**MilanMUN 2024** Research Report

# Regulating the Use of Lethal Autonomous Weapons and Cyber Warfare Techniques

Student Officer **Jennyfer Lavinia Soncina**

Committee **GA1 • DISEC**

## Introduction

The regulation of lethal autonomous weapons and cyber warfare techniques requires the establishment of guidelines and international agreements in order to address legal, ethical and security issues related to these technologies. Such regulations are needed in order to prevent malicious activities and a complete lack of accountability of potentially criminal and destructive acts.

## Definition of Key Terms

**Lethal Autonomous Weapons Systems (LAWS)** are weapon systems which employ computer algorithms and use sensors in order to autonomously identify and destroy targets without the need for direct human intervention.

**Cyber warfare techniques** involve the use of digital tools to attack computer systems causing critical technological damage to another nation's information networks. They can be used by nation-states or other malicious actors.

**CCW** stands for "Certain Conventional Weapons" (Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects); these are weapons that are thought to have excessively harmful effects on civilians and soldiers and cause unnecessary suffering.

**GGEs** (Groups of Governmental Experts) are appointed to study issues of concern and report findings at the UN General Assembly.

The **Principle of Proportionality** is a principle of International Humanitarian Law that states that

The **Principle of Distinction** is a principle of International Humanitarian Law that states that

# Background Information

## Classification of LAWS

The first difficulty we encounter when analysing this issue is that there is currently no universally shared definition of Lethal Autonomous Weapons Systems (LAWS). It might therefore be difficult to conclusively classify a particular weapon as "autonomous" or not; in addition, rapidly evolving technologies and the development of new hybrid systems may make it even harder to apply clear ethical distinctions.

When dealing with the problem of LAWS, however, delegates should keep in mind the following classification:

- **Automatic Defensive Systems**, such as land and naval mines; they are usually explosive devices automatically triggered by, for example, a human presence and have been in use for centuries;
- **Autonomous offensive systems**, such as loitering munitions (explosive drones or unmanned vehicles) and killer robots; a 2012 Human Rights Watch report classified these into three subcategories, depending on how much control humans have over them:
    - **human-in-the-loop** weapons can find targets but are only triggered by human action;
    - **human-on-the-loop** weapons are similar to the previous ones, but only require human supervision as opposed to direct action to trigger them;

- **human-out-of-the-loop** weapons can detect and destroy targets without the need for any kind of human interaction; these are also commonly known as “killer robots” or “slaughterbots” and might use Artificial Intelligence to select targets autonomously.

## Current Situation

### Automatic Defensive Systems

Anti-personnel mines were banned by the 1997 Ottawa Treaty (Anti-Personnel Mine Ban Convention), ratified by 164 states. Other automatic defensive systems, for example anti-vehicles mines or systems to intercept incoming missiles and other projectiles, are routinely used on ships and on land in several conflict areas (e.g. Israel’s “Iron Dome” air defence system). They are usually able to identify incoming threats based on criteria programmed by humans but do not require direct intervention to be triggered, because their response needs to be very fast. A possible concern connected to these systems is that they might misidentify targets (such as civil aircraft or vehicles) if not adequately programmed. Most major military powers do not support the expansion of bans to other defensive systems.

### Autonomous Offensive Systems

A number of military powers (including the United States of America, Russia, China, Israel, Iran, the United Kingdom, etc.) are currently developing drones, torpedoes, robots, ships, and other kinds of autonomous vehicles capable of carrying weapons or explosive payloads. The debate on the international stage has been heated for several years now, but no unanimous consensus has been reached yet.

Some have argued that LAWS as a whole violate International Humanitarian Law, because they cannot ensure the proper application of the principles of distinction and proportionality. Others say that it is hard to argue that all autonomous systems are unlawful as such, because their status depends on the effectiveness of each system in properly identifying military targets.

