PRESENTATION BY MR. IAN BRASURE, LEGAL ADVISOR AND SPECIAL ADVISOR TO THE ARMED FORCES DEPARTMENT, REGIONAL DELEGATION OF THE INTERNATIONAL COMMITTEE OF THE RED CROSS (ICRC) FOR THE UNITED STATES AND CANADA

BEFORE THE COMMITTEE ON JURIDICAL AND POLITICAL AFFAIRS OF THE ORGANIZATION OF AMERICAN STATES

24 JANUARY 2019

Good afternoon, Ladies and Gentlemen. It is a great privilege to be with you today to represent the International Committee of the Red Cross and summarize our positions on the important intersection between international humanitarian law and the increasing role new technologies play in armed conflict, specifically, autonomous weapons and cyber warfare.

As a starting point for my remarks, which I hope will generate a good discussion to follow, it is important to acknowledge that technological advances in the weapons of war are not new and understand that international humanitarian law remains capable of providing authoritative answers, even for the most contemporary challenges. Historical advancements in the weapons of war include the spear, bow and arrow, rifle, machine gun, ballistic missile, and nuclear weapons, to name a few. Although the challenges associated with lethal autonomous weapons systems and cyber operations present some unique challenges, international humanitarian law provides firm guideposts for the further development and use of these technologies.

AUTONOMOUS WEAPONS SYSTEMS

The idea of developing autonomous weapons is nothing new, and much of the earliest planning and use of autonomous or semi-autonomous weapons date back centuries. In fact, in 1495, Leonardo da Vinci produced a draft design of a "mechanical knight" that would be capable of mimicking a range of human motions. In 1898, Nikola Tesla unveiled the first wireless remote-controlled vehicle, a small iron-hulled boat, before a crowd in New York's Madison Square Garden. In 1950 British mathematician Alan Turing, whom many consider the godfather of artificial intelligence noted in his writing "I propose to consider the question, 'Can machines think?'"

At this point, it may be helpful to provide some definitions to ensure we all have a common understanding of what we are talking about.

The Oxford English Dictionary defines the word autonomous as follows:

1.1 Having the freedom to act independently

1.2 Denoting or performed by a device capable of operating without direct human control

I find it incredibly interesting, too, that the Greek origin of the word autonomous translates into "having its own laws."

The ICRC has characterized autonomous weapon systems broadly as

> Any weapon system with autonomy in its critical functions. That is, a weapon system that can select and attack targets without human intervention. After launch or activation by a human operator, the weapon system – though its sensors, programming (software algorithms) and connected weapon(s) – takes on the targeting functions that would normally be controlled by humans.

In other words, the weapon system self-initiates the attack. This encompasses any weapon system that can independently select and attack targets, including some existing weapons as well as potential future systems.

Technical sophistication is not the defining characteristic of whether a weapon is autonomous, rather it is whether the weapon system self-initiates the attack. Therefore, notions of “automated” and “autonomous” weapons are interchangeable because they raise the same legal, ethical and humanitarian questions. This is why the ICRC intentionally includes both “dumb” and “intelligent” autonomous weapon systems.

A weapon could be very simple and “unintelligent” in its design, but highly autonomous in its critical functions (for example, a machine-gun that is triggered by a motion or heat sensor). In fact, a “dumb” autonomous weapon systems could even raise greater legal concerns, and lead to worse humanitarian consequences. In addition, predictability in programming of a weapon system does not necessarily equal predictability in consequences. Autonomous weapon systems all raise questions about predictability, owing to varying degrees of uncertainty as to exactly when, where and/or why a resulting attack will take place.

HUMAN CONTROL

The ICRC has posited that **human control must be maintained for both legal and ethical reasons**. Indeed, the loss of human control over the selection and attack of targets in armed conflict could entail significant humanitarian consequences and IHL violations. In addition to questions about IHL compliance, autonomy in the critical functions of weapon systems raises profound ethical concerns about the erosion of human responsibility for decisions to kill, injure or destroy.

The ICRC is of the view that civilians are put at risk when the design and/or the use of a weapon system with autonomy in its critical functions prevents the human commander or operator from making the judgments required by IHL. It is not machines that ‘apply’ or ‘respect’ the law, it is humans who are responsible and accountable for respecting the law.

