Cyberwarfare and international humanitarian law: the ICRC's position

What limits does the law of war impose on cyber attacks?

Does cyber warfare have limits and rules? Are civilian computers, networks and cyber infrastructure protected against cyber attacks? A group of international legal and military experts says "yes" in the recently published Tallinn Manual[1], a process in which the ICRC took part as an observer. Laurent Gisel, legal adviser at the ICRC, explains why the Tallinn Manual is an important step towards underscoring the relevance of international humanitarian law (IHL) in armed conflicts of every kind, with the aim of reducing human suffering.

Why is the ICRC concerned by cyber warfare?

The expression "cyber warfare" appears to have been used by different people to mean different things. The term is used here to refer to 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 IHL. The ICRC is concerned about cyber warfare because of the vulnerability of cyber networks and the potential humanitarian cost of cyber attacks. When the computers or networks of a State are attacked, infiltrated or blocked, there may be a risk of civilians being deprived of basic essentials such as drinking water, medical care and electricity. If GPS systems are paralysed, there may be a risk of civilian casualties occurring – for example, through disruption to the flight operations of rescue helicopters that save lives. Dams, nuclear plants and aircraft control systems, because of their reliance on computers, are also vulnerable to cyber attack. Networks are so interconnected that it may be difficult to limit the effects of an attack against one part of the system without damaging others or disrupting the whole system. 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, which apply just as much to the use of cyber warfare as to the use of rifles, artillery and missiles.

[1] *Tallinn Manual on the International Law Applicable to Cyber Warfare* – prepared by the International Group of Experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence, Cambridge University Press, 2013

A group of legal and military experts recently published a manual – known as the Tallinn Manual – stating that IHL applies to cyber warfare and setting out how the rules of IHL will play out in this area. Why is that important?

We welcome the fact that experts are thinking about the consequences of cyber warfare and the law applicable to it. The use of cyber operations in armed conflict can potentially have devastating humanitarian consequences. For the ICRC, it is crucial to identify ways of limiting the humanitarian cost of cyber operations and, in particular, to reaffirm the relevance of IHL to this new technology when used in armed conflict. This is precisely what the experts say in the Tallinn Manual. Means and methods of war evolve over time, and are clearly not the same as the ones available when 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.

While the Tallinn Manual is a non-binding document prepared by a group of experts, we certainly hope that it can usefully contribute to further discussion among States on these challenging issues, and that States and non-State armed groups will ensure that any use of cyber operations in armed conflict will be in accordance with their international obligations. There is currently much debate about how international law, including IHL, should be interpreted and how it should apply to State and non-State activities occurring in cyberspace. The ICRC will continue to offer its expertise in IHL to address these challenges.

This does not mean that IHL applies to any cyber operation or to all those that are often called "cyber attacks" in common parlance: IHL does not regulate cyber operations that fall outside a situation of armed conflict. Business corporations and governments are as much concerned by cyber espionage, cyber crimes, and other malicious cyber activity as they are by cyber attacks that would fall under IHL. The technical means of protecting cyber infrastructure from espionage or from an attack might be similar, but the law governing these operations is not. One of the key issues is therefore to identify the circumstances in which cyber operations may be regarded as occurring in the course of armed conflict, or giving rise to armed conflict in and of themselves, such that IHL would apply.

So what does the Tallinn Manual say on the scope of application of IHL in cyberspace?

The Tallinn Manual offers interesting perspectives in this respect. For example, it upholds the classical dichotomy between international and non-international armed conflicts, and recognizes that cyber operations alone may constitute armed conflicts depending on the circumstances – notably on the destructive effects of such operations. In this regard, the manual defines a "cyber attack" under IHL as "a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects." The crux of the matter, however, lies in the detail, namely what must be understood as "damage" in the digital world. After intense discussion, the majority of the experts agreed that beside physical damage, loss of functionality of an object may also constitute damage. The ICRC's view is that if an object is disabled, it is immaterial how this occurred, whether through kinetic means or a cyber operation. This issue is very important in practice, as, otherwise, a cyber operation aimed at making a civilian network

dysfunctional would not be covered by the IHL prohibition on targeting directly civilian persons and objects.

What was the role of the ICRC in this process and are its positions reflected in the manual?

The ICRC contributed, as an observer, to the discussions of the experts who drafted the Tallinn Manual in order to ensure that it reflects as far as possible existing IHL and to uphold the protection this body of law affords to the victims of armed conflicts. The 95 rules set forth in the manual reflect text on which it was possible to achieve consensus among the experts. The ICRC generally agrees with the formulation of the rules; however, there may be exceptions. For example, the rule that recalls the prohibition of belligerent reprisals against a number of specially protected persons and objects does not include cultural property, contrary to the finding of the ICRC's study on customary IHL. The manual also provides useful commentaries to the rules, including the expression of diverging views among the experts. One example of such divergence concerns the obligation of parties to an armed conflict to take all feasible precautions to protect the civilian population and civilian objects under their control against the effects of cyber attacks: while the manual's commentary argues that this rule's scope of application would be limited to international armed conflicts, the ICRC considers the obligation to apply in any type of armed conflict.

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. Furthermore, the expected incidental civilian losses and damage must not be excessive in relation to the concrete and direct military advantage anticipated by the cyber attack. If these conditions cannot be met, the attack must not be launched. The manual appropriately recalls in this regard that collateral damage consists of both direct and indirect effects, and that any anticipated indirect effect must be factored into the proportionality assessment during the planning and execution of an attack, a point highly relevant in cyberspace. These challenges underline the importance of States being extremely cautious when resorting to cyber attacks.

Are hackers a legitimate target in cyber warfare?

The term "hackers" encompasses so many people engaged in so many different activities that it cannot be said that hackers as such can be attacked. 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 – although they would remain subject to law enforcement and possible criminal prosecution depending on whether their activities violated other bodies of law.

The situation is different if hackers take a direct part in hostilities by way of a cyber attack in support of one side in an armed conflict. In such a situation, the hackers cannot expect the enemy to remain idle; they lose their legal protection against direct attack during the

execution of the cyber attack and the preparatory measures forming an integral part thereof.

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. Without underestimating the challenges, one cannot rule out the possibility that technological evolution might lead in the future 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, another 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.