The Objective: Laws of War for Cyber Warfare

The International Committee of the Red Cross enforces the Geneva Convention in cyberspace, preparing for the day when a cyber warfare attack will lead to a war between countries. Exclusive interview

By Ami Rojkes Dombe

The Red Cross in Afghanistan *(Photo: AP)*

Cyber warfare has evolved into a fifth dimension of warfare for many countries, including Israel. As such, the Laws of War apply to it. The organ responsible for supervising the application of the Geneva Convention is the International Committee of the Red Cross (ICRC), which has recently been dealing with the cyber warfare context of the Convention. Among other things, ICRC reviews the question of whether the existing Laws of War are sufficient in order to cover the cyber warfare dimension as well. Meanwhile, most of the ICRC's activities are conducted opposite the countries that are signatories to the Convention, including Israel, so as to raise the level of awareness regarding the Laws of War during the development stages of those countries' technology and exports. In the future, when warlike events take place in cyberspace, ICRC will have to investigate those events just as it does in the physical world.

State Supervision during Development

"We are responsible for ensuring that the Laws of War are upheld in cyberspace, too," says Larry Maybee, Head of the Legal Department for the International Committee of the Red Cross (ICRC) Delegation for Israel. "This compels us to review technologies that are being developed, among other things, cyber technology and autonomous machines ("Killer Robots"). These are the two technologies currently on the agenda. Our objective is to cooperate with the Government of Israel and the IDF and see to it that when those technologies are being developed, it is done according to the Laws of War. In this context, cyber technologies may be used for warlike activities.

"A part of the problem is understanding what is relevant to an armed conflict and what isn't. A clear distinction should be made between (different) activities (taking place) in cyberspace – hacking, crime, espionage or war. Only a small percentage of cyberspace activities are warlike activities. These are acts that could ignite physical warlike activities between countries or between a country and a non-state organization. When and how a cyber warfare attack can ignite a war – that is the question. That is what our interest focuses on.

"A part of the problem is terminology. We must all use the same terms. I am not aware of any agreement in cyberspace that covers the Laws of War according to the Geneva Convention. Under that Convention, there is an undertaking of the signatory countries according to which they are obliged to develop weapons that comply with these laws. This pertains to cyber weapons, too, namely – every country should have a control mechanism that reviews the development of cyber weapons so that they comply with these laws.

"Today, countries do not admit that they were attacked, that they are vulnerable or that they had initiated successful (cyber warfare) attacks. A part of the discussions being conducted around the world addresses the question of when a cyber warfare attack ignites a physical counterattack. Attribution is another major challenge. How to identify the attacker. It is very difficult to know who was responsible for the attack, and that affects the Laws of War – how a country would react.

"We try to figure out whether the existing Laws of War are sufficient to be applied to cyber warfare, too. We have statutory power on behalf of the countries that are signatories to the Geneva Convention. A part of it is monitoring the development of the Laws of War. They change all the time. We also have to develop an ability within the organization to understand the technology, but that is difficult, mainly because of the challenge of gaining access to the places where that technology is being developed.

> "Countries that were the victims of cyber warfare attacks understand that the existing laws do not cover war in cyberspace. It is a major challenge"

"We remind countries possessing cyber warfare capabilities of their commitment to the Convention," says Maybee. "It is their commitment. Our job is legal primarily – to check whether the laws are consistent with the technology. If not – they should be revised. With certain technologies, like blinding lasers, countries had developed restrictions regarding the application of the laser (system) before it was developed. The same goes for robotic weapons, too. We are constantly conducting classified discussions with countries and also take part in international processes.

"We occupied a supervisory position at the discussions around the Tallinn Manual on the International Law Applicable to Cyber Warfare. That was a process initiated by NATO. That manual is important as it provides the basis for legal interpretation regarding cyber warfare. Admittedly, it has also left many questions unanswered, but that is a process under consolidation. It is an example of a process where countries convene to discuss the implications of technology in the context of the Laws of War.

"In the context of Killer Robots, one of the questions is how the machine selects a target. If there is no man in the loop, how can you verify who is protected and who is a legitimate target? What threatens the machine? From the perspective of ICRC, we are not saying that the development of one technology or another should be banned, but rather that the development should take the Laws of War into consideration. What will happen if an automatic machine kills people by mistake, whose fault is it? The Laws of War apply to a specific person who made a decision. In the case of a machine, whose fault is it? The programmer? The designer?

