International Review of the Red Cross (2020), **102** (913), 481–492.
Digital technologies and war
doi:10.1017/S1816383120000478

IRRC

REPORTS AND DOCUMENTS

International humanitarian law and cyber operations during armed conflicts

ICRC position paper submitted to the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security and the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, November 2019

Executive summary

- **Cyber operations have become a reality in contemporary armed conflict**. The International Committee of the Red Cross (ICRC) is concerned by **the potential human cost** arising from the increasing use of cyber operations during armed conflicts.

- **In the ICRC's view, international humanitarian law (IHL) limits cyber operations during armed conflicts** just as it limits the use of any other weapon, means or method of warfare in an armed conflict, whether new or old.
- Affirming the applicability of IHL does not legitimize cyber warfare, just as it does not legitimize any other form of warfare. **Any use of force by States – cyber or kinetic – remains governed by the Charter of the United Nations and the relevant rules of customary international law**, in particular the prohibition against the use of force. International disputes must be settled by peaceful means, in cyberspace as in all other domains.
- It is now critical **for the international community to affirm the applicability of international humanitarian law** to the use of cyber operations during armed conflicts. The ICRC also calls for discussions among governmental and other experts on *how* existing IHL rules apply and whether the existing law is adequate and sufficient. In this respect, the **ICRC welcomes the intergovernmental discussions** currently taking place in the framework of two United Nations General Assembly mandated processes.
- Events of recent years have shown that cyber operations, whether during or outside armed conflict, can disrupt the operation of critical civilian infrastructure and hamper the delivery of essential services to the population. **In the context of armed conflicts, civilian infrastructure is protected against cyber attacks by existing IHL principles and rules,** in particular the principles of distinction, proportionality and precautions in attack. IHL also affords special protection to hospitals and objects indispensable to the survival of the civilian population, among others.
- **During armed conflicts, the employment of cyber tools that spread and cause damage indiscriminately is prohibited.** From a technological perspective, some cyber tools can be designed and used to target and harm only specific objects and to not spread or cause harm indiscriminately. However, the interconnectivity that characterizes cyberspace means that whatever has an interface with the Internet can be targeted from anywhere in the world and that a cyber attack on a specific system may have repercussions on various other systems. As a result, there is a real risk that cyber tools are not designed or used – either deliberately or by mistake – in compliance with IHL.
- **States' interpretation of existing IHL rules will determine the extent to which IHL protects against the effects of cyber operations**. In particular, States should take clear positions about their commitment to interpret IHL so as to preserve civilian infrastructure from significant disruption and to protect civilian data. The availability of such positions will also influence the assessment of whether the existing rules are adequate or whether new rules may be needed. If States see a need to develop new rules, they should **build on and strengthen the existing legal framework – including IHL**.

1. Introduction

The use of cyber operations during armed conflicts is a reality.[1] 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.

Moreover, there have been significant technological advances in offensive cyber capabilities: in recent years, cyber operations have shown that they can seriously affect civilian infrastructure and might result in human harm.

In line with its mission and mandate, the International Committee of the Red Cross (ICRC) is primarily concerned with cyber operations used as means and methods of warfare during an armed conflict and the protection that international humanitarian law (IHL) affords against their effects.

The ICRC welcomes the intergovernmental discussions currently taking place in the framework of the two United Nations General Assembly mandated processes, namely the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security and the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security. Both groups are mandated to study "how international law applies to the use of information and communications technologies by States".[2] The ICRC submits this position paper to both groups to support States' deliberation on this matter.

This position paper is limited to legal and humanitarian questions arising from the use of cyber operations during armed conflict. It does not address questions relating to the legal framework applicable to cyber operations unrelated to armed conflict.

2. The potential human cost of cyber operations

During armed conflict, cyber operations have been used in support of or alongside kinetic operations. The use of cyber operations may offer alternatives that other means or methods of warfare do not, but it also carries risks. On the one hand, cyber operations have the potential to enable parties to armed conflicts to achieve their military aims without harming civilians or causing physical damage to civilian infrastructure. On the other hand, recent cyber operations – which have been mostly conducted outside the context of armed conflict – show that

1 In this position paper, the term "cyber operations during armed conflicts" is used to describe operations against a computer, a computer system or network, or another connected device, through a data stream, when used as a means or method of warfare in the context of an armed conflict. Cyber operations rely on information and communication technologies.

