Joint submission of the International Committee of the Red Cross and Australian Red Cross

to the Australian Department of Foreign Affairs and Trade

Public consultation: Responsible state behaviour in cyberspace in the context of international security at the UN

Who we are

The International Red Cross Red Crescent Movement (Movement) is a neutral, independent and impartial humanitarian organisation that operates worldwide in accordance with our internationally recognised Statutes and Regulations. It consists of three components: International Committee of the Red Cross (ICRC); 192 Red Cross/Red Crescent National Societies (such as Australian Red Cross); and the International Federation of Red Cross Red Crescent Societies.

The ICRC's mission and mandate, which stems from the 1949 Geneva Conventions and the universally endorsed Statutes of the Movement,[1] includes working for the faithful application, dissemination and development of international humanitarian law (IHL). Accordingly, the ICRC has an interest with respect to the law applicable to cyber operations employed as means and methods of warfare during an armed conflict and the protection afforded to civilians against their effects.

Australian Red Cross (ARC) has been a critical part of Australian life since 1914, mandated by the Royal Charter of 1941 as an auxiliary to Australia's public authorities in the humanitarian field including during emergencies and armed conflict. Its mission, to alleviate vulnerability, includes championing the importance of international humanitarian law in Australia.

Executive Summary

The ICRC and ARC welcome the opportunity to provide input in relation to Australia's engagement in the *Open Ended Working Group on developments in the field of information and telecommunications in the context of international security* (OEWG) and the *Group of Governmental Experts on advancing responsible state behaviour in cyberspace in the context of international security* (GGE).

In terms of **existing and emerging threats** (Q1), this submission outlines four key areas of concern:

1. the specific vulnerabilities of certain types of infrastructure, primarily the health-care sector as well as other critical civilian infrastructure relying on industrial control systems;
2. the risk of overreaction due to a misunderstanding by a target as to the intended purpose of a cyber activity;
3. the proliferation of cyber tools; and
4. the challenges raised by the attribution of cyber operations.

Regarding the **best practice implementation of the norms** contained in the 2015 GGE report (Q3), there are a number of pertinent good practices identified below, including with respect to industry standards and legal regulation, the creation of "digital watermarks" to identify protected actors or

[1] See Art 5(2)(g) of the Statutes of the Movement.

infrastructure, the creation of obstacles to make re-purposing difficult and expensive, and the disclosure of vulnerabilities so that they can be fixed.

When considering **potential areas for national contributions** on the application of IHL to cyberspace (Q4), we recommend Australia elaborate on its position on the protection that existing IHL affords, in particular by going beyond the principles of necessity, proportionality and distinction to consider other IHL principles and rules. Further, we encourage elaboration of *how* IHL principles and rules are to be interpreted and applied to cyber operations during armed conflicts, including discussion of the dual use (military and civilian) nature of cyberspace, the notion of 'attack' under IHL, and the extent to which civilian data is protected by IHL.

Q 1. Existing and emerging threats

The Movement is concerned about the potential human cost of cyber operations. In particular, based on an expert meeting convened in November 2018, the ICRC has identified four areas of concern:

a) The specific vulnerabilities of certain types of infrastructure

Cyber attacks can affect the delivery of health care and other critical civilian infrastructure, notably those operated by industrial control systems.

One area of concern for the ICRC, given its mandate, is the **health-care sector**. In this regard, research shows that the healthcare sector appears to be particularly vulnerable to direct cyber attacks and incidental harm from such attacks directed elsewhere. Its vulnerability is a consequence of increased digitisation and interconnectivity in health care. For example, medical devices in hospitals are connected to the hospital network, and biomedical devices such as pacemakers and insulin pumps are sometimes remotely connected through the internet. This growth of connectivity increases the sector's digital dependence and "attack surface" and leaves it exposed, especially when these developments are not matched by a corresponding improvement in cyber security.[2]

