The law of war imposes limits on cyber attacks too

Cyber warfare is limited by rules, and civilian computers, networks and cyber infrastructure are protected against cyber attacks.

These are among the conclusions reached by a group of legal and military experts in a manual on international law applicable to cyber warfare (Tallinn Manual). Laurent Gisel, legal adviser at the ICRC, explains why this is an important step towards reducing human suffering.

What is cyber warfare and why is the ICRC concerned?

By cyber warfare, we’re talking here solely about means and methods of warfare that consist of cyber operations amounting to, or conducted in the context of, an armed conflict, within the meaning of international humanitarian law (IHL). IHL does not apply to every kind of activity called “cyber attacks” in common
Cyber networks are vulnerable. When the computers or networks of a State are attacked civilians could be deprived of basic essentials such as drinking water, medical care and electricity. Cyber attacks could interfere with rescue services that save lives or disrupt vital infrastructure such as dams, nuclear plants and aircraft control systems. The well-being, health and even lives of hundreds of thousands of people could be affected. One of the ICRC’s roles is to remind all parties to a conflict that constant care must be taken to spare civilians: wars have rules and limits that apply to all means and methods of warfare.

In the Tallinn Manual, legal and military experts state that IHL applies to cyber warfare. Why is it important?

We welcome the fact that experts reaffirm the relevance of IHL to this new technology, as it is crucial to identify ways of limiting the potential humanitarian cost of cyber operations in armed conflict. We certainly hope that the Tallinn Manual can usefully contribute to further discussion among States on these challenging issues. The ICRC will continue to offer its expertise in IHL to address these challenges.

Means and methods of war have evolved since the Geneva Conventions were drafted in 1949, but IHL continues to apply to all activities conducted by parties in the course of armed conflict, and must be respected. It cannot be ruled out, however, that there might be a need to develop the law further to ensure it provides sufficient protection to the civilian population, as cyber technologies evolve or their humanitarian impact is better understood. That will have to be determined by States.
What was the role of the ICRC in this process?

The ICRC contributed, as an observer, to the experts’ discussions in order to ensure that the manual reflected as far as possible existing IHL and to uphold the protection IHL affords to the victims of armed conflicts. The manual sets rules and provides useful commentaries. The ICRC generally agrees with the formulation of the rules; however, there may be exceptions.

What are the main challenges raised by cyber warfare?

There is only one cyberspace, shared by military and civilian users, and everything is interconnected. The key challenges are to ensure that attacks are directed against military objectives only and that constant care is taken to spare the civilian population and civilian infrastructure. States have to be extremely cautious when resorting to cyber attacks.

Are hackers a legitimate target in cyber warfare?

Most cyber operations are not linked to an armed conflict, so IHL does not even apply. Even in armed conflict, most hackers would be civilians who remain protected by IHL against direct attack, though they would remain subject to possible criminal prosecution depending on what they did.

But if hackers take a direct part in hostilities, carrying out a cyber attack in support of one side in an armed conflict, they lose their protection against direct attack during the execution of the cyber attack.
Can cyber technology have positive uses in armed conflict?

When conducting military operations, States have an obligation to avoid or at least minimize incidental civilian casualties and damage to civilian infrastructure. Advances in technology might one day lead to the development of cyber weapons that would, in specific circumstances, cause fewer casualties and less collateral damage than traditional weapons, to achieve the same military advantage. The ICRC will continue to monitor developments in this regard.

Cyber weapons: what does international law say?

Assessing the legality of new weapons is in the interest of all States, as it will help them ensure that their armed forces act in accordance with their international obligations. Article 36 of the 1977 Protocol I additional to the Geneva Conventions requires each State party to make sure that any new weapons it deploys or considers deploying comply with the rules of IHL, a point usefully recalled by the Tallinn Manual.

At the 28th International Conference of the Red Cross and Red Crescent, in 2003, States party to the Geneva Conventions called for “rigorous and multidisciplinary review” of new weapons and means and methods of warfare, to make sure that the law’s protection is not overtaken by the development of technology. The use of cyber operations in armed conflict is a perfect example of such rapid technological development.