2 UNGA Res. 73/27, "Developments in the Field of Information and Telecommunications in the Context of International Security", UN Doc. A/RES/73/27, 5 December 2018, op. para. 5; UNGA Res. 73/266, "Advancing Responsible State Behaviour in Cyberspace in the Context of International Security", UN Doc. A/RES/73/266, 22 December 2018, op. para. 3.

sophisticated actors have developed the capability to disrupt the provision of essential services to the civilian population.

By means of cyber operations, it is possible for belligerents to infiltrate a system and collect, exfiltrate, modify, encrypt or destroy data. It is also possible to trigger, alter or otherwise manipulate processes controlled by a compromised computer system. A variety of "targets" in the real world can be disrupted, altered or damaged, such as industries, infrastructures, telecommunications, transport, or governmental and financial systems. Based on discussions with experts from all parts of the world and its own research, the ICRC is particularly concerned about the potential human cost of cyber operations on critical civilian infrastructure, including health infrastructure.[3]

In recent years, cyber attacks have exposed the vulnerability of essential services. They are reportedly becoming more frequent and their severity is increasing more rapidly than experts had anticipated. Moreover, much is unknown with respect to the most sophisticated cyber capabilities and tools that have been or are being developed, how technology may evolve, and the extent to which the use of cyber operations during armed conflicts might be different from the trends observed so far.

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

Cyber tools also proliferate in a unique manner. Once used, they can be repurposed and widely used by actors other than the one that developed or used them initially.

3. The application of IHL to cyber operations during armed conflicts

For the ICRC, there is no question that IHL applies to, and therefore limits, cyber operations during armed conflict – just as it regulates the use of any other weapon, means or method of warfare in an armed conflict, whether new or old.[4]

3 See ICRC, *The Potential Human Cost of Cyber Operations*, Geneva, 2019, available at: www.icrc.org/en/download/file/96008/the-potential-human-cost-of-cyber-operations.pdf.

4 ICRC, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts*, 31IC/11/5.1.2, Geneva, 2011 (ICRC Challenges Report 2011), pp. 36–37, available at: www.icrc.org/en/doc/assets/files/red-cross-crescent-movement/31st-international-conference/31-int-conference-ihl-challenges-report-11-5-1-2-en.pdf; ICRC, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts*, 32IC/15/11, Geneva, 2015 (ICRC Challenges Report 2015), p. 40, available at: www.icrc.org/en/download/file/15061/32ic-report-on-ihl-and-challenges-of-armed-conflicts.pdf; ICRC, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts*, 33IC/19/9.7, Geneva, 2019 (ICRC Challenges Report 2019), p. 18, available at: https://rcrcconference.org/app/uploads/2019/10/33IC-IHL-Challenges-report_EN.pdf.

This holds true whether cyberspace is considered as a new domain of warfare similar to air, land, sea or outer space; a different type of domain because it is man-made while the former are natural; or not a domain as such.

When States adopt IHL treaties, they do so to regulate present and future conflicts. States have included rules that anticipate the development of new means and methods of warfare in IHL treaties, presuming that IHL will apply to them. For instance, if IHL did not apply to future means and methods of warfare, it would not be necessary to review their lawfulness under existing IHL, as required by Article 36 of the 1977 Additional Protocol I.

This conclusion finds strong support in the International Court of Justice's Advisory Opinion on the *Legality of the Threat or Use of Nuclear Weapons*: the Court recalled that the established principles and rules of IHL applicable in armed conflict apply "to all forms of warfare and to all kinds of weapons", including "those of the future".[5] In the ICRC's view, this finding applies to the use of cyber operations during armed conflict.

The ICRC welcomes that an increasing number of States and international organizations have affirmed that IHL applies to cyber operations during armed conflicts and welcomes discussion on how IHL applies.