Critical civilian infrastructure – including electrical, water, and sanitation facilities – is another area in which cyber attacks can cause significant harm to the civilian population. This infrastructure is often operated by industrial control systems. Industrial control systems are protected by complex safety mechanisms and often have built-in redundancy to guarantee safety and reliability. For example, electrical networks are grids with multiple power sources to avoid widespread effects when one of their parts is affected. Nonetheless, attacks on specific nodes of industrial control systems may cause a significant impact, such as if a critical system (like a hospital) depends on a specific sub-system or node, or because they have cascading harmful consequences. A cyber attack against an industrial control system requires specific expertise and sophistication, as well as specifically designed cyber tools. While attacks against industrial control systems have been less frequent than other types of cyber operations, their frequency is reportedly increasing, and the severity of the threat has evolved more rapidly than anticipated only a few years ago.[3]

---

[2] ICRC, 'International Humanitarian Law and the Challenges of Contemporary Armed Conflicts', Report, October 2019 ('2019 IHL Challenges Report'), p. 26-27, available from https://www.icrc.org/en/document/icrc-report-ihl-and-challenges-contemporary-armed-conflicts. See also ICRC, 'The potential human cost of cyber operations' (L. Gisel and L. Olejnik, eds), Expert Meeting Report ('Human Cost Report'), May 2019, pp. 6, 18-22 and 60-62; L Gisel and T Rodenhauser, 'Cyber operations and international humanitarian law: five key points', *Law and Policy Blog,* 28 November 2019, https://blogs.icrc.org/law-and-policy/2019/11/28/cyber-operations-ihl-five-key-points/https://www.icrc.org/en/download/file/97346/the-potential-human-cost-of-cyber-operations.pdf.

[3] 2019 IHL Challenges Report, p. 27; Human Cost Report, pp. 6, 23-28 and 62 – 65.

b) Risk of overreaction due to misunderstanding of intended purpose

Cyber operations carry a risk of overreaction and escalation, and related human harm, due to the fact that it may be extremely difficult – if not impossible – for the target of a cyber attack to detect whether the attacker's aim is to spy or to cause physical damage. As the aim of a cyber operation might be identified only after the target system has been harmed, there is a risk that the target will imagine the worst-case scenario and react much more strongly than it would have done if it had known that the attacker's true intent was limited to espionage, for example.[4]

c) Proliferation of cyber tools

Cyber tools and methods can proliferate in a unique manner that is difficult to control. Today, sophisticated cyber attacks are carried out only by the most advanced and best-resourced actors. Once cyber tools have been used, stolen, leaked or otherwise become available, actors other than those who developed them might be able to find them, reverse engineer them and reuse them for their own - possibly malicious - purposes.[5]

d) Attribution of attacks

The ability of threat actors to obscure or effectively hide the origin of their operations on the internet, compounded by the ability to buy, repurpose or reengineer cyber tools developed or used by other actors continues to make it difficult to rapidly and reliably attribute cyber attacks to a specific actor. This creates major difficulties. For example, even during armed conflict, IHL only applies to 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.[6]

Q 3. Best practice implementation of norms

Below are examples of good practices which the ICRC has identified, which could be considered in relation to selected norms contained in the 2015 GGE report.

(g) States should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account General Assembly resolution 58/199 on the creation of a global culture of cybersecurity and the protection of critical information infrastructures, and other relevant resolutions

While cyber security and defence are constantly improving, older systems with **outdated or even non-existent cyber security** are particularly vulnerable to cyber attacks and will remain a concern in the years to come. Both the public and private sectors have a role to play through industry standards and legal regulation.[7]

In the health-care sector, for instance, the regulatory environment should be adapted to the increased risk, such as through standardisation requirements, with a view to ensuring resilience in the event of a cyber attack. Cyber security needs to be taken into account in the design and development of medical

---

[4] 2019 IHL Challenges Report, p. 27; Human Cost Report, pp. 7 and 11-12.
[5] 2019 IHL Challenges Report, p. 27; Human Cost Report, pp. 7.
[6] ICRC, 'International Humanitarian Law and Cyber Operations during Armed Conflicts', Position Paper, November 2019 ('Position Paper'), p. 9 https://www.icrc.org/en/download/file/108983/icrc_ihl-and-cyber-operations-during-armed-conflicts.pdf; see also ICRC, 'International humanitarian law and the challenges of contemporary armed conflicts', 2011 ('2011 IHL Challenges Report'), p. 37 available from https://www.icrc.org/en/doc/resources/documents/report/31-international-conference-ihl-challenges-report-2011-10-31.htm ; 2019 IHL Challenges Report, p. 20.
[7] Human Cost Report, p 9.

