.⁴¹

While the question of whether and to what extent civilian data constitute civilian objects remains unresolved, in the ICRC’s view the assertion that deleting or tampering with such essential civilian data would not be prohibited by IHL in today’s data-reliant world seems difficult to reconcile with the object and purpose of IHL. Logically, the replacement of paper files and documents with digital files in the form of data should

³⁵ AP I, Art. 54; AP II, Art. 14; ICRC Customary Law Study, *supra* note 13, Rule 54.

³⁶ See *Tallinn Manual 2.0*, *supra* note 9, para. 6 of the commentary on Rule 100. The experts relied on the 1987 ICRC Commentary which notes that objects are material, visible and tangible; this explanation in the Commentary however, aimed at distinguishing objects from concepts such as “aim” or “purpose”, not at differentiating between tangible and intangible goods, and therefore cannot be seen as determinative for the debate on data (see Gisel, Rodenhäuser and Dörmann, *supra* note 1, p. 318).

³⁷ See e.g. Denmark, *Military Manual on International Law Relevant to Danish Armed Forces in International Operations*, 2016, p. 292; Chile, Response submitted by Chile to the OAS Inter-American Juridical Committee Questionnaire (14 January 2020), cited in OAS, *Improving Transparency: International Law and State Cyber Operations: Fifth Report*, OAS Doc. CJI/doc. 615/20 rev.1, 7 August 2020, para. 36; Roy Schöndorf, ‘Israel’s Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations’, *International Law Studies*, Vol. 97, 2021, pp. 395–406, at 401.

³⁸ See e.g. Finland, *International law and cyberspace: Finland’s national positions*, 2020, p. 7; Germany, *On the Application of International Law in Cyberspace Position Paper*, March 2021, p. 8; Romania, “National contribution on the subject of how international law applies to the use of information and communications technologies by States” in UNGA, *Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States* submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution 73/266 (13 July 2021), p. 78; Norway, *Manual i krigens folkerett*, 2013, para. 9.58.

³⁹ Kubo Mačák, “*Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law*”, *Israel Law Review*, Vol. 48, No. 1, 2015, pp. 55–80, at 80; see also Robert McLaughlin, “*Data as a Military Objective*”, *Australian Institute of International Affairs*, 20 September 2018.

⁴⁰ Gisel, Rodenhäuser and Dörmann, *supra* note 1, p. 319.

⁴¹ France, *Ministry of the Armies, International Law Applied to Operations in Cyberspace*, 2019, p. 14. For the view that, conversely, operational-level data (i.e., code) may qualify as an object, see Heather Harrison Dinniss, “*The Nature of Objects: Targeting Networks and the Challenge of Defining Cyber Military Objectives*”, *Israel Law Review*, Vol. 48, No. 1, 2015, pp. 39–54.

not decrease the protection that IHL affords to them.⁴² In essence, excluding essential civilian data from the protection afforded by IHL to civilian objects would result in an important protection gap.

Please see scenario 2 in the Annex for a case study illustrating this topic.

QUESTIONS TO CONSIDER

- Are medical, humanitarian or other specific data encompassed in the protection afforded by the various specific protection regimes under IHL?
- Do data in general, or only some specific types of data (such as content data or operational data), qualify as an “object” for the purposes of IHL?
- For those types of civilian data that might not be considered as “objects”, what IHL rules govern cyber operations against them? In particular, what is the protection afforded to essential civilian datasets such as social security data, property ownership data, tax records or bank accounts?

THE MILITARY USE OF CYBERSPACE AND THE EFFECT ON ITS CIVILIAN CHARACTER

In order to protect critical civilian infrastructure that relies on cyberspace, it is also crucial to protect the infrastructure of cyberspace itself. The challenge lies, however, in the interconnectedness of civilian and military networks.

Except for some specific military networks, cyberspace is predominantly used for civilian purposes. Furthermore, military networks may rely on civilian cyber infrastructure, such as undersea fibre-optic cables, satellites, routers or nodes. Conversely, civilian vehicles, shipping and air traffic controls increasingly rely on navigation satellite systems that may also be used by the armed forces. Civilian logistical supply chains and essential civilian services use the same web and communication networks through which some military communications pass. In other words, except for certain networks that are specifically dedicated to military use, it is to a large extent impossible to differentiate between purely civilian and purely military cyber infrastructures.⁴³