Some of the arguments arguments advanced by supporters of autonomous offensive systems are:

- they will increase military effectiveness, because AI has the potential to become even better than humans at identifying military targets, and because automatic systems work much better in environments in which field communications are disrupted or impossible;
- they constitute the future of warfare and states have a vested interest in developing them, as unfriendly powers will eventually come to master these technologies anyway;

- they are actually preferable to human fighters as they ensure losses are kept to a minimum.

Some of the arguments used by opponents of such systems are:

- by lowering the human cost for any country to go to war, they will increase the attractiveness of violent solutions to international disputes;
- it is often unclear whether a weapon is offensive or defensive, and the complex technology used to develop many of these systems makes it impossible to classify them clearly into any of the categories above;
- in modern warfare, military targets are often difficult to define (for example, when combatants are mixed with civilians); the delegation of life-or-death decisions to machines is inhumane and will make it much more likely that civilians will bear the consequences during armed conflicts;
- these systems could be used by non-state actors for any kind of malicious purpose;

Autonomous offensive systems, especially loitering munitions, have been around since the 1990s. However, the emergence of AI, according to several experts, poses a great danger as it has the potential of making these systems much more autonomous and of relying less and less on human action. Drones with heavier and heavier explosive payloads are currently being developed and used in Ukraine, Gaza, the Strait of Hormuz, Myanmar, among others.

## Cyber Warfare

There is no universally shared definition of cyber warfare either. While most agree that “cyber warfare” refers to state or state-sponsored actors carrying out attacks on a nation’s communication and information networks, some also include actions perpetrated by terrorist organisations and independent hackers. The goal is to cripple the attacked nation’s telecom infrastructure to limit its ability to wage war or to damage its security or stability.

The main techniques used in cyber warfare are: sabotage of military systems or critical civilian infrastructure (through malware such as “Stuxnet”); attacks on grids and telecommunications to cause blackouts; propaganda attacks; denial-of-service attacks (DDoS).

Cyber espionage and hacking of private companies are usually not considered cyber warfare. However, some operations of very large scale can cause tensions between nations. Examples include: the NSA’s “Prism” programme (worldwide), the Cambridge Analytica scandal (US and UK primarily), and several cases of government data breach.

In cyber warfare, complex techniques are used to protect the attackers' identity. Governments might use other entities (private companies, hackers, etc.) to carry out the attacks while still being able to deny they were behind them.

### Accountability

Ultimately, one of the most relevant concerns about both LAWS and cyber warfare is accountability and the attribution of potential crimes and abuses.

For completely automatic LAWS, military personnel and governments involved in potential misuses can easily pin any violation of International Humanitarian Law on machines themselves and that no specific individual or body can be held accountable. It means that a government might feel free to carry out extrajudicial killings with no fear of legal retribution.

In cyber warfare, the complexity of the attacks and the techniques used by hackers to conceal their origin create a situation where it is impossible to trace them back unequivocally to a single source. Accusations of hacking and cyber attacks between nations carry a high potential for escalation on an international level. The growing importance of these new technologies leads to the need to find a common agreement between the member states for the regulation of the use of such means.

## Major Parties Involved

### The UN

The UN Convention on Certain Conventional Weapons (CCW) became effective in 1983, with 127 parties as of to date. It instituted restrictions (but not total bans) that cover weapons that are deemed too destructive or indiscriminate in their targets, to protect civilians but also combatants from excessive suffering. The treaty restricts: weapons with fragments, landmines, incendiary weapons, laser weapons. The 1997 Ottawa Treaty (Anti-Personnel Mine Ban Convention), ratified by 164 states, then instituted a complete ban on anti-personnel mines.

The CCW parties held several discussions on a complete ban on LAWS, but all major military powers opposed it.

Several reports to the Human Rights Council (HCR) have also been very critical of LAWS. In 2013, UN Special Rapporteur on extrajudicial, summary or arbitrary executions, Christof Heyns raised alarms about the danger of LAWS used to carry out executions outside of any legal framework. In 2023, UN Special Rapporteur on counter-terrorism and human rights, Fionnuala Nī Aoláin, joined the Secretary-General in calling for a complete ban on LAWS due to their potential to violate human rights.