devices and networks and updated throughout their lifetime, no matter how long they last. Similarly, for industrial control systems, industry standards, whether imposed or self-imposed, are critical. This includes reporting incidents and sharing information between trusted partners.[8]

In terms of IHL, **parties to armed conflicts must take all feasible precautions to protect civilians and civilian objects under their control against the effects of attack**. This is one of the few IHL obligations that States must already implement in peacetime, especially with regard to fixed installations. While cyberspace is a virtual global domain, the obligation to take precautions against the effects of attacks extends at least to the physical infrastructure of cyberspace (and to objects whose functioning depends on that infrastructure) located in a State's territory, or in any territory that may be occupied by a party to the conflict.[9]

Among many other avenues that could be explored,[10] States could consider creating a "digital watermark" to identify certain actors or infrastructure in cyber space that must be protected (such as objects that enjoy specific protection under IHL). The aim would be to help their identification and prevent them from being targeted during armed conflicts. The potentially positive effects in terms of protection against unintended harm by law-abiding actors would however need to be balanced against the risk of disclosing information on critical infrastructure to potential adversaries, including criminals. The prospects of positive effects might depend in part on attribution becoming easier.[11]

(i) States should take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products. States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions;

Those who develop cyber capabilities should consider **creating obstacles to make repurposing difficult and expensive**. While it is hardly possible from a technical standpoint to guarantee that malware cannot be repurposed, methods like encrypting its payload and including obstacles in different components of the code, for example, could raise the bar in terms of the expertise required to reengineer malicious tools.[12]

(j) States should encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies to such vulnerabilities to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure;

The preferred option for enhancing the safety of cyber space should be disclosing vulnerabilities to the appropriate software developer or vendor so that the vulnerabilities can be fixed.[13] In this regard, we welcome the fact that the Australian Signals Directorate (ASD) has adopted Responsible Release Principles for Cyber Security Vulnerabilities that take as their starting position to disclose weaknesses found. The risks entailed by a decision not to disclose vulnerabilities in view of the specific characteristics of cyber space should be duly considered in these kinds of decision-making frameworks.

[8] Human Cost Report pp 9 and 39-40.
[9] Position Paper, p. 6; ICRC, 'International Humanitarian Law and the Challenges of Contemporary Armed Conflicts', October 2015, p. 43; https://www.icrc.org/en/download/file/15061/32ic-report-on-ihl-and-challenges-of-armed-conflicts.pdf.
[10] Human Cost Report, pp. 39-42 and 75-77.
[11] Human Cost Report, pp. 9 and 40 - 41.
[12] Human Cost Report, p. 9.
[13] Human Cost Report, pp. 9 and 33-34.

Q 4. Potential areas for national contributions on the application of international humanitarian law to cyberspace

We welcome Australia's statement, in its 2017 Position and 2019 Supplement, that IHL rules will apply to cyber operations conducted in an armed conflict, a view also held by the ICRC. For the ICRC, there is no question that IHL principles and rules apply to new weapons, means and methods of warfare, including those relying on information and telecommunications technology.[14]

Additionally, we encourage Australia to expand on its position on the protection that existing IHL affords, and *how* IHL principles and rules are to be interpreted and applied to cyber operations during armed conflicts, to facilitate the development of common understandings in the OEWG and GGE.

In November 2019 the ICRC submitted a position paper on cyber operations and international humanitarian law (IHL) to both the OEWG and the GGE to support the deliberations of States. In that paper, the ICRC set out the following three (non-exhaustive) areas that would benefit from such elaboration:

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.[15]

We welcome the fact that in its 2017 Position, Australia affirmed that, among other IHL rules, the principles of humanity, necessity, proportionality and distinction apply to cyber operations within an armed conflict, and expanded on the latter three.