Under IHL, attacks must be strictly limited to military objectives. In so far as objects are concerned, 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.⁴⁴ All objects which are not military objectives under this definition are civilian objects under IHL and must not be made the object of an attack or of reprisals.⁴⁵ In case of doubt as to whether an object that is normally dedicated to civilian purposes is being used to make an effective contribution to military action, it must be presumed to remain protected as a civilian object.⁴⁶

It is traditionally understood that an object may become a military objective when its use for military purposes is such that it fulfils the definition of military objective even if it is simultaneously used for civilian purposes (such objects are sometimes referred to as “dual-use objects”).⁴⁷ However, a wide interpretation of this rule could lead to the conclusion that many objects forming part of cyberspace infrastructure would constitute military objectives and would therefore not be protected against attack, whether cyber or kinetic. This would be a matter of serious concern because of the ever-increasing civilian reliance on cyberspace.⁴⁸

⁴² ICRC, *International humanitarian law and the challenges of contemporary armed conflicts* (2019), p. 28.

⁴³ Gisel, Rodenhäuser and Dörmann, *supra* note 1, pp. 320–322.

⁴⁴ AP I, Art. 52(2); ICRC Customary Law Study, *supra* note 13, Rules 7–8.

⁴⁵ AP I, Art. 52(1); ICRC Customary Law Study, *supra* note 13, Rule 9.

⁴⁶ AP I, Art. 52(3); 1996 Amended Protocol II to the Convention on Certain Conventional Weapons, Art. 3(8)(a); see also ICRC Customary Law Study, *supra* note 13, Rule 10, commentary pp. 35–36.

⁴⁷ See e.g. ICRC Customary Law Study, *supra* note 13, Rule 10, commentary p. 32; Tallinn Manual 2.0, *supra* note 9, para. 1 of the commentary on Rule 101.

⁴⁸ Gisel, Rodenhäuser and Dörmann, *supra* note 1, p. 321.

As indicated, not every use for military purposes renders a civilian object a military objective under IHL – all elements of the definition of a military objective must be met.⁴⁹ Clarifying the extent to which the use by the military of a predominantly civilian object in the cyberspace turns this object into a military objective and therefore strips it from the protection afforded to civilian objects by IHL is therefore critical to ensure the protection of the civilian population that relies on these objects.

Please see scenario 3 in the Annex for a case study illustrating this topic.

QUESTIONS TO CONSIDER

- When assessing whether a particular part of cyber infrastructure qualifies as a military objective, what level (i.e., computer, node, router, cables, network, the internet) should that assessment be conducted at?
- What is the role of redundancy (i.e., the ability of computer networks to re-route data traffic) in assessing whether a target's destruction or neutralization would offer a definite military advantage?
- If a particular part of cyber infrastructure has become a military objective but is simultaneously used for civilian purposes ('dual-use'), do the effects on the civilian use have to be considered under the prohibition against indiscriminate attacks, and the rules of proportionality and precautions in attack when considering an attack on that objective?

LIMITS ON THE CONDUCT OF INFORMATION OR PSYCHOLOGICAL OPERATIONS DURING ARMED CONFLICTS

'Information operations' or 'psychological operations' have long been part of armed conflicts.⁵⁰ With the rapid growth of information and communication technology over the past decade, the scale, the speed, the reach of information or psychological operations has increased significantly, raising concerns about their possible humanitarian impact.⁵¹

States and non-state armed groups are using digital information or psychological operations for a variety of purposes. Some of them are meant to reduce the risk of harm to humans during armed conflicts, for example, communications technology can serve to give an effective advance warning of an attack or to help direct civilians to safety.

Conversely, other information or psychological operations are designed to cause confusion or harm, or to support the war effort and the public perception of a party to the conflict. For instance, information operations are used to mislead the adversary or to induce the adversary to act recklessly ('ruses of war'), to propagate the parties' views or 'narrative' about an armed conflict to influence domestic and international audiences, to discredit other parties to a conflict, or to recruit soldiers or fighters. Information or psychological operations have also been used to spread fear and terror among populations or to incite violence.⁵²

Information or psychological operations during armed conflicts are not, as such, unlawful. Experts have stressed that many forms of 'propaganda, even disinformation' are unproblematic under IHL⁵³ and that

⁴⁹ See text to note 44 above.

⁵⁰ There is no generally accepted definition of either of those two terms. The ICRC understands 'information operations' as '[t]he strategic and calculated use of information and information-sharing systems to influence, disrupt or divide society'. See ICRC, *Harmful Information: Misinformation, Disinformation and Hate Speech (MDH) in Conflict and Other Situations of Violence*, 2021, p. 18.

⁵¹ Ibid. p. 10.