States may also decide to impose additional limits to those found in existing law and to develop complementary rules, in particular in order to strengthen the protection of civilians and civilian infrastructure against the effects of cyber operations. In the ICRC's view, any new rules need to build on and strengthen the existing legal framework, including IHL.

In cases not covered by existing rules of IHL, civilians and combatants remain protected by the so-called "Martens Clause", meaning that they remain under the protection and authority of the principles of international law derived from established custom, from the principles of humanity and from the dictates of public conscience.[6]

It is important to underline that affirming the application of IHL to cyber operations during armed conflict does not legitimize cyber warfare or encourage the militarization of cyberspace. In fact, IHL imposes some limits to the militarization of cyberspace by prohibiting the development of military cyber capabilities that would violate IHL.[7] Moreover, any use of force by States – cyber or kinetic – remains governed by the Charter of the United Nations and the relevant rules of

5 International Court of Justice, *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, 8 July 1996 (Nuclear Weapons Advisory Opinion), para. 86.

6 See Protocol Additional (I) to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts, 1125 UNTS 3, 8 June 1977 (entered into force 7 December 1978) (AP I), Art. 1(2); Hague Convention (II) with respect to the Laws and Customs of War on Land and Its Annex: Regulations concerning the Laws and Customs of War on Land, The Hague, 29 July 1899 (entered into force 4 September 1900), preambular para. 9; Hague Convention (IV) respecting the Laws and Customs of War on Land and Its Annex: Regulations concerning the Laws and Customs of War on Land, The Hague, 18 October 1907 (entered into force 26 January 1910), preambular para. 8.

7 See, among others, Jean-Marie Henckaerts and Louise Doswald-Beck (eds), *Customary International Humanitarian Law*, Vol. 1: *Rules*, Cambridge University Press, Cambridge, 2005 (ICRC Customary Law Study), Rules 70, 71, available at: https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1. See also AP I, Art. 36.

customary international law, in particular, the prohibition against the use of force. International disputes must be settled by peaceful means, in cyberspace as in all other domains.

4. The protection afforded by existing IHL

Existing IHL treaties and customary law provide rules on a number of issues during armed conflict. In cyberspace, the rules on the conduct of hostilities are particularly relevant. These rules aim to protect the civilian population against the effects of hostilities. They are based on the cardinal principle of distinction, which requires that belligerents distinguish at all times between the civilian population and combatants and between civilian objects and military objectives, and direct their operations only against military objectives.[8]

Notwithstanding the interconnectivity that characterizes cyberspace, a careful examination of the functioning of cyber tools shows that they are not necessarily indiscriminate. Many of the recent cyber attacks that have been reported in public sources appear to have been rather "discriminate" from a technical point of view: they have been designed and actually used to target and harm only specific objects and have not spread or caused harm indiscriminately. Ensuring that cyber operations affect only the targeted object may, however, be technically challenging and require careful planning in their design and use. Moreover, it must be noted that a cyber operation that is technically discriminate is not necessarily lawful, whether during or outside of an armed conflict.

This being said, some known cyber tools have been designed to self-propagate and indiscriminately affect widely used computer systems. They have not done so by chance: the ability to self-propagate needs to be specifically included in the design of such tools. The interconnectivity that characterizes cyberspace means that whatever has an interface with the Internet can be targeted from anywhere in the world. Moreover, an attack on a specific system may have repercussions on various other systems and cause indiscriminate effects. As a result, there is a real risk that cyber tools are not designed or used – either deliberately or by mistake – in compliance with IHL.

Affirming that IHL – including the principles of distinction, proportionality, and precaution – applies to cyber operations during armed conflicts means that under existing law, among many other rules:

- cyber capabilities that qualify as weapons and are by nature indiscriminate are prohibited;[9]
- direct attacks against civilians and civilian objects are prohibited, including when using cyber means or methods of warfare;[10]

8 AP I, Art. 48; ICRC Customary Law Study, above note 7, Rules 1, 7; Nuclear Weapons Advisory Opinion, above note 5, para. 78.
9 ICRC Customary Law Study, above note 7, Rule 71.
10 AP I, Arts 48, 51, 52; ICRC Customary Law Study, above note 7, Rules 1, 7.