As noted in the Position Paper that the ICRC submitted to the UN OEWG and GGE,[16] affirming that IHL – including the principles of distinction, proportionality, and precautions – 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;[17]
- direct attacks against civilians and civilian objects are prohibited, including when using cyber means or methods of warfare;[18]
- 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;[19]
- 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;[20]

---

[14] Position Paper, pp. 4-5.

[15] Art. 48 of the 1977 Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (AP I); Henckaerts and Doswald-Beck (eds), *Customary International Humanitarian Law, Vol. I: Rules*, ICRC, Cambridge University Press, Cambridge, 2005 (ICRC Customary IHL Study) Rules 1 and 7, available at: https://www.icrc.org/en/doc/assets/files/other/customary-international-humanitarian-law-i-icrc-eng.pdf . International Court of Justice, *Legality of the threat or the use of nuclear weapons*, Advisory Opinion, 8 July 1996, para. 78.

[16] P. 5-6.

[17] Rule 71 ICRC Customary IHL Study.

[18] Arts 48, 51 and 52 AP I; Rules 1 and 7 ICRC Customary IHL Study.

[19] Art. 51(2) AP I; Rule 2 ICRC Customary IHL Study.

[20] Art. 51(4) AP I; Rules 11 and 12 ICRC Customary IHL Study. 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

- 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.[21]
- 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;[22]
- attacking, destroying, removing or rendering useless objects indispensable to the survival of the population is prohibited, including through cyber means and methods of warfare;[23]
- medical services must be protected and respected, including when carrying out cyber operations during armed conflicts.[24]

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.[25] 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 internet; work on the identification in cyberspace of the cyber infrastructure and networks serving specially protected objects like hospitals.[26]

We encourage Australia, as part of its contribution on the application of IHL to cyberspace to go beyond the principles already affirmed in the 2017 Position, and expand on the protections afforded against cyber operation effects in armed conflict by the above-mentioned, and/or other IHL principles and rules.

The need to discuss *how* IHL applies

- **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.

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.

[21] Arts 51(5)(b) and 57 AP I; Rule 14 ICRC Customary IHL Study.

[22] Art. 57 AP I; Rules 15 - 21 ICRC Customary IHL Study.

[23] Art. 54 AP I; Art. 14 of the 1977 Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (AP II); Rule 54 ICRC Customary IHL Study.

[24] See, for instance, Art. 19 Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (GCI); Art. 12 Convention (II) for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea (GCII); Art. 18 Convention (IV) relative to the Protection of Civilian Persons in Time of War (GCIV); Art. 12 AP I; Art. 11 AP II; Rules 25, 28, 29 ICRC Customary IHL Study.

[25] Art. 58 AP I; Rules 22 to 24 ICRC Customary IHL Study.

[26] ICRC, *International humanitarian law and the challenges of contemporary armed conflicts*, 2015 ('2015 IHL Challenges Report'), p. 43, available at: https://www.icrc.org/en/document/international-humanitarian-law-and-challenges-contemporary-armed-conflicts

This dual usage, for both civilian and military purposes, creates vulnerabilities for civilian facilities and depending on the application of the definition of military objective may render such facilities subject to attack in armed conflict.

Not every use for military purposes renders a civilian object a military objective under IHL.[27] If it does, however, the object is no longer protected by the prohibition to 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 of indiscriminate attacks and the rules of proportionality and precautions in attack.[28] Precisely because civilian and military networks are so interconnected, assessing the expected incidental civilian harm of any cyber operation is critical to ensure that the civilian population is protected against its effects.[29]

In view of the above, we encourage Australia to elaborate its position on:

- What are the limits that govern the targeting of dual-use objects, for example if certain parts of the cyberspace infrastructure were no longer protected as civilian objects during armed conflicts because their use for military purposes would have rendered them military objectives under IHL?; and
- how Australia practically assesses, and take all feasible precautions to avoid or at least reduce, the expected incidental civilian harm of any cyber operation, considering the interconnected nature of civilian and military networks.

