

**LEGAL AND
ETHICAL ASPECTS
OF AUTONOMOUS
WEAPONS,
CYBERATTACKS, AND AI**

Igor Kotsiuba

Partner, CyberDesk



Conference proceeding

Behind the Digital Curtain. Civil Society vs State Sponsored Cyber Attacks

Brussels - 25/06/2019

DOI 10.34054/bdc000

One of the most important principles is the principle of proportionality, which means that damage to the civilian population and civilian objects cannot exceed the military advantage that the party expects to receive utilizing a cyber attack. The most significant difficulties, in this case, arise because of the close interconnection of civilian and military objects as well as civil and military infrastructure in cyberspace. Military facilities from IHL are those objects that by their location and purpose make an effective contribution to the military success of the state.

It is tough to make this distinction in cyberspace, when, for example, GPS-navigation, computer networks, the Internet work both

for the civilian population and the success of the military operation. There is a great risk that civilian objects will be considered as dual-purpose objects and be destroyed - in cyberspace, however, almost everything will be a dual purpose object. How, in this case, does one consider this proportionality, how does one protect the civilian population and how does one determine if the damage to the civilian population would outweigh the military advantage or not?

Also, the state will need substantial technical expertise to anticipate and calculate whether any damage will be done at all. From the point of view of the IHL, this involves the responsibility of the State party to the conflict: to cal-

culate the damage, to provide for the possibility of a return journey, if it becomes clear that the civilian objects will suffer during the attack. But it is much easier to give instructions to stop a tank on its way to a city than to stop the work of viruses that have already been launched into a computer system, and the result of which was the failure of the objects.

Thus, although we can assert affirmatively that IHL regulates cybercrime, it obviously requires considerable refinement. Particularly relevant in the context of the application of IHL in cyberspace are the following issues:

- the contradiction between anonymity on

the Internet and the need for individual criminal responsibility for military offenses,

- the state's obligation to ensure IHL compliance by States in cyberspace,
- direct participation in cyberconflicts and its possible consequences for IT companies and other possible non-state actors, even just private campaigns in military operations using computer technology.

Cyber-attacks can cause humanitarian problems, in particular, if they are not limited to the impact on a specific computer or computer system. Indeed, their results are usually seen in the real world.

There is, however, which is a certain complexity - the anonymisation of information. When conducting cyber attacks, autonomous weapon attack - anonymity is rather a rule than an exception. In some cases, it is not possible to determine the sender. The main challenge stems from

the fact that all rights are based on the establishment of liability (in the IHL these are parties in the conflict or individuals). In particular, if it is impossible to establish who carried out a particular operation and, accordingly, if it is impossible to establish its connection with the armed conflict, it will be challenging to determine whether the IHL is generally applicable to this operation.

Technological Capabilities and Requirements of the IHL.

Obviously, I have to determine if there are stand-alone armaments that reach such a level of difference, proportionality and precautionary measures, or if they can be developed in the future. Therefore, first of all, it should be made clear that if technically it is not possible to comply with certain requirements of the IHL with automated weapons, this is not enough reason to refuse these requirements. The use of

Compared to personal battles, all these technologies have simplified war. This question concerns the admissibility of war (jus ad bellum) and the issue of disarmament.

autonomous weapons will simply be illegal. Current international meetings are in fact being focused on such issues.

The countries of the "big twenty" first agreed on the principles of handling artificial intelligence (AI). They are listed in a joint statement released on Saturday, June 8, 2019, according to the G20 summit in the Japanese city of Tsukuba.

Ease of Use of Force and Warfare

Some argue that using automated weapons it is easier to wage war and use force outside the state. But this is also true for many types of weapons and technology - it was true for new weapons in the Middle Ages, and it was true when the first artillery, aircraft and modern fleets were developed. Compared to personal battles, all these technologies have simplified war. This question concerns the admissibility of war (*jus ad bellum*) and the issue of disarmament. It is understood that robots also fall under the general disarmament problem.

It may well be that (the possibility of) secrecy around the use of automated weapons and, as a result, the difficulties of attribution complicate the implementation of state liability and international criminal responsibility for

the act of aggression. On the other hand, the fact that computer systems record everything simplifies the request for criminal liability, at least when the party uses automated weapons.

