REGIONAL CONSULTATION OF ASIA-PACIFIC STATES
29–30 NOVEMBER 2022

INTERNATIONAL HUMANITARIAN LAW AND CYBER OPERATIONS DURING ARMED CONFLICTS
CONTENTS

Introduction............................................................................................................................................ 4
Session 1: Digital operations during armed conflicts: current realities .............................................. 4
Session 2: The prohibition against the use of force under the UN Charter and when IHL applies to cyber operations during armed conflict................................................................................................................................. 5
Session 3: The notion of ‘attack’ under IHL and the protection of civilian objects.......................... 7
Session 4: The protection afforded to civilian electronic data under IHL ........................................... 8
Session 5: The military use of cyberspace and the effect on its civilian character ......................... 9
Session 6: Limits on the conduct of information or psychological operations during armed conflicts .................................................................................................................................................................................. 10
Session 7: National positions on international law and cyberspace: practical aspects .................. 11
Session 8: Multilateral discussions on cyber operations during armed conflict .............................. 13
Annex 1: List of participating states ..................................................................................................... 15
Annex 2: Background paper .................................................................................................................. 16
Annex 3: Agenda.................................................................................................................................... 30
EXECUTIVE SUMMARY

The Ministry of Foreign Affairs of the Republic of Indonesia and the International Committee of the Red Cross (ICRC) jointly organized – on 29 and 30 November 2022 – a regional consultation of states in the Asia-Pacific region on international humanitarian law (IHL) and cyber operations during armed conflicts. The aim of the event was to facilitate a dialogue between states in the region, with a view to fostering the exchange of views and developing a common understanding of how and when IHL applied to the use of information and communication technologies (ICT) during armed conflicts. These were the main points of discussion at the event:

IHL IMPOSES LIMITS ON CYBER OPERATIONS DURING ARMED CONFLICTS BUT THIS AFFIRMATION DOES NOT LEGITIMIZE CONFLICT IN CYBERSPACE

• Several participants expressed the view that IHL applies to cyber operations during armed conflict, such as those conducted alongside kinetic military operations during armed conflict, and that this affirmation by no means legitimizes or encourages conflict.
• IHL (jus in bello) and the prohibition against the use of force under the United Nations (UN) Charter and customary international law (jus ad bellum) are separate fields of international law. A military operation may constitute a lawful use of force under the UN Charter and at the same time violate IHL – or vice versa. Legal consequences of such violations have to be assessed separately under each field of law.

FURTHER STUDY IS NEEDED TO CLARIFY HOW IHL APPLIES TO CYBER OPERATIONS DURING ARMED CONFLICTS

• Current trends in the use of cyber operations during armed conflict show that there is a real risk of harm to civilians or damage to civilian objects. To know whether the protection afforded by IHL is sufficient to prevent or mitigate such harm or damage, further study on how IHL applies to cyber operations is needed.
• Clarifying which cyber operations amount to an ‘attack’ as defined in IHL is needed to determine the applicability of several IHL rules on the conduct of hostilities to such operations. Some participants opined that cyber operations that can be reasonably expected to cause a loss of functionality in the target amount to an ‘attack’, but others questioned whether that view would be too inclusive. It was clarified that the notion of ‘attack’ under IHL was legally different from the notion of ‘armed attack’ under the UN Charter.
• In today’s digitalized society, tampering with and deleting civilian electronic data can have a significant impact on civilian life. There is a need to develop a shared understanding of whether IHL affords civilian data protection similar to that given to a ‘civilian object’. One participant expressed the position that data were an ‘object’ under IHL. The contrary view was acknowledged, but not endorsed by any of the participants.
• Use of the same cyber infrastructure by civilians and the military poses a risk of such infrastructure becoming a military objective under IHL. This underscores the need to further study the circumstances in which ‘dual-use’ cyber infrastructure would qualify as a ‘military objective’ as defined in IHL and the conditions under which targeting such infrastructure would not be a violation of IHL.
• Information or psychological operations may have serious humanitarian consequences and are today exacerbated by digital technology. It was recalled that IHL limits must be observed by those conducting such operations.

STATES CAN HELP CLARIFY HOW INTERNATIONAL LAW APPLIES TO CYBERSPACE BY DEVELOPING NATIONAL POSITIONS

• Several participants shared their experience in developing national positions and encouraged other states to do the same. In their view, this could help advance multilateral discussions on this subject, with a view to building common ground and clarifying how IHL protects civilians against the danger of cyber operations during armed conflicts.
INTRODUCTION

The Ministry of Foreign Affairs of the Republic of Indonesia and the International Committee of the Red Cross (ICRC) jointly organized – on 29 and 30 November 2022 – a regional consultation of states in the Asia-Pacific region on international humanitarian law (IHL) and cyber operations during armed conflicts. The aim of the event was to facilitate a dialogue between states in the region, with a view to fostering an exchange of views and developing a common understanding of how and when IHL applies to the use of information and communication technologies (ICT) during armed conflicts.

This report aims to provide an account of the discussions among experts and other participants that took place during the consultation. It summarizes the main points of the discussions at each session, without attributing them to specific participants. An earlier draft of the report was submitted to participants for comments.

The report includes a list of participating states (Annex 1), a detailed background document with a set of hypothetical scenarios (Annex 2) and the agenda of the consultation (Annex 3).

The report does not purport to represent the views of the ICRC, the Government of the Republic of Indonesia or any of the participating states.

SESSION 1: DIGITAL OPERATIONS DURING ARMED CONFLICTS: CURRENT REALITIES

Moderator: Harditya Suryawanto, Counsellor, Directorate of International Security and Disarmament, Ministry of Foreign Affairs of the Republic of Indonesia
Expert presentation: Mauro Vignati, Adviser on Digital Technologies of Warfare, ICRC

The framing presentation summarized current military use of cyber operations and its potential human cost. Many states have developed cyber capabilities such as phishing, sending decoy documents with malware attached, disinformation campaigns and website defacement. In addition, there are two worrying trends in current military use of cyberspace, notably malware with destructive effects on networks, software and data that is increasingly used against critical civilian infrastructure, and the involvement of civilians in digital operations in support of a party to conflict.

The latter trend of civilian involvement in digital operations is apparent notably in the emergence of groups of ‘hacktivists’ who conduct operations against a party to conflict or against private companies whose services are used by a party to conflict. Civilians have also participated in intelligence gathering by uploading images and the location of enemy forces to an application.

Another challenge stems from the ‘dual use’ of digital technologies by civilians and the military, which may call into question the civilian character of such technologies under IHL. The fact that these technologies are generally owned by private companies, and may be located outside the territory of parties to armed conflict, adds a layer of complexity. Additional challenges are also seen in the distribution of DDoS tools to a large number of civilians, massive exfiltration of data belonging to civilians and civilian entities and the use of malware of low quality with greater risk of collateral harm.

1 DDoS (distributed denial of service) is an event-based operation without network access, in which the attacker uses a botnet – i.e. a series of infected computers – to bring down a web server, and thus disrupt the services that the server provides.
During the discussion, a concern was raised regarding civilians’ involvement in armed conflict through social media, where it is difficult to draw a line between the types of conduct that would be regarded as being linked to armed conflict – and therefore limited by IHL – and those that would not. Similarly, as regards civilians conducting harmful digital operations against a party to conflict, the question arose of whether they should be classified as ‘fighters’.