- **The notion of 'attack' under IHL and cyber operations**

Determining whether a cyber operation during an armed conflict constitutes an 'attack' for the purposes of IHL[30] is essential for the applicability of IHL 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 our 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. If the notion of attack is interpreted as only referring to operations that

[27] See Art. 52(2) AP I; Rule 8 Customary IHL Study: "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 military objectives under IHL, see ICRC, *International humanitarian law and the challenges of contemporary armed conflicts*, 2015, p. 42.

[28] Rule 8 ICRC Customary IHL Study.

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

[30] The notion of attack under IHL is defined in Art. 49 AP I as 'acts of violence against the adversary, whether in offence or in defence'. This notion is different from and should not be confused with the notion of 'armed attack' under Art. 51 of the UN Charter, which belongs to the realm of *jus ad bellum*. To affirm that a specific cyber operation, or a type of cyber operations, amounts to an attack under IHL does not necessarily mean that it would qualify as an armed attack under the UN Charter.

cause death, injury or physical damage, a cyber operation that is directed at making a civilian network (such as electricity, banking, or communications) dysfunctional, or is expected to cause such effect incidentally, might not be covered by essential IHL rules protecting the civilian population and civilian objects. Such an overly restrictive understanding of the notion of attack would be difficult to reconcile with the object and purpose of the IHL rules on the conduct of hostilities. It is therefore essential that States find a common understanding in order to adequately protect the civilian population against the effects of cyber operations.[31]

Australia has stated in its 2019 Supplement that it considers that, if a cyber operation rises to the same threshold as that of a kinetic 'attack' under IHL, the rules governing such attacks during armed conflict will apply to those kinds of cyber operations. We encourage Australia to continue to develop and disseminate its views on the circumstances in which, during an armed conflict a cyber operation will rise to the threshold of an attack under IHL.

- **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 digitised 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.

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.[32]

More generally, the main IHL principles and rules governing the conduct of hostilities protect civilians and civilian objects.[33] 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.[34] Excluding essential civilian data from the protection afforded by IHL to civilian objects would result in a significant protection gap.

Conclusion

The use of cyber operations as means or methods or warfare in an armed conflict poses a real risk of harm to civilians.

Threats may arise not only due to the particular vulnerabilities of certain sectors (eg. the healthcare sector), but also as a result of the specific technical characteristics of cyber operations. Difficulties in determining the aim of a cyber operation can lead to overreaction and escalation. Cyber tools can proliferate in a manner that is hard to control. And attributing attacks and holding actors responsible for violations of IHL in cyberspace is likely to be challenging.

[31] Position Paper, pp. 7-8.
[32] See footnote 24 above.
[33] See text in relation to notes 18 to 23 above.
[34] 2015 IHL Challenges Report, p. 43; 2019 IHL Challenges Report, p. 21.

A number of avenues could be explored to reduce the potential human cost of cyber operations, including enhancing cyber security posture and resilience of the actors potentially affected, marking certain civilian infrastructure, imposing measures to prevent proliferation and disclosing vulnerabilities.

Cyber warfare also raises a number of challenges for the interpretation and application of IHL. We recommend Australia elaborate on its position on the protection that existing IHL affords. Further, we encourage elaboration of *how* IHL principles and rules are to be interpreted and applied to cyber operations during armed conflicts, to facilitate the development of common understandings in the OEWG and GGE. It is critical that the protection afforded by IHL to civilians and other victims of armed conflicts be upheld in cyberspace.

The Movement is grateful for the opportunity to share its views with Australia as part of this public consultation process and stands ready to continue to lend its expertise as appropriate.

28 January 2020

Contacts

Australian Red Cross
Tara Gutman
Legal Adviser, International Humanitarian Law
Red Cross House Garran ACT 2605
Tel 02 6234 7609 Mob: 0419 099152

International Committee of the Red Cross
Georgia Hinds
Regional Legal Adviser
15 National Circuit Barton ACT 2604
Tel: 02 6273 2968 Mob: 0419 218231