⁵² For an overview of reported usages of information operations in contemporary armed conflicts, see Minority Rights Group International, *Peoples under Threat 2019*; see also Graphika, *French and Russian Influence Operations Go Head to Head Targeting Audiences in Africa*, 2020.

⁵³ Sassòli and Issar, "Challenges to International Humanitarian Law", in von Arnaud, Matz-Lück and Odendahl (eds), *100 Years of Peace Through Law: Past and Future*, Duncker & Humblot, Berlin, 2015, pp. 181–235.

‘psychological operations directed at the civilian population have been a feature of warfare for centuries’.⁵⁴ However, these operations do not occur in a normative void and insofar as they have a nexus to an armed conflict, they are subject to the applicable rules of IHL.

In broad terms, IHL contains two types of rules that address information or psychological operations during armed conflict. First, there are a few rules which address directly certain types of such operations. This category includes, for example, the prohibition of acts or threats of violence the primary purpose of which is to spread terror among the civilian population,⁵⁵ or the mentioning of ‘misinformation’ as a lawful ruse of war.⁵⁶ IHL also prohibits using ‘pressure or propaganda which aims at securing voluntary enlistment’ of protected persons in occupied territories.⁵⁷

The second category of IHL rules does not address propaganda or other types of information or psychological operations explicitly; instead, it imposes limits on the effects that can be lawfully pursued through such operations. This category includes a variety of rules, among others the prohibition against encouraging IHL violations,⁵⁸ the requirement to respect and protect specific categories of actors, such as medical personnel and humanitarian relief personnel.⁵⁹

On a number of these issues, IHL provides clear and well-established limits that apply to all methods of warfare, including digital ones. On others, however, further analysis and clarification is needed.

Please see scenario 4 in the Annex for a case study illustrating this topic.

QUESTIONS TO CONSIDER

- Is the use of information or psychological operations to encourage the commission of violations of IHL prohibited under IHL even in situations where it would be difficult to foresee whether they would actually trigger specific instances of IHL violations?
- Can information or psychological operations amount to inhumane treatment or outrages upon personal dignity prohibited by IHL?
- Are information or psychological operations designed or expected to result in physical violence governed by the principles of distinction, proportionality and precautions? What about those designed or expected to result in mental harm?

⁵⁴ Schmitt, [France Speaks Out on IHL and Cyber Operations](#): Part II, EJIL:Talk!, 1 October 2019.

⁵⁵ AP I, Article 51(2); AP II, Article 13(2), ICRC Customary Law Study, supra note 13, Rule 2.

⁵⁶ AP I, Article 37(2).

⁵⁷ GC IV, Article 51.

⁵⁸ Common Article 1; ICRC Customary Law Study, supra note 13, Rules 139 and 144.

⁵⁹ See ICRC Customary Law Study, supra note 13, Rules 25, 26, 31, and 32.

ANNEX 3: SCENARIOS FOR DISCUSSION

SCENARIO 1: CYBER OPERATIONS AND THE NOTION OF “ATTACK” UNDER IHL

In the context of an international armed conflict between states A and B, state A designs a cyber operation that aims to encrypt all data found on computers used by state B’s military, making the computers (and their data) unusable. State A knows that while its operation will not destroy the computer hardware, software will have to be reinstalled and it will take at least several days to do so.

State A plans to conduct this attack by means of a malware that is programmed to spread automatically and exploit a zero-day vulnerability in a specific security software. State A also knows that in state B, this software is used on computers of important government agencies, notably the armed forces, but also the government-owned electricity provider, which supplies 30 percent of state B’s electricity.

Upon deciding to launch the attack, state A expects that the operation will succeed in blocking many computers used by the military but also a number of those of the government-owned electricity provider, and that the disruption of the computers used by the government-owned electricity provider will lead to electricity outages in several parts of the country, affecting not only military installations but also civilian infrastructure, including hospitals and water facilities. While unable to quantify the consequences precisely, state A foresees that civilians will be adversely affected as a result, possibly including civilian deaths because of electricity cuts affecting hospitals’ intensive care units.

QUESTIONS TO CONSIDER

- Is the harm due to the foreseeable direct and indirect (or reverberating) effects of a cyber operation relevant to identify whether this operation is governed by the rules on “attack” under IHL?
- Is the loss of functionality relevant to identify whether a cyber operation is governed by the rules on “attack” under IHL?
- What protection does IHL afford with respect to those cyber operations that do not qualify as “attacks” under IHL?