The ICRC noted that civilians’ participation in armed conflict was a reality in both cyber and kinetic warfare. The most common practice was the participation in armed conflict of civilian government agencies – such as intelligence services – and private individuals. IHL addresses this phenomenon through its rules on ‘direct participation in hostilities’. While there is broad agreement on the main aspects of what this notion means under IHL, further study is needed in the specific context of cyber operations.

The harm suffered by private companies who have their confidential information exfiltrated and distributed online was also underlined. These companies may not have any relationship with parties to conflict. It was noted that both states and companies have roles in preventing and addressing such exfiltration.

In addition, the expert presenter drew attention to the fact that while some forms of malware were becoming more mature or targeted, they were also becoming more destructive. At the same time, some of the malware used in armed conflict was of poor quality or had not been tested prior to its deployment. This meant that the operators did not fully understand the functioning of such malware and might not be able to contain their effects as required by IHL.

Finally, it was queried whether IHL was sufficient to address all these challenges. In response, the ICRC noted that this question only underscored the importance of discussions between states on the dangers created by cyber operations during armed conflicts, and how IHL protects civilians against such risks. The ICRC said that it had not taken a definitive position on the sufficiency of IHL in this regard, and that much depended on how states understood and applied the existing rules, which can offer strong protection by imposing important limits on many cyber operations.

**SESSION 2: THE PROHIBITION AGAINST THE USE OF FORCE UNDER THE UN CHARTER AND WHEN IHL APPLIES TO CYBER OPERATIONS DURING ARMED CONFLICT**

*Moderator:* Kubo Mačák, Legal Adviser, ICRC  
*Expert presentations:*  
• Benjamin Ang, Deputy Head of the Centre of Excellence for National Security; Coordinator of the Cyber and Homeland Defence Programme, Singapore  
• Tilman Rodenhäuser, Legal Adviser, ICRC

The starting point of the framing presentations was the explicit reference to IHL in the 2021 report of the UN Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (GGE), which is generally regarded as being a recognition of IHL application to the use of ICT in situations of armed conflict. The report mentions some IHL principles and states that recalling these principles by no means legitimizes or encourages conflict. It was further noted that if the term ‘cyber’ was replaced with ‘missiles’, no one would question whether affirming IHL application to ‘missiles’ legitimized or encouraged their use.

---

When a cyber operation is carried out by one state against another, such conduct must also be analysed under the UN Charter. In this regard, it was noted that the question of which cyber operation qualified as a resort to “armed force” for the purpose of Article 2 common to the four Geneva Conventions of 1949 – hence triggering the application of IHL – was different from the question of whether it qualified as “use of force” or an “armed attack” under Articles 2(4) and 51 of the UN Charter, respectively. The two questions derived from two distinct fields of international law, must be treated separately, and entailed different legal consequences.

Moving to when IHL applied, there should be no question that IHL applied to a specific cyber operation conducted alongside, and with a nexus to, kinetic operations during an ongoing armed conflict. What remains unsettled is whether a cyber operation can in and of itself trigger the application of IHL – namely be the first, or possibly only, operation legally classified as an international armed conflict and therefore subject to IHL rules. For this to be the case, the cyber operation would need to be regarded as ‘a resort to armed force’ between states.\(^3\) It was argued that cyber operations that had effects similar to those of kinetic operations should be governed by IHL, but it appeared less clear if this should also be the case for cyber operations that resulted only in disruption of the targeted system.

During the discussion, it was opined that determining the applicability of IHL based on the effects of a specific cyber operation would mean not knowing whether IHL applied to that operation until after it was executed. In response, an expert presenter noted that under IHL the commander had an obligation to assess the reasonably expected impact of the operation before carrying it out, with a view to determining whether and which IHL rules and principles applied.

The relationship between the prohibition against the use of force \((jus ad bellum)\) and IHL \((jus in bello)\) was the subject of further reflection. An expert presenter explained that when a state used force against another state, it must examine the lawfulness of such use of force under both fields of law. The conclusions drawn from them are completely separate. A military operation may constitute lawful use of force under the UN Charter and may also be a violation of IHL. An example of this situation is a cyber operation carried out by a state within the framework of its right to self-defence that would violate the obligation to do everything feasible to verify that the target was a military objective under IHL.

One participating state affirmed its position that acknowledging the application of IHL to cyber operations did not mean legitimizing conflict in cyberspace. No contrary view was expressed.

The discussion also touched on the applicability of IHL to cyber operations conducted by private actors. An expert presenter noted that these private actors would have an obligation to comply with IHL only with regard to cyber operations that had a nexus to an armed conflict. Moreover, even if an operation was conducted by private actors, it may be attributable to a state if the actors operated under the state’s instruction, direction or control.

Some attention was also given to nuclear, chemical and biological weapons, which have been regulated by specific treaties in recent years – unlike cyber operations that have been left to be governed by long-standing rules of IHL. States should reflect on the continuous evolution of cyber capabilities and consider whether the law needed to be developed further. In this respect, the expert presenters noted that existing IHL rules and principles could be implemented in cyberspace, but there remained questions – about the details of how to apply certain rules and principles – that required further clarification. Some of the questions that need to be addressed included the following: Does stealing, tampering or deleting data constitute an ‘attack’ under IHL? Does ‘attack’ require physical damage to the target? Do data qualify as an ‘object’ under IHL? Discussing these questions is necessary in order to find out whether the law needs to be developed through a new legal instrument, international consensus on certain definitions or other avenues.

The ICRC stated that it continued to foster multilateral discussions on this subject and had issued a report that could help states reduce civilian harm from military cyber operations.

Attribution was mentioned as another challenging issue. The anonymity of cyber operations made it difficult to attribute them to a specific actor. An expert presenter suggested that if states were to agree on an attribution framework, they could establish a threshold of evidence required for it. The discussion then shifted to the involvement of non-state actors in cyber operations and how to ensure that they complied with IHL. In this respect, it was noted that states had the primary obligation to ensure respect for IHL, especially when the act in question was attributable to them. The ICRC also described its efforts to promote respect for IHL by all parties to conflict, including non-state armed groups.

**SESSION 3: THE NOTION OF ‘ATTACK’ UNDER IHL AND THE PROTECTION OF CIVILIAN OBJECTS**

**Moderator:** Tilman Rodenhäuser, Legal Adviser, ICRC  
**Expert presentation:** Professor Yoo Joon-Koo, Institute of Foreign Affairs and National Security, Republic of Korea

The framing presentation noted that most rules of IHL on the conduct of hostilities applied only to an ‘attack’ as defined in IHL. These notably include rules derived from the principles of distinction, proportionality and precaution. Therefore, it was imperative to clarify which cyber operations qualified as an ‘attack’ under IHL, thereby triggering the application of such rules.

