Norms for responsible State behavior on cyber operations should build on international law

Statement to the UN Open-ended working group on developments in the field of information and telecommunications in the context of international security; Second substantive session; Agenda item "Norms, rules and principles"

Véronique Christory, ICRC New York
Distinguished chair, excellencies, ladies and gentlemen,

The International Committee of the Red Cross (ICRC) is grateful for the opportunity to address the second substantive session of the “Open-ended working group on developments in the field of information and telecommunications in the context of international security”.

In previous sessions, States and other stakeholders have raised important concerns about the threat that the malicious use of information and telecommunication technologies poses to critical civilian infrastructure. The ICRC shares these concerns. As highlighted in the position paper we submitted in November 2019, cyber operations that destroy, interrupt or manipulate critical civilian infrastructure can cause serious human harm – whether in times of peace or during an armed conflict.[1]

In the ICRC’s view, reaching consensus on norms, rules and principles is particularly important in rapidly-changing environments, such as those we are facing in the field of information and communications. In our view, discussions concerning norms for responsible State behavior are closely linked to, and should build on, international law, which the UN General Assembly recognized as applying in cyberspace.

In fact, some of the norms agreed in 2015, and endorsed by the General Assembly through the resolution creating this working group, reflect – at least in part – States’ existing international law obligations. This is especially the case if we consider cyber operations during armed conflict. In the ICRC’s view, cyber operations during armed conflict are regulated, and therefore restricted, by existing rules of international humanitarian law (IHL).

We would like to elaborate on this point with regard to two of the norms that aim to protect critical infrastructure.

Firstly, norm (f) stresses that no State should conduct ICT activity that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public, if such operations are contrary to the State’s obligations under international law.

In times of armed conflict, this norm reflects legally binding obligations under IHL.

For example, under IHL parties to armed conflict are prohibited from directing attacks against civilian objects.[2] This means that it is prohibited to use cyber means to destroy or disrupt critical civilian infrastructure – unless this infrastructure qualifies as a military objective.

Moreover, IHL prohibits attacking, destroying, removing or rendering useless objects indispensable to the survival of the population.[3] During armed conflicts, this rule prohibits, for example, the use of cyber means to manipulate and render dysfunctional water supply facilities.

IHL also demands that medical services be protected and respected.[4] Under IHL, parties to conflict must not harm medical infrastructure through cyber operations, and take great caution to avoid incidental harm. These rules are all the more important because health infrastructure is often not adequately protected from direct cyber attacks or incidental harm caused by cyber operations.

In our view, the particular vulnerability of health care facilities may also warrant the articulation of an additional norm of responsible States behavior. A possible new norm could elaborate on norm (f) and demand that States should not conduct or knowingly support ICT activity that would harm medical services or medical facilities, and should take measures to protect medical services from harm.

Secondly, according to norm (g), States should take appropriate measures to protect their critical infrastructure from ICT threats. Again, this norm reflects legally binding obligations under IHL.

In particular, existing IHL rules require States to take all feasible precautions to protect civilian objects under their control – including critical civilian infrastructure – against the dangers resulting from military operations. This is one of the few IHL obligations that States must already implement in peacetime. [5] What is feasible for each State depends, of course, on that State’s resources. One concrete measure to strengthen the protection of essential civilian infrastructure in cyberspace would be to segregate from the internet computer systems on which critical civilian infrastructure depends.[6]

To conclude, the ICRC reiterates the importance of protecting critical civilian infrastructure against harmful cyber operations. When discussing existing and possible new norms in this respect, the ICRC encourages States to consider, and to build on, their existing legal obligations under IHL.

Thank you.

[2] Arts 48, 51 and 52 Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (API); Rules 1 and 7 ICRC Customary IHL Study.

[3] Art. 54 AP I; Art. 14 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.

[4] 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.