"We have weapon system specialists in Geneva as well as a cyber warfare specialist. He develops the positions of ICRC regarding the legal aspects of cyber warfare. We communicate intensively with the Government of Israel on this issue. One should bear in mind that we are not the technology police. We do not have the resources to monitor every private cyber technology company. Our work is mainly opposite the organizations in charge of the technology export process (IMOD/DECA – Defense Export Controls Agency). ICRC does not replace the local government, but only raises the awareness of the issue. The country is the party that sets forth the regulation."

War Crimes in Cyberspace?

"Countries that were the victims of cyber warfare attacks understand that the existing laws do not cover war in cyberspace," explains Maybee. "It is a major challenge. In order to enact new laws for the Geneva Convention, the signatory countries must reach a consensus around a set of laws for cyber warfare. Even after that, only countries that are signatories to the Convention will be bound by those laws. It is by no means an easy process.

"We had discussions in Geneva attended by specialists from different countries regarding the challenges of the Laws of War in the context of cyber warfare. We did it in the past for various technologies such as cluster bombs, mines or chemical weapons. It is not a new process when a new technology enters the battlefield. These discussions are classified.

"I do believe that countries can reach general guidelines around the proper conduct in cyber warfare. For example, not to attack infrastructures supplying ➜

The Red Cross *(Photo: AP)*

> "We operate in 80 countries. Wherever there is a conflict – we will be there. We will have to gain an understanding of cyber technology to remain relevant"

water and food to civilians. The problem is enforcing those laws when dual-function targets are involved. When you attack the grid of the electrical corporation, you damage the military as well as the civilian population. The same goes for air traffic control. How can you ensure that civilian flights are not damaged? The differentiation is a challenge. To this day, an armed attack was regarded as such if physical damage was inflicted. The Tallinn Manual resolved this issue by stating that an attack does not have to include physical damage. Even definitions like this one are important.

"One of the questions is when you will be able to prosecute someone for war crimes in cyberspace. For example, in the context of UAV operation, if you are a civilian who operates UAVs for the military (a sub-contractor), you will be committing a war crime, as if you were a soldier, it would be your job, but as a civilian, you do not have the legal defense that soldiers have. Some laws cover mercenaries that work for governments. The challenge is to establish the link between a country and a non-government party. In cyberspace, attribution is highly problematic. It is a challenge to attribute war crimes to parties involved in cyber warfare attacks." ICRC also investigates warlike events, and in this context it will be called upon in the future to investigate cyber warfare events. For this purpose, the organization will have to maintain specialists who would be able to reach a site that had experienced a cyber warfare attack, and determine whether the attack complied with the Laws of War. "We have the right to investigate cases during the actual fighting," says Maybee. "Today we have specialists who know how to investigate events of kinetic warfare. In the future, we will require specialists in the field of cyber warfare, too. If you want to reach a conclusion as to whether the use of technology was legal or not, you will need the knowledge to investigate. We operate in 80 countries. Wherever there is a conflict – we will be there. We will have to gain an understanding of cyber technology to remain relevant."

As ICRC deals with supervision for the purpose of determining that the Laws of War are actually upheld, it is only logical that it should employ the same new technologies it monitors, like UAVs or cyber technology. "If we want a Red Cross UAV to fly over Syria, we need the consent of the warring parties for that," explains Maybee. "Our UAV should be identifiable as belonging to the Red Cross, rather than as a threat, as otherwise it will be shot down. Ten years ago we had discussions around the question of how we should monitor the new weapon system, and we did it.

"Owing to the difficulty of monitoring the battlefield in real time, we invest in connections with the countries that develop the weapon systems. In Israel we are in contact with IDF and the government. We have good connections with jurists in the military around a range of issues that pertain to war. The standard of discussions we have in Israel is better than what we have in many other countries. We have been here for 50 years. Many wars have taken place here. In other countries it is different, and in other places they do not always cooperate with us as they do here. There are conflicts where one of the sides is a non-government organization and it is more challenging (for us) to communicate with them, but we always try.

"In the context of cyber warfare, programmers should teach themselves the Laws of War. They should step out of their professional and commercial envelope and understand what the tools they are developing can do. They need to develop social ethics and be aware of the fact that there is a context that is broader than their private world. They need to be more responsible. The government, for its part, should control the development and exportation of the technology. Admittedly, there is always tension between the economic reality and the legal and moral aspirations. But everyone should be aware. Imagine Asia or other regions that are less strictly supervised and have no regulation. It is a major potential threat." ⦿