Article 49 of Protocol I of 1977 additional to the Geneva Conventions (Additional Protocol I) defines attacks as “acts of violence against the adversary, whether in offence or in defence”. While acknowledging that opposing views existed, it was posited that the notion of ‘violence’ did not necessarily require physical damage. IHL principles and rules governing ‘attacks’ should therefore apply to cyber operations that disabled the targeted system through loss of functionality. Further, in the view of the expert presenter, the precautionary principle appeared to pose the most challenges in terms of application to cyber operations.

During the discussion a concern was raised that including cyber operations that only result in the loss of functionality, in the meaning of the notion of ‘attack’, could be too inclusive. In response, the ICRC noted that IHL looked at the effects of the act in question. For example, a party to conflict that seeks to deprive its adversary of electricity may choose to physically destroy the power grid or simply disable it with a graphite bomb. While only one causes physical damage, both result in the loss of electricity and are governed by the rules on ‘attacks’ under IHL. To say that IHL rules did not apply to a cyber operation that results in similar loss of functionality may depart from the object and purpose of IHL of protecting civilians against the harmful effects of armed conflict. It also risked creating loopholes in the protection of civilian objects. This being said, any act falling short of an attack was still subject to other rules of IHL.

It was further queried whether an expansive interpretation of the notion of ‘attack’ under IHL could also result in a broad interpretation of the notion of ‘armed attack’ under the UN Charter. In this respect, the ICRC recalled that while some terms may appear similar under IHL and the UN Charter, their meaning was different. The notion of ‘attack’ under IHL determined which rules of IHL imposed limits on a specific operation, which was completely different from the question of which operations may amount to an ‘armed attack’ and give rise to the right of self-defence under the UN Charter.

---

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

Moderator: Laurent Gisel, Head of the Arms and Conduct of Hostilities Unit, ICRC
Expert presentation: Papawadee Tanodomdej, Lecturer, Chulalongkorn University, Thailand

The main question dealt with by the framing presentation was how civilian electronic data were protected under IHL. This depended on whether civilian data could qualify as a ‘civilian object’ for the purpose of the IHL rules on the conduct of hostilities, which protect civilian objects. Those arguing that data were not an ‘object’ relied on the ordinary meaning of the term, i.e. something that was visible and tangible. Those arguing in favour of the opposite view invoked, among other things, the meaning of the term ‘object’ in French (les biens), which included tangible and intangible sub-categories and the definition of military objective that is understood to encompass locations or animals, neither of which are usually understood as being ‘objects’. Moreover, the interpretation of data as a non-object risked expanding the scope of permissible targets and exposing the civilian population to additional danger, in contravention of the object and purpose of IHL.

It was also noted that even if civilian data were not regarded as a civilian object, they were not necessarily unprotected under IHL. In the expert presenter’s view, the precautionary principle would prohibit the deletion of or tampering with civilian data, if doing so would cause incidental harm to civilians that would be excessive in relation to the anticipated concrete and direct military advantage.

One participant expressed the view that civilian data should be regarded as a civilian object under IHL. In response to a question about the measures states had taken to protect civilian data from being targeted, the expert presenter noted that that kind of information was difficult to obtain. Some states had incorporated rules on the protection of civilian data in their military manuals or published national positions. It was further noted that in light of the interconnectedness of cyberspace states may explore multilateral cooperation in data protection.

The discussion also highlighted a recent cyber attack against Medibank, a large health insurance provider in Australia. The attackers exfiltrated a significant amount of sensitive medical information and threatened to release the information on the dark web if a ransom was not paid. It was queried how such an operation would be addressed by IHL if it took place in the context of an armed conflict. The expert presenter opined that if the said cyber operation were governed by IHL, it would be directed against a civilian object in violation of the principle of distinction. Even though the data were themselves intangible, they were stored in a computer that was tangible in nature and undoubtedly an object. This logic also applied to data stored in the cloud, as such digital storage cannot exist without the physical infrastructure owned by the cloud company. In the ICRC’s view, regardless of whether such medical data constituted a civilian object, they were protected by the obligation to respect and protect medical facilities.
SESSION 5: THE MILITARY USE OF CYBERSPACE AND THE EFFECT ON ITS CIVILIAN CHARACTER

Moderator: Tilman Rodenhäuser, Legal Adviser, ICRC Geneva
Expert presentation: Professor Rain Liivoja, The University of Queensland, Australia

The framing presentation started with a technical description of cyberspace, which consists of a social layer (persons), a logical layer (software/data) and a physical layer (hardware/infrastructure). The focus of the presentation was the physical layer or cyber infrastructure and whether it could qualify as a military objective under IHL.

Article 52 of Additional Protocol I defines military objectives as objects that (1) by their nature, location, purpose or use, make effective contribution to military action and (2) whose total or partial destruction, capture or neutralization offers a definite military advantage. With regard to the first limb of the definition, military objectives may include military IT systems (‘by nature’) and internet infrastructure used by both civilians and the military (‘by use’). With regard to the second limb, it was noted that ‘definite military advantage’ did not necessarily require denying a particular capability; depending on the situation, this requirement may be met also by making communication slower and less reliable.

In order to determine whether an attack against a military objective was lawful, further consideration must be given to the principles of proportionality and precaution. With regard to the former, it was noted that it was still a subject of debate whether impact on data, loss of functionality of a targeted system and remote effects of the operation must be taken into account as collateral damage. Regarding the principle of precaution, Article 57 of Additional Protocol I sets out a long list of precautions in attack, which must also be implemented in the context of cyber operations that qualified as attacks.

Because of the interconnectedness of cyberspace, cyber operations can have repercussions beyond the territory of the targeted state. The expert presenter noted that if the harm in question was foreseeable, this would have to be considered in the proportionality analysis of the cyber operation. Moreover, the fact that it materialized abroad may have legal implications beyond IHL, in particular under the UN Charter.

Regarding the concurrent use of cyber infrastructure by civilians and the military, the expert presenter suggested that states should implement all feasible measures to prevent any impact on civilians, such as by keeping military and civilian infrastructure separate. Nevertheless, determining the feasibility of this requires a technical assessment.

As to how proportionality should be assessed for a ‘dual-use’ object, the expert presenter noted that there was no specific formula for balancing collateral harm with military advantage. This was a decision for the military commander, to be made on the basis of legal advice. The greater the extent and likelihood of collateral harm, the higher up the chain of command at which the decision would normally be taken. It was also noted that there were technical means that the military could use to limit civilian harm. These included testing cyber capabilities before deploying them and using technical measures such as system fencing, geo-fencing or a ‘kill switch’.

---

7 See also ICRC Customary Law Study, Rules 15–21.
A question was posed with regard to works and installations containing dangerous forces that were given specific protection under IHL. This rule may be relevant for cyber operations that could cause significant levels of harm foreseen in the relevant provision.

The potential impact of artificial intelligence (AI) was also discussed, as militaries increasingly relied on it. It was noted that the main concern with regard to AI is its self-learning and self-evolving capacities, which are often difficult for human beings to comprehend.

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

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

*Expert presentation: Tilman Rodenhäuser, Legal Adviser, ICRC Geneva*

Information or psychological operations have long existed in armed conflicts. They are commonly seen as a means to influence the views, attitudes or behaviour of adversaries or civilian populations in order to achieve military aims. Examples include misleading the adversary through ‘ruses of war’, influencing the political narratives accompanying the armed conflict, discrediting the enemy and recruiting new soldiers through propaganda. While these practices are often lawful under IHL, there are limits imposed by certain rules of IHL.