This responsibility and accountability cannot be transferred to a machine, a computer program, or a weapon system. It follows that human combatants will need to retain a level of control over weapon systems and the use of force so that they can make context-specific legal judgments in specific attacks as required by IHL, notably the rules of distinction, proportionality, and precautions.

Human control is also critical to ensure accountability, as it is unclear how responsibility could be attributed in relation to unpredictable acts by autonomous weapon systems. There are doubts about the capability of developing and using autonomous weapon systems that would comply with IHL in all but the narrowest of scenarios and the simplest of environments, at least for the foreseeable future.

Moreover, the loss of human agency in decisions to use force, diffusion of moral responsibility and loss of human dignity raise profound ethical concerns. From an ethical perspective, human control would be required to a level that preserves human agency and upholds moral responsibility in decisions to use force.

CYBER WARFARE

Turning our attention now to the topic of cyber warfare, I will begin by noting an important function the ICRC performs. Specifically, I am addressing the importance of conflict classification, which is the process by which we use to consider the two main categories of armed conflict: international armed conflict, and non-international armed conflict. Conflict classification is critically important for two reasons. First, it identifies the law that applies to the conflict. Second, conflict classification clarifies the legal basis for ICRC action.

It is important up front to note that armed conflict is triggered by attacks, and the ICRC recognizes that many cyber “attacks” or intrusions are NOT considered attacks under IHL. Under Article 49, of Additional Protocol 1 to the Geneva Conventions of 1949, attacks are defined as “acts of violence against the adversary, whether in offence or in defence.” It is ICRC’s position that cyber operations that merely capture data related to commercial consumers does not rise to the level of an attack within the meeting of Article 49, and therefore does not rise to the level of an armed conflict. ICRC’s position is clear, however, that cyber operations having similar effects to classic kinetic operations will trigger the application of IHL requiring the parties to adhere to all of the rules and principles, such as distinction, proportionality, and precautions in attack.

To illustrate the challenges cyber operations present in determining the classification of conflict, and accordingly the applicable law, be aware that one of the intended characteristics of cyber warfare is the lack of attribution and purposeful ambiguity.

One of the best examples that combines the challenges related to attribution and ambiguity and the difficulty of accurately classifying the conflict is the unclear facts surrounding the discussion of the Stuxnet Virus. As reported in the media, the Stuxnet Virus may have been a collaboration between the two allied governments to attack Iran’s nuclear weapons program. Some reports indicate that the cyber-attack resulted in substantial physical damage to Iran’s centrifuges, which are designed to separate nuclear material.

In trying to assess what body of law applies to the reported use of the virus, consider the fact that the two ally States deny involvement in the cyber-attack, and finally consider the fact that Iran denies such an attack occurred at all.

In addition to the challenges of attribution and ambiguity, another central challenge associated with cyber operations pertains to dual use objects and systems. Dual use objects are those that may be used by the military, and therefore may lawfully be subject to attack, and civilians objects or systems that are immune from attack. The **interconnectivity of military and civilian computer systems** **increases the risk that the effects of an attack might spread beyond the intended target**. This heightened attention can be attributed to the increased interconnectedness and interdependence of modern societies.

Another challenge associated with cyber operations pertains to the status of those conducting cyber warfare. Are hackers subject to attack? The term hacker encompasses too many people in different activities, so they are not lawful targets under IHL. Most cyber activities are not linked to armed conflict, so IHL doesn't apply. Even during an armed conflict, most hackers would be civilians protected by IHL. BUT, if hackers are directly participating in hostilities in support of one side to the armed conflict, they may lose their legal protection against direct attack during the execution of the cyber-attack and the preparatory measures forming an integral part thereof.

In closing, it is clear that emerging technical capabilities related to autonomous weapons systems and cyber warfare present growing challenges as they are increasingly employed during armed conflict. However, the ICRC position is clear that existing IHL provides the parties to armed conflict with authoritative navigational tools to ensure that the development and implementation of these technologies in armed conflict are consistent with IHL.