- acts or threats of violence the primary purpose of which is to spread terror among the civilian population are prohibited, including when carried out through cyber means or methods of warfare;[11]
- indiscriminate attacks, namely those of a nature to strike military objectives and civilians or civilian objects without distinction, are prohibited, including when using cyber means or methods of warfare;[12]
- disproportionate attacks are prohibited, including when using cyber means or methods of warfare. Disproportionate attacks are those which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated.[13]
- during military operations, including when using cyber means or methods of warfare, constant care must be taken to spare the civilian population and civilian objects; all feasible precautions must be taken to avoid or at least minimize incidental civilian harm when carrying out attacks, including through cyber means and methods of warfare;[14]
- attacking, destroying, removing or rendering useless objects indispensable to the survival of the population is prohibited, including through cyber means and methods of warfare;[15]
- medical services must be protected and respected, including when carrying out cyber operations during armed conflicts.[16]

In addition, all feasible precautions must also be taken to protect civilians and civilian objects against the effects of attacks conducted through cyber means and methods of warfare, which is an obligation that States must already implement in peacetime.[17] Measures that could be considered include, among others: segregating military from civilian cyber infrastructure and networks; segregating computer systems on which essential civilian infrastructure depends from the

11 AP I, Art. 51(2); ICRC Customary Law Study, above note 7, Rule 2.

12 AP I, Art. 51(4); ICRC Customary Law Study, above note 7, Rules 11, 12. Indiscriminate attacks are those: (a) which are not directed at a specific military objective; (b) which employ a method or means of combat which cannot be directed at a specific military objective; or (c) which employ a method or means of combat the effects of which cannot be limited as required by international humanitarian law; and consequently, in each such case, are of a nature to strike military objectives and civilians or civilian objects without distinction.

13 AP I, Arts 51(5)(b), 57; ICRC Customary Law Study, above note 7, Rule 14.

14 AP I, Art. 57; ICRC Customary Law Study, above note 7, Rules 15–21.

15 AP I, Art. 54; Protocol Additional (II) to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts, 1125 UNTS 609, 8 June 1977 (entered into force 7 December 1978) (AP II), Art. 14; ICRC Customary Law Study, above note 7, Rule 54.

16 See, for instance, Geneva Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed forces in the Field of 12 August 1949, 75 UNTS 31 (entered into force 21 October 1950), Art. 19; Geneva Convention (II) for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of the Armed Forces at Sea of 12 August 1949, 75 UNTS 85 (entered into force 21 October 1950), Art. 12; Geneva Convention (IV) relative to the Protection of Civilian Persons in Time of War of 12 August 1949, 75 UNTS 287 (entered into force 21 October 1950), Art. 18; AP I, Art. 12; AP II, Art. 11; ICRC Customary Law Study, above note 7, Rules 25, 28, 29.

17 AP I, Art. 58; ICRC Customary Law Study, above note 7, Rules 22, 24.

Internet; and working on the identification in cyberspace of the cyber infrastructure and networks serving specially protected objects like hospitals.[18]

5. The need to discuss how IHL applies

Affirming that IHL applies to cyber operations in armed conflict is an essential first step to avoiding or minimizing the potential human suffering that cyber operations might cause. However, the ICRC also encourages States to work towards a common understanding of *how* IHL principles and rules apply to cyber operations. This is necessary because the interconnected nature of cyberspace and its largely digital character pose challenges for the interpretation of key IHL principles and concepts on the conduct of hostilities.

Among the various issues, in this position paper the ICRC emphasizes three.

The military use of cyberspace and the effect on its civilian character

Except for some specific military networks, cyberspace is predominantly used for civilian purposes. However, civilian and military networks may be interconnected. 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 military. Civilian logistical supply chains and essential civilian services use the same web and communication networks through which some military communications pass.