Secretary-General António Guterres has been very vocal against LAWS, arguing that they are “morally repugnant” and “politically unacceptable.” In the 2023 New Agenda for Peace, he called on member states to agree on a legally binding treaty to ban the development and use of human-out-of-the-loop LAWS (autonomous systems with no human oversight).

## The United States of America

The USA is making large investments in LAWS; its policy “neither encourages nor prohibits” the development of these systems. Officials agree that they raise important ethical issues, but also underline that they might have positive outcomes, such as limiting the loss of human life on battlefields. The government regularly participates in international talks on LAWS.

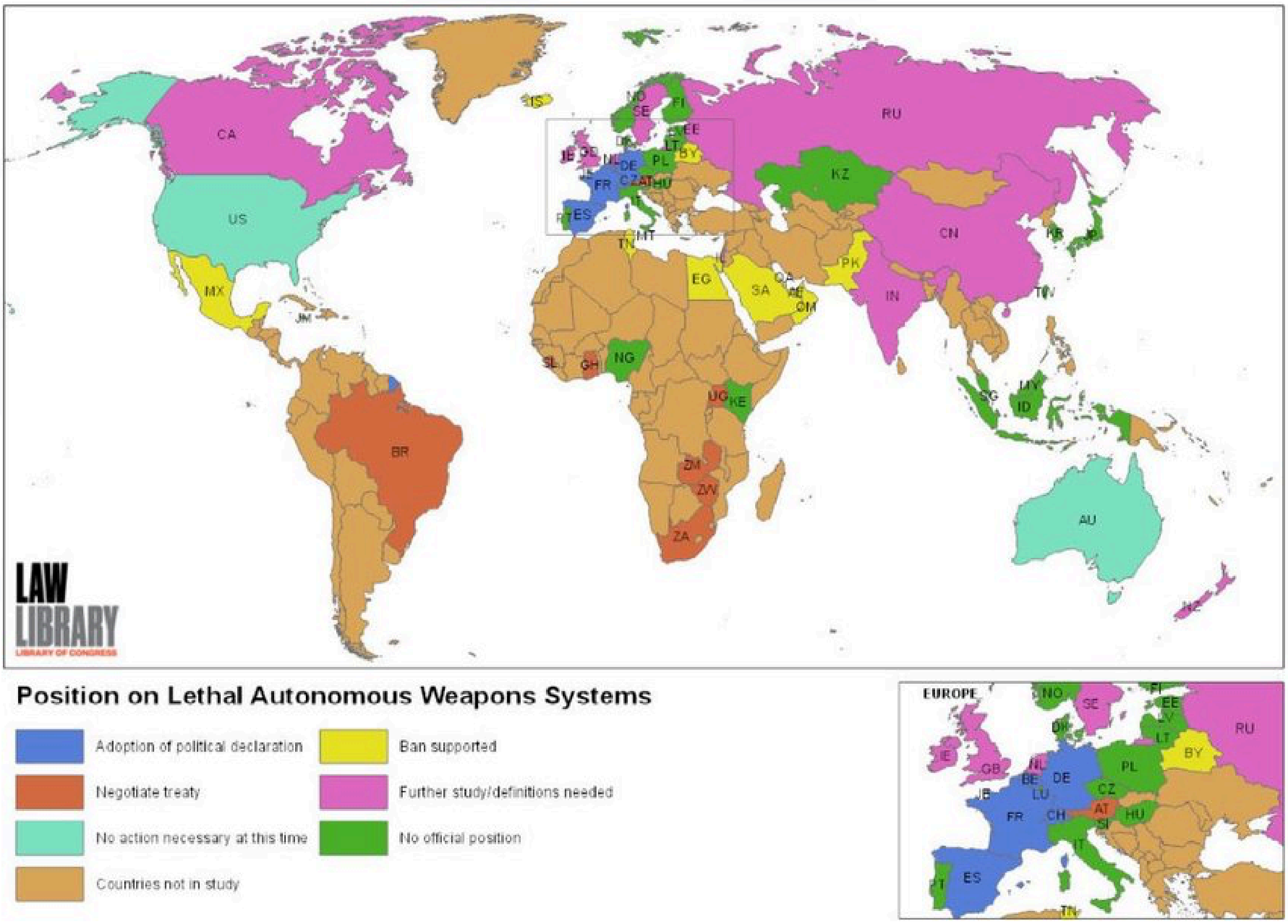
## China

China declared that fully autonomous systems create ethical problems and might violate humanitarian law. Its government called for a ban on the deployment of fully autonomous LAWS, but not on their development. It is actively investing on LAWS, although its officials cautioned that they might upend the international order.

## Russian Federation

Russia has argued that the degree of “human involvement” in LAWS is problematic and sometimes difficult to ascertain. Its government agrees that fully autonomous lethal systems might pose ethical challenges in the future, but it has consistently opposed negotiating binding international treaties on LAWS.

For more information on other countries involved, please see Stopping Killer Robots: Country Positions on Banning Fully Autonomous Weapons and Retaining Human Control | HRW or the map below.



Position on Lethal Autonomous Weapons Systems

**Source:** Created by the Law Library of Congress based on information provided in this report.

https://www.researchgate.net/figure/Positions-on-Lethal-Autonomous-Weapon-Systems-2_fig2_351662028

# Timeline of Relevant Events

2007 → NATO creates the Cooperative Cyber Defence Centre of Excellence (CCD CoE)

2013 → The Campaign To Stop Killer Robots is formed

2013 → The Tallinn Manual on the International Law Applicable to Cyber Warfare is published