For example, digital communications used to encourage or fuel violence may contravene the obligation to ‘respect and ensure respect’ for IHL under Article 1 common to the four Geneva Conventions of 1949. The International Court of Justice has interpreted this provision to mean that parties to armed conflict must not encourage persons or groups to violate IHL. Publishing pictures of prisoners of war is also unlawful under Article 13(2) of the Third Geneva Convention. As explained in the ICRC’s updated commentary, this provision prohibits publication of pictures or videos of prisoners of war irrespective of the communication channel being used, thus including social media. Disinformation campaigns against impartial organizations that affect their operations may also violate the customary obligation to respect and protect humanitarian personnel and allow and facilitate the unimpeded passage of humanitarian relief.

In addition, certain information or psychological operations could arguably be regarded as attacks under IHL, in which case most of the conduct-of-hostilities rules were applicable. This particularly concerns information campaigns that cause destruction of objects or loss of life.

During the discussion, the expert presenter noted that rules derived from other fields of international law also addressed information or psychological operations. These included a specific prohibition against the incitement of genocide under international criminal law and the right to freedom of expression under international human rights law, which is understood as including the right to receive adequate or appropriate information.

With regard to the prohibition against exposure to public curiosity under IHL, it was clarified that IHL did not prohibit the online publication of pictures of soldiers who had not been detained or otherwise fallen into the power of the enemy.

---

9 Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the I the Protection of Victims of International Armed Conflicts (AP I), Art. 56; ICRC Customary Law Study, Rule 42.


The discussion also touched upon the role of private actors, such as social media companies, in mitigating information or psychological operations and whether they had IHL or human rights obligations. The expert presenter noted that IHL bound parties to armed conflict, including non-state armed groups and private individuals operating in the context of an armed conflict, whereas obligations under international human rights law were binding only on states. Nevertheless, it was generally accepted that private companies had a duty of due diligence. The example was given of a policy adopted by Twitter prohibiting the sharing on its platform of pictures and videos of prisoners of war.

Responding to a question on this issue, the expert presenter highlighted that the truthfulness of an information or psychological operation was not always relevant in determining its legality. For example, publishing pictures of prisoners of war was unlawful, regardless of whether it conveyed false messages. Conversely, truthfulness or falsity would be relevant in the case of an information operation that accused a humanitarian organization of not being neutral, thereby endangering its humanitarian operations.

SESSION 7: NATIONAL POSITIONS ON INTERNATIONAL LAW AND CYBERSPACE: PRACTICAL ASPECTS

*Moderator:* Tilman Rodenhäuser, Legal Adviser, ICRC

*Introductory presentations:*
- Triinu Kallas, Legal Adviser, Legal Division of the Ministry of Foreign Affairs of Estonia
- Angad Keith, Assistant Director, International Law and Security Section of the Legal Division of the Department of Foreign Affairs and Trade of Australia
- Harditya Suryawanto, Counsellor, Directorate of International Security and Disarmament of the Ministry of Foreign Affairs of the Republic of Indonesia
- Naushyn Janah, Legal Adviser, Legal Division of the Ministry of Foreign Affairs and Trade of New Zealand

*Ms Kallas* opened the session by presenting the decision-making process behind the adoption of Estonia’s national position on international law applicable to cyberspace. Estonia was a member of the UN GGE and had always been an active advocate for the applicability of international law in cyberspace. In light of the multilateral discussions, there was a need to further develop Estonia’s understanding of how international law applied in cyberspace. The rise in malicious activities in cyberspace made it even more urgent to develop such understanding. Estonia began to develop its national position in August 2018, the process being initiated by its president and guided by the question of how it should react to malicious cyber activities that may or may not amount to the use of force.

The Ministry of Foreign Affairs was responsible for coordinating this task between several ministries and their subsidiary authorities. The team involved legal, political and technical experts and consulted academics and the private sector. The entire process was closely followed by the president.

While discussing the substance, including specific areas of international law to focus on, the team’s primary resource was the *Tallinn Manual*. It took nine months for the national position to be adopted.12

---

12 The national position was delivered in the President’s speech at the opening of CyCon 2019. See also Estonia’s national position 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), pp. 23–30.
Mr Keith emphasized that in Australia’s view, it was essential for states to articulate their positions on how international law, including IHL, applied to cyberspace. It was a means to increase accountability, stability and trust in cyberspace.

The legal teams of the Department of Foreign Affairs and Trade and the Attorney-General’s Department worked closely together in developing national positions on the application of international law to cyberspace. During this process, the Department of Defence and policy experts were also consulted, including the Ambassador for Cyber Affairs and Critical Technology.

Australia had published a series of national positions in 2017, 2019 and 2021, the last of which was included in the 2021 UN GGE official compendium of voluntary national contributions by participating governmental experts on the subject of how international law applied to the use of ICT.

Mr Suryawanto stated that Indonesia was currently developing its national position. Indonesia recognized the fundamental importance of acknowledging the application of international law in cyberspace. The UN Charter principles, including sovereignty, non-intervention, peaceful settlement of disputes and respect for human rights did apply in the use of ICT.

While the UN GGE had made some headway by affirming the application of international law, there remained some gaps in the details. Further interpretation and clarification were needed, as international law could not automatically be applied to the unique context of cyberspace.

Beginning in 2019, the Ministry of Foreign Affairs had engaged in discussions with other relevant ministries and stakeholders. The government shared the view that cyberspace was not a lawless domain. In Indonesia’s view, IHL applied to states’ behaviour in cyberspace during armed conflict and that in no way legitimized cyber warfare.

Ms Janah echoed the previous speakers’ view that national positions offered values of clarity and certainty. New Zealand issued its national position on the application of international law to state’s activities in cyberspace in December 2020.

The UN GGE and the UN Open–Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (OEWG) were strong drivers for New Zealand to clarify its thinking and articulate a clear national position. The position was developed by an inter-agency working group, led by the Ministry of Foreign Affairs and Trade. The domestic agencies involved include the Cabinet, the National Cyber Security Centre, the New Zealand Police, the New Zealand Defence Force and the Crown Law Office. The private sector and industry were informed of the process.

The team consulted other states’ national positions and practices and deliberated a broad range of international law and policy considerations. The whole process took nearly a year. While it was challenging to coordinate and accommodate different perspectives across government agencies, it was important to make sure that the final product was relevant for the government.

15 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), pp. 3–17.
16 New Zealand’s Position on the Application of International Law to State Activity in Cyberspace, 2020, available in www.dpmc.govt.nz
During the discussion, experts shared insights into the process of seeking input from technical experts. For example, Indonesia’s Ministry of Foreign Affairs had consultations with the National Cyber and Crypto Agency. Estonia’s Ministry of Foreign Affairs, which also consulted technical experts, saw this step as an important part of the process, as the lawyers needed to apply the law in light of the state’s degree of digitalization.