SCENARIO 2: THE PROTECTION AFFORDED TO CIVILIAN ELECTRONIC DATA UNDER IHL

In the context of an international armed conflict between states A and B, state A conducts a series of cyber operations as part of its military efforts:

1. State A conducts a cyber operation against data stored in the computer network at state B’s central military command. The operation results in the deletion or corruption of all data stored in the network, which contained the identity, location, physical condition, staffing, and battle readiness of state B’s warships and military aircraft.
2. State A conducts a cyber operation against data held by state B’s central registry office, a governmental authority maintaining digital records on all state B’s citizens concerning non-military purposes, including census taking, the provision of social benefits, voting, and taxation. The operation results in the deletion of all data held by the office.
3. State A conducts a cyber operation against data held by a military hospital in state B that provides health care to members of state B’s armed forces, military retirees, and family members. The operation results in the deletion of all personal medical data of patients treated in the hospital since the beginning of the armed conflict.

QUESTIONS TO CONSIDER

- Are medical, humanitarian or other specific data encompassed in the protection afforded by the various specific protection regimes under IHL?
- Do data in general, or only some specific types of data (such as content data or operational data), qualify as an “object” for the purposes of IHL?
- For those types of civilian data that might not be considered as “objects”, what IHL rules govern cyber operations against them? In particular, what is the protection afforded to essential civilian datasets such as social security data, property ownership data, tax records or bank accounts?

SCENARIO 3: THE MILITARY USE OF CYBERSPACE AND THE EFFECT ON ITS CIVILIAN CHARACTER

States A and B are engaged in an international armed conflict against each other. The following incidents take place:

1. State A’s armed forces use several servers located in a large commercial data centre in state A’s own territory. The servers in question are used only for military purposes by state A; however, the data centre also contains many other servers used exclusively by civilians. State B launches a cyber operation that shuts down the entire data centre’s cooling system, thus overheating and damaging all the servers within it.
2. A military base in state A uses a specifically dedicated network that relies on power supplied by the general electricity grid. State B gains persistent access to the control station for the main power line supplying the region where the base is located. As state B starts a surprise ground offensive against the military base, its operators induce a power blackout throughout the region in order to hamper force co-ordination by state A. As a result, the civilian population in the region, as well as the local hospital and water treatment facility, lose their power supply.
3. State A relies on a global navigation system to generate location data for the purposes of co-ordinating the movement and manoeuvres of its armed forces, such as its military aircraft, warships, and armoured vehicles. The same system is used by the civilian population in many states around the world. State B launches a cyber operation against the system, rendering it dysfunctional for several days.

QUESTIONS TO CONSIDER

- When assessing whether a particular part of cyber infrastructure qualifies as a military objective, what level (i.e., computer, node, router, cables, network, the internet) should that assessment be conducted at?
- What is the role of redundancy (i.e., the ability of computer networks to re-route data traffic) in assessing whether a target’s destruction or neutralization would offer a definite military advantage?
- If a particular part of cyber infrastructure has become a military objective but is simultaneously used for civilian purposes (‘dual-use’), do the effects on the civilian use have to be considered under the prohibition against indiscriminate attacks, and the rules of proportionality and precautions in attack when considering an attack on that objective?

SCENARIO 4: LIMITS ON THE CONDUCT OF INFORMATION OR PSYCHOLOGICAL OPERATIONS DURING ARMED CONFLICTS

During an international armed conflict between states A and B, the following incidents occur:

1. State A designs and spreads messages on social media that refer to an ethnic group resident in state B as ‘terrorists’ and ‘traitors’ that deserve serious punishment. Subsequently, many individuals belonging to that group are subject to acts of violence.
2. State A uses its control over the telecommunications infrastructure in a region in state B to send text messages to civilians fleeing hostilities in that region. In the messages, it falsely describes as ‘safe’ routes that in fact lead through minefields. As a result, a number of individuals die.
3. State A publishes fabricated humiliating information about certain religious leaders resident in a part of state B occupied by state A. Those individuals were supportive of state B’s war effort and the information is designed to damage their reputation, thus weakening civilian morale and their support for state B’s war effort.

QUESTIONS TO CONSIDER

- Is the use of information or psychological operations to encourage the commission of violations of IHL prohibited under IHL even in situations where it would be difficult to foresee whether they would actually trigger specific instances of IHL violations?
- Can information or psychological operations amount to inhumane treatment or outrages upon personal dignity prohibited by IHL?
- Are information or psychological operations designed or expected to result in physical violence governed by the principles of distinction, proportionality and precautions? What about those designed or expected to result in mental harm?