2013 → CCW Parties agree on a LAWS mandate and start holding international talks

2016 → CCW Parties establish a GGE on Lethal Autonomous Weapons System

2020 → First attack on human target in Libya

2021 → AI guided attack in Gaza by Israel

# Possible Solutions

- Establishing international agreements in order to develop agreed norms for a responsible use of LAWs and cyber warfare.
- Institute universally accepted and respected standards for the design and use of such tools with he purpose of promoting transparency and alliances
- Call for more member states to ratify the 1997 Ottawa Treaty, and/or expand its scope to include other kinds of weapons

# Sources & Further Study

## LAWS

Robotics: Ethics of artificial intelligence | Nature

Lethal Autonomous Weapon Systems (LAWS) – UNODA

The Convention on Certain Conventional Weapons – UNODA

The Need for and Elements of a New Treaty on Fully Autonomous Weapons | Human Rights Watch

Defense Primer: U.S. Policy on Lethal Autonomous Weapon Systems

United Nations Office for Disarmament Affairs Treaties Database

Autonomous Weapons

Educating about Lethal Autonomous Weapons - Future of Life Institute

GGE on lethal autonomous weapons systems | Digital Watch Observatory

What you need to know about autonomous weapons | ICRC

Getting to grips with military robotics

Autonomous weapons are a game-changer

Pros and Cons of Autonomous Weapons Systems

Killer drones pioneered in Ukraine are the weapons of the future

## Cyber Warfare

NATO Review - Cyberwar - does it exist?

Who are the cyberwar superpowers? | World Economic Forum

Cyber Warfare | RAND

Massive Data Breach Puts 4 Million Federal Employees' Records At Risk

https://archive.nytimes.com/bits.blogs.nytimes.com/2010/09/24/malware-hits-computerized-industrial-equipment/

Merkel Compared NSA To Stasi in Complaint To Obama

U.S. Disrupts Hacking Operation Led by Russian Intelligence - The New York Times

Hacking Diplomatic Cables Is Expected. Exposing Them Is Not | WIRED

What is Cyber Warfare | Types, Examples & Mitigation | Imperva