To identify specific areas of international law to be covered in the national position, Estonia used the Tallinn Manual and the guiding question provided by its president (i.e. how Estonia would react to hostile cyber operations) as a starting point. Australia decided on the basis of issues often encountered nationally and topics discussed in multilateral processes. Similarly, New Zealand considered a broad range of issues and identified the most relevant ones, based on input from national agencies and multilateral discussions. It was queried whether states with developed national positions had considered the risk of fragmenting international law by publishing their national positions. Presenting state representatives took the view that publishing national positions helped to build common ground and did not risk fragmentation. As with other issues, disagreement about interpretations with regard to cyberspace was inevitable. Moreover, it was stated, states generally agreed on the baseline: it was the details that they needed to discuss further. Having national positions could facilitate this discussion.

Some attention was also given to the norms, rules, and principles of responsible state behavior in cyberspace, within the context of international security. It was generally agreed that they were voluntary norms that complemented existing international legal obligations.

**SESSION 8: MULTILATERAL DISCUSSIONS ON CYBER OPERATIONS DURING ARMED CONFLICT**

**Moderator:** Harditya Suryawanto, Counsellor, Directorate of International Security and Disarmament, Ministry of Foreign Affairs of the Republic of Indonesia

**Expert presentations:**
- Professor Johanna Weaver, Director of the Tech Policy Design Centre, Australian National University; formerly Australia’s independent expert and lead cyber negotiator at the United Nations
- Professor Zhixiong Huang, Institute of International Law, Wuhan University, China; Special Rapporteur of the Working Group on International Law in Cyberspace, the Asian–African Legal Consultative Organization (AALCO)

**Professor Weaver** opened the session by recalling discussions in the UN GGE and the UN OEWG, particularly in relation to the acknowledgement of IHL application in cyberspace. In 2013, the UN GGE acknowledged the application of international law in cyberspace,17 and in 2015, it noted the principles of humanity, proportionality, and distinction, albeit without mentioning IHL explicitly.18 Finally, in 2021, the UN GGE achieved explicit recognition of IHL application to cyber operations in situations of armed conflict, in a report that was welcomed by every UN member state in the UN General Assembly.19

---

The expert presenter acknowledged that this recognition was hard fought. One of the key concerns that had to be resolved during the UN GGE negotiations was that such acknowledgment would encourage the use of ‘cyber weapons’ in cyberspace. In her view, one of the best responses was that this was equivalent to saying that enforcing speed limits encouraged drivers to drive at high speed. Another concern was that further study was required to determine whether cyber tools could qualify as weapons to which IHL applies. The UN GGE report overcame these concerns by acknowledging “the need for further study on how and when IHL applies to cyber operations” and recalling “the principles of humanity, necessity, proportionality and distinction” while underscoring “that recalling these principles by no means legitimizes or encourages conflict”.

Professor Huang then made a presentation about the multilateral discussions at the AALCO. The topic of cyber operations was introduced to the agenda during the 53rd session in 2014. A working group on international law in cyberspace was formed during the 54th session in 2015. At the working group’s meeting in September 2019 – on the topic of peaceful use of cyberspace – the delegations discussed the application of IHL to cyber operations during armed conflict.

In a non-binding document titled “Consensual basic principles of international law applicable in cyberspace”, which was submitted in 2019 and revised in 2021, states were encouraged to “cooperate to regulate military use of cyberspace so as to safeguard respect for fundamental principles of international law in time of armed conflict”.20

Professor Huang said that states’ views on the application of IHL in cyberspace could be divided into three categories: (1) states that endorse or advocate the application of IHL in cyberspace; (2) states that generally accept the application of IHL but are of the opinion that some significant issues remain unresolved; and (3) states that take a prudent attitude towards the application of IHL. States in the last group oppose the militarization of cyberspace and a cyber arms race and worry that the ‘digital gap’ between developing and developed countries would put the former in a disadvantageous position in the discussion about IHL application in cyberspace and in the potential development of IHL rules and principles.

During the discussion, one expert presenter emphasized that all UN member states had endorsed the application of IHL in cyberspace, based on the UN General Assembly’s endorsement of the 2021 UN GGE report. What needed to be discussed was not whether, but how, IHL applied to cyber operations during armed conflict. It was important that states shared their national positions on this subject, to increase predictability.

However, the other expert presenter noted that some states – including in the Asia-Pacific region – were reluctant to discuss IHL application in cyberspace. The novelty of cyberspace and its unique nature or characteristics could make any discussion of the subject a complicated affair. In response, it was argued that not articulating how the law applied will not stop states from resorting to cyber operations, which has been a reality for some time now.

The expert presenters agreed that there was a need to build bridges and work towards consensus. They also noted that whereas the UN OEWG could offer a platform to achieve such progress, securing any agreement in this forum could be difficult. Publication of national positions and a database that collected them would be helpful in this regard. The ICRC highlighted the Cyber Law Toolkit as an example of such a database.21

---

20 AALCO, International Law in Cyberspace, AALCO/58/ DAR ES SALAAM /2019/ SD/17, p. 26, para. 2.0(h).
21 See https://cyberlaw.cccdce.org/wiki/Main_Page.
ANNEX 1: LIST OF PARTICIPATING STATES

- Australia
- China
- India
- Indonesia
- Iran
- Japan
- Malaysia
- New Zealand
- Pakistan
- Singapore
- Thailand
ANNEX 2: BACKGROUND PAPER

The aim of the regional consultation is to facilitate a dialogue between states in the Asia-Pacific region on international humanitarian law (IHL) and cyber operations, with a view to fostering the exchange of views and developing a common understanding of how and when IHL applies to the use of information and communication technologies (ICT) during armed conflicts. The purpose of this background document is to provide relevant material and food for thought to support the discussions during the event. It does not necessarily reflect the views or positions of any of the organizers.

Discussions during the event will focus on selected issues in connection with the specific question of the application of IHL in the context of cyber operations, with a view to hearing the position of the participating experts on these issues, 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 on the understanding that the opinions expressed will not be attributed to the meeting’s participants, also known as the ‘Chatham House rule’. Individual sessions will be chaired by experts from the organizers. A report summarizing the discussions will be prepared after the event and published by the organizers. The report will include the list of participating countries, but the substance of the discussion will be reported without attribution.

1 INTRODUCTION

The use of cyber operations during armed conflicts is a reality today. 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. Like any other means and methods of warfare, cyber operations have the potential to seriously affect civilian infrastructure and harm human beings. They also raise a number of questions about precisely how certain rules of IHL – which were drafted before the emergence of cyber operations as a means or method of warfare – apply to and impose limits on 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 – including cyber operations – during an armed conflict. 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, which form the basis for its engagement with states in this matter and which have informed the preparation of this document.

Indonesia views it as important and timely to reflect on the humanitarian consequences of cyber operations in the Asia-Pacific region. Our increasing dependence on technologies demands a clear legal framework to ensure responsible behaviour in cyberspace and protect civilians from harmful cyber operations. But the nature of cyber operations represents a challenge when interpreting rules originally designed with a focus on regulating physical forms of violence. The present consultation is a good opportunity to express our opinions concerning future regulation of cyber capabilities.

