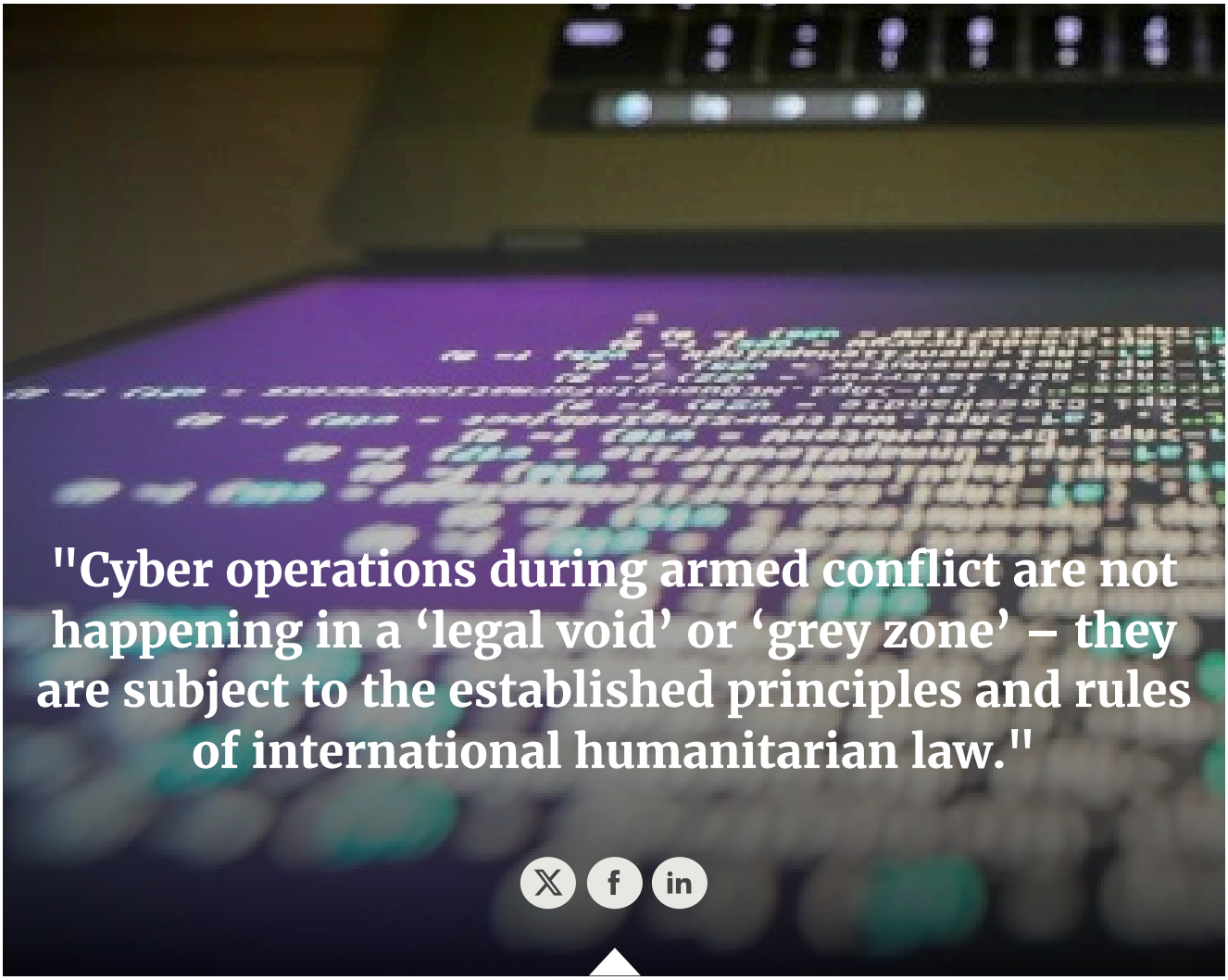

Statement by the International Committee of the Red Cross to the UN Security Council Open Debate on Cyber Security, maintaining international peace and security in cyberspace.

STATEMENT | 29 JUNE 2021

Excellencies,

The International Committee of the Red Cross (ICRC) is grateful for the opportunity to contribute to this UN Security Council Open Debate on 'Maintaining International Peace and Security in Cyberspace'.

Over the past two decades, hostile cyber operations have become an increasingly important concern for the maintenance of international peace and security. As societies are digitalizing, so are military capabilities of States and other actors. Today, the international community recognizes that 'a number of States are developing ICT capabilities for military purposes' and that 'the use of ICTs in future conflicts between States is becoming more likely'.[1]

In light of this reality, the ICRC would like to recall the potential harm to humans that the use of cyber technology can cause, and afterwards present how States can mitigate these adverse humanitarian consequences through action at the international and at the national level.