Not every use for military purposes renders a civilian object a military objective under IHL.[19] If it does, however, the object is no longer protected by the prohibition against direct attacks on civilian objects. It would be a matter of serious concern if the military use of cyberspace led to the conclusion that many objects forming part thereof would no longer be protected as civilian objects. This could lead to large-scale disruption of the ever-increasingly important civilian usage of cyberspace.

This being said, even if certain parts of the cyberspace infrastructure were no longer protected as civilian objects during armed conflicts, any attack would remain governed by the prohibition on indiscriminate attacks and the rules of proportionality and precautions in attack. Precisely because civilian and military networks are so interconnected, assessing the expected incidental civilian harm of

18 ICRC Challenges Report 2015, above note 4, p. 43.

19 See AP I, Art. 52(2); ICRC Customary Law Study, above note 7, Rule 8: "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 partial or total destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage." For more details on the limits to cyber infrastructure becoming a military objective under IHL, see ICRC Challenges Report 2015, above note 4, p. 42.

any cyber operation is critical to ensuring that the civilian population is protected against its effects.[20]

The notion of "attack" under IHL and cyber operations

Critical civilian infrastructure enabling the provision of essential services increasingly relies on digitalized systems. Safeguarding such infrastructure and services against cyber attacks or incidental damage is essential to protect the civilian population.

IHL provides specific protection for certain infrastructure, such as medical services and objects indispensable to the survival of the population, regardless of the type of harmful operation.[21] However, most rules stemming from the principles of distinction, proportionality and precaution – which provide general protection for civilians and civilian objects – apply only to military operations that qualify as "attacks" as defined in IHL.[22] Article 49 of Additional Protocol I defines attacks as "acts of violence against the adversary, whether in offence or in defence".[23] 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.

It is widely accepted that cyber operations expected to cause death, injury or physical damage constitute attacks under IHL. In the ICRC's view, this includes harm due to the foreseeable direct and indirect (or reverberating) effects of an attack, for example the death of patients in intensive care units caused by a cyber operation on an electricity network that results in cutting off a hospital's electricity supply.

Beyond this, attacks that significantly disrupt essential services without necessarily causing physical damage constitute one of the most important risks for civilians. Diverging views exist, however, on whether a cyber operation that results in a loss of functionality without causing physical damage qualifies as an attack as defined in IHL. In the ICRC's view, during an armed conflict an operation designed to disable a computer or a computer network constitutes an attack under IHL, whether the object is disabled through kinetic or cyber means.[24] 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

20 See ICRC, *The Principle of Proportionality in the Rules Governing the Conduct of Hostilities under International Humanitarian Law*, Geneva, 2018, pp. 37–40, available at: www.icrc.org/en/download/file/79184/4358_002_expert_meeting_report_web_1.pdf.

21 See text in relation to above notes 16 and 15. With regard to the latter, they must not be attacked, destroyed, removed or rendered useless.

22 The notion of attack under IHL, defined in Article 49 of AP 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 operations, amounts to an attack under IHL does not necessarily mean that it would qualify as an armed attack under the UN Charter.

23 For rules that apply specifically to attacks, see text in relation to above notes 10–14.

24 See ICRC Challenges Report 2011, above note 4, p. 37; ICRC Challenges Report 2015, above note 4, pp. 41–42.

(such as electricity, banking or communications) dysfunctional, or is expected to cause such effect incidentally, might not be covered by essential IHL rules protecting the civilian population and civilian objects. Such an overly restrictive understanding of the notion of attack would be difficult to reconcile with the object and purpose of the IHL rules on the conduct of hostilities. It is therefore essential that States find a common understanding in order to adequately protect the civilian population against the effects of cyber operations.

Civilian data and the notion of "civilian objects"

Essential civilian data – such as medical data, biometric data, social security data, tax records, bank accounts, companies' client files or election lists and records – are an essential component of digitalized societies. Such data are key to the functioning of most aspects of civilian life, be it at the individual or societal level. There is increasing concern about safeguarding such essential civilian data.

Some of the specific protection afforded by IHL extends to essential data, such as data belonging to medical units, which are encompassed in the obligation to respect and protect such units.[25]

More generally, the main IHL principles and rules governing the conduct of hostilities protect civilians and civilian objects.[26] It would therefore be important for States to agree on an understanding that civilian data is protected by these rules.

