ATLANTA INTERNATIONAL SCHOOL
MODEL UNITED NATIONS

AISMUN VI
Background Guide

Committee:
United Nations Office for Disarmament Affairs (UNODA)

Topic: Establishing International Guidelines for the Deployment of Autonomous Weapons and Cyber Warfare Technologies

AISMUN CONFERENCE

Table of Contents

Letter from our Chairs

Esteemed delegates,

Welcome to UNODA! Malaika Minja and I, Patricia Cánovas, will be your chairs for this committee. We're both juniors, and we've been in MUN for as long as we can remember and attended more conferences than I can count. We understand your experience as a delegate and know what it's like to be in your position: sometimes it's exciting, sometimes it's stressful, but we will ensure that you stay engaged and have a fun experience at AISMUN!

We're really looking forward to seeing the discussion and solutions that you all bring to the table! We're here for all of you, and feel free to ask any questions about parliamentary procedure throughout the conference. This background guide is here to help you, so please use it to familiarize yourself with the topic and our committee!

We can't wait to see all of you, and we hope you find this background guide helpful! Come prepared for thrilling debate, inspiring discussions, and incredible solution-making!

See you soon!

Patricia Cánovas & Malaika Minja

Introduction to the UNODA

The United Nations Office for Disarmament Affairs (UNODA) is a part of the UN responsible for reducing the risks posed by weapons and promoting peace through disarmament. It addresses nuclear weapons, conventional arms, and, more recently, emerging technologies that could play a role in warfare. The goal of UNODA is to make the world safer by creating agreements and rules around weapons while encouraging countries to work together rather than against one another. In recent years, the office has shifted more attention toward modern challenges such as autonomous weapons and cyber warfare, recognizing that these issues are becoming just as important as traditional weapons in shaping today's conflicts.

See their website for more information: https://disarmament.unoda.org/en

Key Terms

When discussing the international guidelines for autonomous weapons and cyber warfare technologies, several key terms and concepts are essential to understand. These terms are crucial in the context of global efforts to harness the benefits of these war techniques and address safety concerns. Here are some key terms:

Autonomous Weapons System (AWS): Weapons that can select and engage targets without direct human intervention once activated.

Lethal Autonomous Weapons System (LAWS): A subset of AWS capable of independently applying lethal force, which means that it could lead to death.

Cyber Warfare: The use of computer-based attacks by a state to disrupt, damage, or gain control over another state's system, infrastructure, or data.

Artificial Intelligence (AI): The simulation of human intelligence by machines, often essential for the creation of AWS or for cyber warfare.

Machine Learning: A method of Artificial Intelligence (AI) that enables systems to improve performance as they process data.

International Humanitarian Law (IHL): The body of international law that regulates conduct during armed conflict, including the principles of distinction, proportionality, and necessity.

Dual-Use Technology: Technology that can be applied for both civilian and military purposes. (Examples include: AI, drones, or cyber tools)

Cyberattack: Any attempt to expose, alter, disable, destroy, steal, or gain unauthorized access to computer systems or networks.

Critical Infrastructure: Essential systems and assets (ex., power grids, financial systems, healthcare networks) that, if disrupted, could impact national security or safety.

Cyber Defense: Measures taken to protect against cyberattacks.

Cyber Deterrence: Strategies aimed at discouraging adversaries from launching cyberattacks, often through the threat of retaliation.

Zero-day Exploit: A cyberattack that targets a previously unknown software vulnerability.

UN Office for Disarmament Affairs (UNODA): UN body working to promote disarmament in nuclear, chemical, biological, and conventional weapons, now increasingly engaged with new technologies.

Convention on Certain Conventional Weapons (CCW): Treaty framework often used to discuss AWS regulation.

Arms Control: International agreements or efforts aimed at limiting or regulating weapon development, deployment, and proliferation.

Topic Introduction

Autonomous weapons and cyber warfare are changing the way wars are fought. Autonomous weapons, often referred to as “killer robots,” are systems that can identify and attack targets on their own without direct human control. Cyber warfare, meanwhile, relies on computer systems to disrupt or damage things like infrastructure, government networks, or communication systems.