This background document first briefly sets 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 when IHL applies to cyber operations and how it relates to the prohibition against the use of force under the UN Charter and customary international law (Section 3). It then zooms in on four specific issues related to how IHL principles and rules apply to cyber operations during armed conflict (Section 4; this section is accompanied by brief scenarios...
that will be used to complement the discussion). Finally, the document covers the practical issue of preparing state position papers on international law and cyber operations (Section 5) and current multilateral processes to build a common understanding of how IHL applies to cyber operations during armed conflict.

2 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 security and military strategies 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”.

In recent years, societies have become largely dependent on ICT, a process only accelerated by the COVID-19 pandemic. While the benefits of increased interconnectivity, and the opportunities created by it, are countless, increased dependency also implies increased vulnerability. While 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. These risks are compounded by the interconnectivity that characterizes cyberspace, which means that anything that 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 for various other systems, regardless of where those systems are located.

There is a real risk that cyber tools – either deliberately or by mistake – may have large-scale and diverse effects on critical civilian infrastructure, such as essential industries, telecommunications, and transport, governmental and financial systems. Cyber operations conducted in 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. As one cyber-security expert put it, such military operations constitute a “humanitarian crisis in the making”.

Cyber operations can harm infrastructure in at least two ways. First, they can disrupt the delivery of essential services to civilians, as has been shown by cyber operations against electrical grids, the health-care sector, and other infrastructure. 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 of escalation and related human harm because it may be difficult for the targeted party to know whether the attacker’s aim is intelligence collection or something more harmful, such as disrupting or destroying an asset. The target may therefore react with greater force than necessary out of anticipation of a worst-case scenario.

23 ICRC position paper, supra note 1, p. 3 fn. 1.
24 See further ICRC, The potential human cost of cyber operations (May 2019).
25 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. For some discussion, see Laurent Gisel and Lukasz Olejnik, “The Potential Human Cost of Cyber Operations: Starting the Conversation”, Humanitarian Law and Policy Blog, 14 November 2018.
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.

There is a multiplication and diversification of actors at work in the context of cyber operations during armed conflict. Some types of operation can be conducted with easily accessible tools available to technology-savvy civilians. Other operations require expertise that is normally found in different state agencies (the armed forces, intelligence agencies), but also in certain technology companies. The multiplication and diversification of actors operating in cyberspace risks leading to the participation in conflict of actors that are not aware of or trained in the limits imposed by IHL.

A further concern is the difficulty of reliably attributing 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. 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.

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 applicable international law.

3 THE PROHIBITION AGAINST THE USE OF FORCE UNDER THE UN CHARTER AND ‘WHEN’ IHL APPLIES TO CYBER OPERATIONS DURING ARMED CONFLICT

States have repeatedly reaffirmed that international law, and in particular the UN Charter, is applicable to the use of ICT, most recently in the 2021 reports of the UN Open-Ended Working Group (OEWG) and the UN Group of Governmental Experts (GGE). The 2021 UN GGE report also expressly referred to IHL in the cyber context, noting that this branch of international law “applies only in situations of armed conflict” and “that recalling [IHL] principles by no means legitimizes or encourages conflict”. The reports thus affirmed the prohibition against the use of force as set out in the UN Charter and noted that in situations of armed conflict additional rules apply.

From a legal point of view, the prohibition against the use of force under the UN Charter and customary international law (jus ad bellum) is separate from the IHL rules applicable during armed conflict (jus in bello). In the event of a cyber operation conducted by one state against another state, the two fields of law serve different — but complementary — purposes.

Under the UN Charter, states have an obligation to “settle their international disputes by peaceful means in such a manner that international peace and security, and justice, are not endangered”. A state is prohibited from using force against another state except in case of self-defence and when authorized by the UN Security Council. States have repeatedly reaffirmed their commitment to several of these principles of the UN Charter and international law. Different views exist, however, on which cyber operations may be

28 ICRC position paper, supra note 1, p. 8.
31 Ibid. para. 71(f).
32 Charter of the United Nations, Article 2(3).
regarded as the “use of force” under the UN Charter.\textsuperscript{33} Determining whether a state violated the UN Charter by conducting a cyber operation can have specific legal consequences, for instance, whether an internationally wrongful act has been committed, or whether the victim state may take counter measures or act in self-defence.\textsuperscript{34} While these are critical aspects of the discussion on the application of international law and cyberspace, they are outside the scope of this consultation, which focuses on IHL.

The legal assessment of a cyber operation under IHL serves a different purpose. States adopted IHL treaties with the objective of “protecting the victims of armed conflict”.\textsuperscript{35} These rules are designed to impose limits on military operations during armed conflict, with a view to minimizing the humanitarian consequences of armed conflict, whether caused by kinetic or other means.

States recognized the need for further studying how and when IHL applies to the use of ICT by states. With regard to ‘when’ it applies, states clarified that this is the case “only in situations of armed conflict”. Thus, if a cyber operation is conducted in the context of an armed conflict in conjunction with and in support of more traditional military operations, in the ICRC’s view there can be no question that IHL applies to, and therefore limits, such cyber operations.\textsuperscript{36} This is likely to be the most frequently occurring situation; indeed, the few acknowledgments made by states of the use of cyber operations during armed conflict were in the framework of such types of situation. Whether cyber operations alone may be regarded as triggering the application of IHL, and the limits it affords, is to be assessed according to IHL rules on conflict classification. In accordance with Article 2, paragraph 1(1) common to the four Geneva Conventions of 1949, IHL applies “to all cases of declared war or of any other armed conflict which may arise between two or more of the High Contracting Parties”, the latter being commonly understood as being the case “whenever there is a resort to armed force between states”.\textsuperscript{37} Therefore, cyber operations, on their own, have in principle the potential to amount to a resort to armed force that is subject to IHL, for instance, if cyber operations have effects similar to those of traditional kinetic operations.\textsuperscript{38} Such a cyber operation would also have to be analysed under various other rules of international law, and may in particular violate state sovereignty, the prohibition of non-intervention, or the prohibition against the threat or use of force under the UN Charter.

In conclusion, while the UN Charter sets out a prohibition against the use of force, IHL imposes limits on military operations during armed conflict, with a view to minimizing the humanitarian consequences of armed conflict, whether caused by kinetic or other means.

\textsuperscript{33} Some have asserted that cyber operation can qualify as “use of force” if its effects are similar to those that result from the use of conventional weapons. See e.g. Australian Government, Australia’s position on how international law applies to state conduct in cyberspace: Brazil’s position as incorporated in UNGA, Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communication technologies by states, A/76/136, August 2021, p. 19; 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), para. 1 of the commentary on Rule 69. Some others have stated that a cyberoperation without physical effects may also be characterised as a use of force. See e.g. French Ministry of the Armies, International Law Applied to Operations in Cyberspace, 2019, p. 3; Dutch Ministry of Foreign Affairs, Letter to the Parliament on the International Legal Order in Cyberspace, 5 July 2019, p. 4.

\textsuperscript{34} Multilateral discussions have also shown, however, that certain questions of international law require further clarification, which include, inter alia, the kind of ICT-related activity that might be interpreted by other states as a threat or use of force (Art. 2(4) of the Charter) or that might give a state cause to invoke its inherent right to self-defense (Art. 51 of the Charter). Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, Chair’s Summary, para. 18.