Deleting or tampering with essential civilian data can quickly bring government services and private businesses to a complete standstill. Such operations could cause more harm to civilians than the destruction of physical objects. 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. 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.[27] Excluding essential civilian data from the protection afforded by IHL to civilian objects would result in an important protection gap.

6. Attribution of conduct in cyberspace for the purposes of State responsibility

Cyberspace provides various technical possibilities for actors to hide or falsify their identity, which increases the complexity of attribution by other actors. This creates major difficulties. For example, even during armed conflict, IHL only applies to

25 See above note 16.
26 See text in relation to above notes 10–15.
27 ICRC Challenges Report 2015, above note 4, p. 43; ICRC Challenges Report 2019, above note 4, p. 21.

operations that are linked to the conflict. If the author of a cyber operation – and thus the link of the operation to an armed conflict – cannot be identified, it may be difficult to determine whether IHL is even applicable to the operation. Attribution of cyber operations is also important to ensure that actors who violate international law, including IHL, can be held accountable. The perception that it will be easier to deny responsibility for such attacks may also weaken the taboo against their use – and may make actors less scrupulous about using them in violation of international law.[28]

This being said, attribution is not a problem from the perspective of the actors who conduct, direct or control cyber operations: they have all the facts at hand to determine under which international legal framework they are operating and which obligations they must respect.

Under international law, a State is responsible for conduct attributable to it, including possible violations of IHL. This includes:

- conduct by organs of the State, including its armed forces or intelligence services;
- conduct by persons or entities, such as private companies, that the State has empowered to exercise elements of governmental authority;
- conduct by persons or groups, such as militias or groups of hackers, acting in fact on the State's instructions, or under its direction or control; and
- conduct by private persons or groups which the State acknowledges and adopts as its own conduct.[29]
- These principles apply whether the conduct is carried out by cyber or any other means.

7. Conclusion

The use of cyber operations as means or methods or warfare in an armed conflict poses a real risk of harm to civilians. For the protection of the civilian population and civilian infrastructure, it is critical to recognize that such operations do not occur in a legal vacuum. The ICRC urges all States to affirm that IHL applies to cyber operations during armed conflicts, on the understanding that such affirmation neither encourages the militarization of cyberspace nor legitimizes cyber warfare.

At the same time, the ICRC believes that further discussion – especially among States – is needed on how IHL should be interpreted and applied in cyberspace. There is a pressing need for such discussion because States that decide to develop or acquire cyber capabilities that qualify as weapons, means or methods of warfare – whether for offensive or defensive purposes – must ensure that these capabilities can be used in accordance with their obligations under

28 ICRC Challenges Report 2011, above note 4, p. 37; ICRC Challenges Report 2019, above note 4, p. 20.
29 See ICRC Customary Law Study, above note 7, Rule 149. See also International Law Commission, *Responsibility of States for Internationally Wrongful Acts*, 2001, in particular Arts 4–11.

IHL.[30] Discussion should be informed by an in-depth understanding of the development of military cyber capabilities, their potential human cost, and the protection afforded by existing law. States need to determine whether existing law is adequate and sufficient to address the challenges posed by the interconnected and largely digital character of cyberspace, or whether it needs adaptation to the specific characteristics of cyberspace. If new rules are to be developed to protect civilians against the effects of cyber operations or for other reasons, they should build on and strengthen the existing legal framework – including IHL.

The ICRC welcomes the intergovernmental discussions currently taking place in the framework of two United Nations General Assembly mandated processes and it is grateful for the opportunity to share its views with the participating States. The ICRC also stands ready to lend its expertise to such discussions, as States deem appropriate.

30 See ICRC Challenges Report 2019, above note 4, pp. 28–29; ICRC, *A Guide to the Legal Review of New Weapons, Means and Methods of Warfare: Measures to Implement Article 36 of Additional Protocol I of 1977*, Geneva, 2006, p. 4; AP I, Art. 36.