In addition, there may be a psychological problem, but I can not judge its reality. It can be argued that those who build and program automated weapons and those who can be the last person in a loop, even without knowing where these weapons will be used, feel less responsible. But there is no scientific research on such an effect or the opposite.


Robots and Systems are Not the Addressees of the Law

When trying to apply IHL norms, there are some preliminary questions that need to be clarified. Only human beings obey the Rules

of Law, and only people are obliged to adhere to them. In the case of automated weapons, the IHL applies to those who develop, manufacture, program, and decide on their use. Regardless of how far we go into the future and regardless of how artificial intelligence will work, people will always be involved, at least during the conception of a machine. The man will decide that this car will be created, and then create a car. Even if one day the robots are being built, it's still the person who built the original work. This person is bound by law. The machine is not legally bound.

The Advantages are Not to Be Human.

The main advantage of automated weapons or automated cyber attacks, from the point of



view of IHL compliance, is that only humans can be inhumane, and only people can deliberately decide not to follow the rules. As soon as the robots have artificial intelligence, it is necessary to make sure that such an intelligence is not used - since intellectual intelligence is sometimes used - to circumvent the rules or to solve from an utilitarian point of view that failure to comply with IHL instructions as it is the best way which facilitates the achievement of the main goal of overcoming the enemy.

The Fundamental Issues of the IHL Have Become More Acute.

The most elementary question that comes to mind is the definition of most armed conflicts, since outside the armed conflict robots could only be used if they could arrest a person and not use (deadly) force. As we know that there is no uniform defi-

nition of armed conflict, the issue is rather an international armed conflict and is not an international armed conflict.

What is the lower threshold of violence between the state and non-state actor (or between non-state actors), which makes it an armed conflict? This is not a specific issue for robots, and even where automated weapons are used, the answer must be given and given by the person. But the answer is even more important when using automated weapons.

Many other questions need to find an answer before an automated weapon can be programmed, for example: What is the geographical scope of the IHL and what constitutes the battlefield?

Automated weapons raise the latter issue more acutely, but legally, considerations should be the same as for air bombing: can a belligerent attack on a target that would be a legitimate goal under IHL, far from the actual struggle, be restrained

only by the rules of the IHL? Or in this place, the IHL does not apply at all? Or is international human rights law predominant as *LexSpecialis*?

Legal Issues for Autonomous Weapon Systems (AWS) and Autonomous Cyber Attacks

The main problems facing AWS from a legal point of view are twofold: on the one hand, AWS will adhere to the principle of distinction, and on the other hand, they must perform the same, if not a more demanding task, compliance with the principle. Proportionality, which states that, before the deployment of any weapon system, each State Party must determine whether a new weapon, means or method of warfare it is studying is being used. , developed, acquired or accepted, in some or all circumstances, will be prohibited by international law. This section, after a short

introduction, places these principles in the IHL and focuses on (1) the principle of distinction, (2) the principle of proportionality, and (3) attempts to outline the problems that cause the introduction of AWS in any combat roles.

Conclusions

The IHL has been elaborated on great detail in a number of areas, including the types of weapons that can be used in armed conflicts, and types of legitimate purposes.

The nature of aggression in Ukraine and the hybrid war, with its massive cyberattacks, showed that where there are indicators, their diplomatic assessment, OSINT and the results of modern criminology, all lead to understanding but not to responsibility. Similarly, cyberspace and attacks today, as well as autonomous lethal weapons of tomorrow, will have indicators, a diplomatic assessment, but too blurred of a legal conclusion and the irreversibility of responsibility.

Web: www.promoteukraine.org
Contact: info@promoteukraine.org

Promote Ukraine is a non-profit start-up. It is a politically and governmentally independent organization situated in Belgium. It consists of a thriving team of professionals who on a pro bono basis seek to give voice to Ukrainian civil society in Europe and, in particular, throughout Belgium. We believe in European values such as civil rights, good governance and equal opportunities. Through connecting EU businesses and politicians with Ukrainian stakeholders, we facilitate the sharing of best practices between EU and Ukrainian partners with the goal to bring Ukraine closer to EU norms and values from a bottom-up perspective.



 [promoteukraine](https://www.facebook.com/promoteukraine)

 [promoteukraine](https://twitter.com/promoteukraine)

 [promoteukraine](https://www.instagram.com/promoteukraine)