ANNEX 4: AGENDA

DAY 1: TUESDAY 9 NOVEMBER 2021

09:45–10:00: Virtual room open for informal meet and greet

10:00–10:30: Introduction

Alejandro Celorio Alcántara, Chief Legal Adviser, Ministry of Foreign Affairs of Mexico

Laurent Gisel, Head of the Arms and Conduct of Hostilities Unit, ICRC

10:30–11:00: Technical overview

Moderator: Salvador Tinajero Esquivel, Coordinator of Public International Law, Ministry of Foreign Affairs of Mexico

Expert presentation: Mauro Vignati, Adviser on Digital Technologies of Warfare, ICRC

11:00–11:15: *Coffee break*

11:15–12:00: Applicability of IHL to cyber operations during armed conflicts

Moderator: Oscar Macías, Legal Adviser, Ministry of Foreign Affairs of Mexico

Expert presentation: Kubo Mačák, Legal Adviser, ICRC

12:00–12:45: Cyber operations and the notion of “attack” under IHL

Moderator: Daniel Cahen, Head of the Legal Department for Mexico and Central America, ICRC

Expert presentation: Kubo Mačák, Legal Adviser, ICRC

12:45–13:00: *Coffee break*

13:00–13:45: The protection afforded to civilian electronic data under IHL

Moderator: Kubo Mačák, Legal Adviser, ICRC

Expert presentation: Romina Soledad Morello, Regional Legal Adviser, ICRC

13:45–14:00: Wrap up of Day 1

14:00–14:15: Virtual room open for informal meet and greet

DAY 2: WEDNESDAY 10 NOVEMBER 2021

09:45–10:00: *Virtual room open for informal meet and greet*

10:00–10:15: **Welcome to Day 2**

10:15–11:00: The military use of cyberspace and the effect on its civilian character

Moderator: Salvador Tinajero Esquivel, Coordinator of Public International Law, Ministry of Foreign Affairs of Mexico

Expert presentation: Laurent Gisel, Head of the Arms and Conduct of Hostilities Unit, ICRC

11:00–11:15: *Coffee break*

11:15–12:00: Limits on the conduct of information or psychological operations during armed conflicts

Moderator: Paola Burgos Zechinelli, Legal Adviser, ICRC

Expert presentation: Talita Dias, Research Fellow, Oxford Institute for Ethics, Law and Armed Conflict

12:00–12:45: National positions on international law and cyberspace: Practical aspects

Moderator: Alfredo Uriel Pérez Manríquez, Legal Adviser, Ministry of Foreign Affairs of Mexico

Expert presentation: Cláudio Leopoldino, Head of the Division for Disarmament and Sensitive Technologies, Ministry of Foreign Affairs, Brazil, and Maitê de Souza Schmitz, First Secretary, Permanent Mission of Brazil to the United Nations

Expert presentation: Maria Tolppa, Legal Advisor, Ministry of Foreign Affairs of the Republic of Estonia

12:45–13:00: *Coffee break*

13:00–13:45: Multilateral engagement

Moderator: Oscar Macías, Legal Adviser, Ministry of Foreign Affairs of Mexico

Expert presentation: Ambassador Burhan Gafoor, Permanent Representative of the Republic of Singapore to the United Nations and Chair of the Open-ended working group on security of and in the use of information and communications technologies

Expert presentation: Mariana Salazar Albornoz, Rapporteur for International Law Applicable to Cyberspace, Inter-American Juridical Committee of the Organization of American States




13:45–14:00: Closing session

Alejandro Celorio Alcántara, Chief Legal Adviser, Ministry of Foreign Affairs of Mexico

Laurent Gisel, Head of the Arms and Conduct of Hostilities Unit, ICRC

MISSION

The International Committee of the Red Cross (ICRC) is an impartial, neutral and independent organization whose exclusively humanitarian mission is to protect the lives and dignity of victims of armed conflict and other situations of violence and to provide them with assistance. The ICRC also endeavours to prevent suffering by promoting and strengthening humanitarian law and universal humanitarian principles. Established in 1863, the ICRC is at the origin of the Geneva Conventions and the International Red Cross and Red Crescent Movement. It directs and coordinates the international activities conducted by the Movement in armed conflicts and other situations of violence.

 facebook.com/icrc
 twitter.com/icrc
 instagram.com/icrc



International Committee of the Red Cross
19, avenue de la Paix
1202 Geneva, Switzerland
T +41 22 734 60 01
shop.icrc.org
© ICRC, June 2022