\textsuperscript{36} ICTRC position paper, supra note 1, p. 4.


\textsuperscript{38} Ibid., paras 253–256; Tallinn Manual 2.0, supra note 12, para 16 of the commentary on Rule 82.

\textsuperscript{39} Gisel, Rodenhäuser and Dörmann, supra note 1, pp. 306–308.
construed as legitimizing or authorizing any act of aggression or any other use of force inconsistent with the Charter of the United Nations”; in other words, IHL cannot serve as a justification for a violation of the UN Charter.

Questions to consider

- Legally speaking, can affirming that IHL limits cyber operations during armed conflicts legitimize cyber operations that would be carried out in violation of the UN Charter?
- When does IHL apply to and limit cyber operations? Can cyber operations alone constitute a ‘resort to armed force’ and therefore be subject to the limits imposed by IHL, and if yes, what types of operation?

4 SPECIFIC QUESTIONS ON ‘HOW’ IHL APPLIES TO CYBER OPERATIONS DURING ARMED CONFLICT

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

(a) 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. The notion of ‘attack’ under IHL – defined in Article 49 of Protocol I of 8 June 1977 additional to the Geneva Conventions (Additional Protocol I) – is different from and should not be confused with the notion of ‘armed attack’ under Article 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 operation, amounts to an ‘attack’ under IHL does not necessarily mean that it would qualify as an ‘armed attack’ under the UN Charter.

Concretely, under IHL rules such as the prohibition against attacks on civilians and civilian objects, the prohibition against 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’ under 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 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 themselves violent.

It is also widely accepted that cyber operations expected to cause death, injury or physical damage constitute ‘attacks’ under IHL. Some states have clarified that this includes harm due to the foreseeable direct

40 AP I, preamble.
and indirect (or reverberating) effects of an ‘attack’; for example, the death of patients in intensive-care units caused by a cyber operation against an electricity network that results in the cutting off of a hospital’s electricity supply – a view shared by the ICRC.

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’ under 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, regardless of 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 – an electrical, banking, or communications network, for instance – 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 to protect civilians from the effects of hostilities.

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 on the protection of civilians against the effects of cyber operations. For the moment, opinions vary among the states that have taken public positions.

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

---


43 ICRC position paper, supra note 1, p. 7.

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

to spare the civilian population, civilians and civilian objects”. 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. Its applicability to cyber operations has been expressly reaffirmed by several states.

On the other hand, some rules of IHL afford specific protection to certain categories of person and object 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”. 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. 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’.

Questions to consider

- Can cyber operations qualify as ‘attacks’ under IHL? Which ones? Are indirect (or reverberating effects) also relevant for this determination/assessment?
- Can cyber operations that are not expected to cause physical damage directly or indirectly, but that are expected to disable ICT infrastructure, qualify as ‘attacks’ under IHL?
- What protection does IHL afford with respect to those operations that do not qualify as ‘attacks’ under IHL? Is this protection sufficient?

---


49 AP I, Art. 53(2); 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. 12; ICRC Customary Law Study, supra note 25, Rule 52.

50 Gisel, Rodenhäuser and Dörmann, supra note 1, p. 327.
Scenario 1: The notion of ‘attack’ under IHL

This scenario aims to provide a practical example to support participants’ discussions during the session and should be considered together with the guiding questions.

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 in computers of important government agencies, notably the armed forces, but also by 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 used by the government-owned electricity provider, and that the disruption of the computers used by the government-owned electricity provider will lead to power 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 power cuts affecting hospitals’ intensive-care units.

(b) THE PROTECTION AFFORDED TO CIVILIAN ELECTRONIC DATA UNDER IHL

Certain kinds of 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 digitized 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 object that enjoy specific protection under IHL, the protective rules are comprehensive. In particular, the obligations to respect and protect medical facilities and humanitarian relief operations must be understood as extending to medical data belonging to those facilities and to the data of humanitarian organizations that are essential for their operations. Similarly, it is prohibited to delete or otherwise tamper 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.

Still, it is important to clarify the extent to which civilian data are protected by the existing general rules on the conduct of hostilities. This debate has critical consequences for the protection of a wide range of civilian data that fall outside the specific protection just mentioned but are nonetheless essential for the sound functioning of societies. The debate has been shaped by the question of whether data constitute

---

51 See, for instance, Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, Art. 20; 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 (GC IV), Art. 12; AP I, Art. 70(4), 71(2); ICRC Customary Law Study, supra note 25, Rules 25, 28, 29.

52 See e.g. AP I, Arts 70(4), 71(2); ICRC Customary Law Study, supra note 25, Rules 21 and 22.

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

objects as understood under IHL, in which case cyber operations against data (such as deleting or damaging them) would notably be 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.55 Some states also subscribe to this view.56

By contrast, others have argued that either all or some types of data should be regarded as objects under IHL. One view, taken by several states, is that the protection of civilian objects extends to civilian data.57 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.58 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 locations and animals as well.59 Another approach, thus far endorsed by one state, is to consider content data as protected under the principle of distinction, leaving to the side whether other types of data (such as ‘operational data’) qualify as objects or not.60

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 not decrease the protection that IHL affords to them.61 In essence, excluding essential civilian data from the protection afforded by IHL to civilian objects would result in an important protection gap.

55 See Tallinn Manual 2.0, supra note 12, 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).


57 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, A/76/136, 13 July 2021, p. 78; Norway, Manual i krigens folkerett, 2013, para. 9.58.


59 Gisel, Rodenhäuser and Dörmann, supra note 1, p. 319.


Questions to consider

- Does the specific protection IHL affords to certain categories of object (such as medical units, humanitarian relief or objects indispensable to the survival of the population) extend to their data?
- Do civilian data in general, or some specific types of civilian data (such as content data or operational data), qualify as a ‘civilian object’ for the purposes of IHL, or otherwise enjoy protection similar to that afforded by IHL to civilian objects?
- If certain civilian data are not regarded as protected in the same way as ‘civilian objects’, what IHL rules limit cyber operations against them? Is this protection sufficient?

Scenario 2: Protection of data against damage or destruction

This scenario aims to provide a practical example to support participants’ discussions during the session and should be considered together with the guiding questions.

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. As expected by state A, 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 for non-military purposes, including census-taking, provision of social benefits, voting and taxation. As expected by state A, 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 healthcare to members of state B’s armed forces, military retirees and family members. As expected by state A, the operation results in the deletion of all the personal medical data of patients treated in the hospital since the beginning of the armed conflict.

(c) 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. One challenge for this lies, however, in the interconnectedness of civilian and military networks.

Except for some specific military networks, cyberspace is used predominantly 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 infrastructure.61

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

---

62 Gisel, Rodenhäuser and Dörmann, supra note 1, pp. 320–322.
circumstances ruling at the time, offers a definite military advantage. All objects that are not military objectives under this definition are civilian objects under IHL and must not be the object of an attack or of reprisals. 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.

It is traditionally understood that an object may become a military objective under IHL 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’). 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.

As indicated, not every use for military purposes renders a civilian object a military objective under IHL. Clarifying the extent to which the use by the military of a predominantly civilian object in cyberspace turns this object into a military objective, and thus strips it of the protection afforded to civilian objects by IHL, is therefore critical in ensuring the protection of the civilian population that relies on these objects.