It is today well-known that cyber operations against critical civilian infrastructure have caused significant economic harm, disruption in societies, and tension among States. In the final report of the 'Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security', all States recognized that cyber operations against critical infrastructure risk having 'potentially devastating humanitarian consequences'.[2] While the ICRC cannot confirm any cyber operations with human casualties, we are concerned about the destructive effects of cyber operations, such as the disruption of electricity supplies, water systems or medical services.[3] These kinds of operations pose acute risks to humans at all times. Our experience shows, however, that disrupting critical civilian infrastructure has particularly severe consequences in societies that are already weakened by armed conflict.

Adverse humanitarian consequences are *not* inevitable. States must take decisive steps to ensure that their use of cyber operations during armed conflict complies with existing rules of international law. In the ICRC's view, this requires action at the international and at the national level.

At the international level, States have affirmed that international law applies in the ICT environment. This comprises, first and foremost, States obligations under the UN Charter, in particular the prohibition against the use of force and the obligation to settle international disputes by peaceful means. Most recently, the UN Group of Government Experts also noted that 'international humanitarian law applies only in situations of armed conflict'. The group recalled 'the established international legal principles including, where applicable, the principles of humanity, necessity, proportionality and distinction that were noted in the 2015 report', and it recognized 'the need for further study on how and when these principles apply to the use of ICTs by States and underscored that recalling these principles by no means legitimizes or encourages conflict'.[4] The ICRC fully supports this view: cyber operations during

armed conflict are not happening in a 'legal void' or 'grey zone' – they are subject to the established principles and rules of international humanitarian law.

To ensure that international humanitarian law is understood and applied effectively, the ICRC welcomes further study of how and when this field of law applies. To avoid adverse humanitarian consequences and disruption of societies, we ask States to interpret and apply the rules and principles of international humanitarian law in a manner that takes into consideration the specific characteristics of the ICT environment. Essential questions on the protection of civilian life require further study and clear positioning by States. For instance, in an increasingly data-driven world, it should be a priority for States to agree that civilian data enjoys protection against attack, just as civilian paper files do. Moreover, States should affirm that cyber operations that damage civilian objects by disrupting their functionality are subject to all international humanitarian law rules on the conduct of hostilities.[5]

While further study and agreement on how international law limits cyber operations during armed conflict is important, these rules will only become effective through implementation at the national level. From discussions with military operators and experts, the ICRC identified a number of key steps on how States can, and should, avoid civilian harm from military operations during armed conflict.[6] Today, we would like to emphasize four of them:

- **First**, each State is responsible for all its organs involved in cyber operations and other actors that act on that State's instructions, or under its direction or control. States must ensure that all of these actors respect international humanitarian law.

- **Second**, States should develop clear internal processes to ensure that if cyber means or methods of warfare are used, they comply with the applicable legal framework.

- **Third**, States have an obligation to take all feasible precautions to avoid or at least minimize incidental civilian harm when carrying out attacks, including through cyber means and methods of warfare. In the ICT environment, this may include implementing technical measures such as 'system-fencing', 'geo-fencing', or 'kill switches'.[7]

- **Four**, States also have an obligation to put in place measures to protect the civilian population against the dangers resulting from military cyber operations. Some of these measures may have to be implemented already in peacetime.

To conclude, the ICRC commends member States for striving to advance international dialogue and agreement on the potential human cost of cyber operations and measures to prevent and mitigate human harm. In our view, international humanitarian law must be part of such debates, and the ICRC remains available to lend its expertise to them.

Thank you.

---

[1] Open-Ended Working Group, Final Report, 2021, para. 16; GGE, Final Report, 2021, para. 7.

[2] Open-Ended Working Group, Final Report, 2021, para. 18.

[3] See ICRC, The Potential Human Cost of Cyber Operations, 2019.

[4] GGE, Final Report, 2021, para. 71(f).

[5] See further ICRC, International humanitarian law and cyber operations during armed conflicts: ICRC position paper, 2019.

[6] ICRC, Avoiding Civilian Harm from Military Cyber Operations During Armed Conflicts, 2021.

[7] 'System-fencing' means preventing malware from executing itself unless there is a precise match with the target system, 'geo-fencing' means limiting malware to only operate in a specific IP range, and 'kill switches' signify a way to disable malware after a given time or when remotely activated.

Related