Questions to consider

- Can cyber infrastructure that is used for civilian and military purposes become a ‘military objective’ as defined in IHL and therefore not be protected against attack?
- 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 (one of the two criteria for classifying an object as a ‘military objective’ under IHL)?
- If a particular element of cyber infrastructure has become a military objective, but is simultaneously used for civilian purposes (‘dual use’), how do the effects on the civilian use have to be regarded under the prohibition against indiscriminate attacks, and the rules of proportionality and precaution in attack, when considering an attack on that objective?

63 AP I, Art. 52(2); ICRC Customary Law Study, supra note 25, Rules 2–8.
64 AP I, Art. 52(3); ICRC Customary Law Study, supra note 25, Rule 6.
65 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 25, Rule 10, commentary pp. 35–36.
66 See e.g. ICRC Customary Law Study, supra note 25, Rule 10, commentary p. 32; Tallinn Manual 2.0, supra note 12, para. 1 of the commentary on Rule 101.
67 Gisel, Rodenhäuser and Dörmann, supra note 1, p. 321.
Scenario 3: Dual-use objects in the ICT environment

This scenario aims to provide a practical example to support participants’ discussions during the session and should be considered together with the guiding questions.

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 coordination 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 purpose of coordinating 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.

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

‘Information operations’ have long been part of armed conflicts.68 With the rapid growth of information and communication technology over the past decade, the scale, speed and reach of information or psychological operations have increased significantly, raising concerns about their possible humanitarian impact.69

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 civilians an effective advance warning of an attack or help direct them to safety.

Conversely, other information or psychological operations are designed to cause confusion or harm, or to support the war effort and public perceptions of a party to 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 in order to influence domestic and international audiences, to discredit other parties to 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.70

---

68 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.

69 Ibid. p. 10.

70 For an analysis of possible human harm, see ICRC, Harmful Information: Misinformation, Disinformation and Hate Speech in Armed Conflict and Other Situations of Violence, 2021. For an overview of reported usages of information operations in contemporary armed conflicts, see Minority Rights Group International, Peoples under Threat 2020; see also Graphika, French and Russian Influence Operations Go Head to Head Targeting Audiences in Africa, 2020.
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 IHL and that “psychological operations directed at the civilian population have been a feature of warfare for centuries.” 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.

Broadly speaking, IHL contains two types of rules that address information or psychological operations during armed conflict. First, there are a few rules that address directly certain types of operation. This category includes the prohibition against acts or threats of violence the primary purpose of which is to spread terror among the civilian population, and the use of “misinformation” as a lawful ruse of war. IHL also prohibits using “pressure or propaganda which aims at securing voluntary enlistment” of protected persons in occupied territories.

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

On a number of these issues, IHL provides clear and well-established limits that apply in information operations. For others, however, further analysis and clarification is needed.

---

**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 ascertain whether they would actually trigger specific instances of IHL violation?
- 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 (i.e. disinformation leading civilians into a mine field) governed by the principles of distinction, proportionality and precaution?

---

74 AP I, Article 39(2); AP II, Article 13(2); ICRC Customary Law Study, supra note 25, Rule 2.
75 AP I, Article 33(2).
76 GC IV, Article 51.
77 Common Article 1 of the 1949 Geneva Conventions; ICRC Customary Law Study, supra note 25, Rules 139 and 144.
Scenario 4: Digital information operations

This scenario aims to provide a practical example to support participants’ discussions during the session and should be considered together with the guiding questions.

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 physical punishment. Subsequently, many individuals belonging to that group are subjected 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 civilians 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 morale among civilians and their support for state B’s war effort.

5 STATE POSITION PAPERS ON INTERNATIONAL LAW AND CYBER OPERATIONS: PRACTICAL ASPECTS

This session will focus on the procedural and policy aspects of drafting public position papers on international law and cyber operations. As more and more states have begun to express their positions on how international law applies in cyberspace, this discussion will mainly aim at giving an overview of how to develop these positions on a national level.79 It will include best practices on how to organize the relevant discussions, whom to consult, what kind of information to collect and what topics to address.

79 For a collection of publicly available positions on how international law applies in cyberspace, see Cyber Law Toolkit.
ANNEX 3: AGENDA

DAY 1: TUESDAY, 29 NOVEMBER 2022

11:45–12:00: Welcome and introduction

Caka Averdi Awal, Director of International Security and Disarmament, Ministry of Foreign Affairs of the Republic of Indonesia

Dorothea Krimitsas, Deputy Head of the Regional Delegation for Indonesia and Timor-Leste, ICRC

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

12:00–12:45: Digital operations during armed conflict: Current realities

Moderator: Harditya Suryawanto, Counsellor, Directorate of International Security and Disarmament, Ministry of Foreign Affairs of the Republic of Indonesia

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

12:45–13:45: The prohibition against the use of force under the UN Charter and ‘when’ IHL applies to cyber operations during armed conflict

Moderator: Kubo Mačák, Legal Adviser, ICRC

Expert presentations:
(1) Benjamin Ang, Deputy Head of Centre of Excellence for National Security; Coordinator of the Cyber and Homeland Defence Programme, Singapore
(2) Tilman Rodenhäuser, Legal Adviser, ICRC

13:45–14:00: Coffee break

14:00–14:45: The notion of ‘attack’ under IHL and the protection of civilian objects

Moderator: Tilman Rodenhäuser, Legal Adviser, ICRC

Expert presentation: Professor Yoo Joon-Koo, Institute of Foreign Affairs and National Security, Republic of Korea

14:45–15:30: The protection afforded to civilian electronic data under IHL

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

Expert presentation: Papawadee Tanodomdej, Lecturer, Chulalongkorn University, Thailand
DAY 2: WEDNESDAY, 30 NOVEMBER 2022

11:45–12:30: The military use of cyberspace and the effect on its civilian character
Moderator: Tilman Rodenhäuser, Legal Adviser, ICRC
Expert presentation: Professor Rain Liivoja, The University of Queensland, Australia

12:30–13:00: Limits on the conduct of information or psychological operations during armed conflicts
Moderator: Laurent Gisel, Head of the Arms and Conduct of Hostilities Unit, ICRC
Expert presentation: Tilman Rodenhäuser, Legal Adviser, ICRC

12:00–13:15: Coffee break

13:15–14:15: National positions on international law and cyberspace: Practical aspects
Moderator: Tilman Rodenhäuser, Legal Adviser, ICRC
Introductory presentations: Australia, Indonesia, New Zealand, Estonia

14:15–15:00: Multilateral discussions on cyber operations during armed conflict
Moderator: Harditya Suryawanto, Counsellor, Directorate of International Security and Disarmament, Ministry of Foreign Affairs of the Republic of Indonesia
Expert presentations:
(1) Professor Johanna Weaver, Director of the Tech Policy Design Centre, Australian National University; formerly Australia’s independent expert and lead cyber negotiator at the United Nations
(2) Professor Zhixiong Huang, Institute of International Law, Wuhan University, China; Special Rapporteur of the Working Group on International Law in Cyberspace, the Asian–African Legal Consultative Organization (AALCO)
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.