Both of these developments carry significant risks. If an autonomous weapon makes a mistake, it is unclear who should be held responsible. In the case of cyber warfare, it is often difficult to even determine which country or group carried out an attack. These uncertainties make it challenging for the international community to set clear rules. There are also major ethical concerns. Autonomous weapons could make it easier for countries to go to war since they reduce the risk to their own soldiers. At the same time, cyberattacks on power grids, hospitals, or water supplies can cause enormous harm to civilians.

Right now, the international community is divided. Some countries are pushing for a complete ban on autonomous weapons, while others believe regulation is a better path forward. Cyber warfare is even more complicated because it is so hard to prove who is responsible for an attack. The main challenge lies in creating global standards before these technologies cause greater harm.

Key Events

1972: Biological Weapons Convention- The first multilateral disarmament treaty was created, which banned the class of weapons of mass destruction, prohibiting the development, production, and possession of biological and toxin weapons.

1980: Convention on Certain Conventional Weapons (CCW)- This is the treaty framework that restricts autonomous weapons even in the modern world, and regulates "inhumane" weapons like landmines, blinding lasers, or incendiaries.

1988: Morris Worms Attack on the US- The first major computer worm, which was released by a Cornell graduate student, caused widespread network slowdowns and crashes, highlighting the vulnerabilities of computer networks and the significance of cybersecurity.

1991: Gulf War- The first "cyber-assisted" conflict, also called the first "information war," where early cyber techniques were used against Iraqi radar and communications.

1998-1999: Kosovo Conflict & NATO Cyber Operations- During the Kosovo Conflict, NATO conducted an air campaign against Yugoslavia, and experienced its first exchange with cyber warfare, suffering denial-of-service attacks and website defacements.

2001: Budapest Convention on Cybercrime- First international treaty on cybercrime, which improved cooperation among states, and set the precedent for "cross-border cyber governance."

2007: Estonia Cyberattacks- Distributed Denial of Service (DDoS) attacks on Estonia's fundamental infrastructure, which highlighted the vulnerability of modern states to cyber operations and pushed cyber norms forward.

2010: Stuxnet Attack on Iran's Nuclear Facilities- Incident that demonstrated the power of cyber weapons to produce physical effects, which led to raised issues of attribution, escalation, and regulation of state-sponsored cyber operations.

2013: Launch of *Campaign to Stop Killer Robots*- Civil Society and NGOs created an initiative calling for the ban of lethal autonomous weapon systems.

2017: Ukraine Ransomware Attacks- Large cyberattacks that spread globally and showed how cyber incidents can have huge effects on civil infrastructure and economies.

2019: CCW Establishes *11 Guiding Principles* for Autonomous Weapons: These principles outlined a shared understanding of autonomy, human control, and legality, but were not binding.

2024: Austria-led International Conference- The topic for this conference was "Humanity at the Crossroads: Autonomous Weapons Systems and the Challenge of Regulation," and helped to consolidate state practices, ethical norms, and wider support for autonomous weapons.

Key UN Suggestions and Actions

The United Nations has already taken several steps to address the challenges of autonomous weapons and cyber warfare. One of the main initiatives is the Group of Governmental Experts (GGE) on lethal autonomous weapons systems, set up under the Convention on Certain

Conventional Weapons. This group meets regularly to discuss how autonomous weapons fit into international law, focusing on ensuring that humans remain responsible for life or death decisions.

The UN has also hosted discussions on cybersecurity at the general assembly, encouraging countries to cooperate and reduce the risk of cyberattacks escalating into wider conflicts. In addition, UNODA works to promote transparency between states, sharing information and best practices to prevent misconduct in both autonomous and cyber technologies.

While there is not yet an official treaty banning autonomous weapons, the UN continues to support negotiations and dialogue aimed at creating international agreements, similar to how past treaties have limited chemical or nuclear weapons. Their actions show that the UN is actively trying to create frameworks for accountability, safety and cooperation in an increasingly technological world.

Possible Solutions

Ensure Meaningful Human Control: Require that humans always remain responsible for critical decisions, especially when lethal force is involved, so machines cannot act entirely on their own.

Develop Binding International Laws: Create a treaty or international agreement under the UN that sets clear rules for how autonomous weapons and cyber technologies may be developed, tested, and used.

Establish Oversight and Monitoring Bodies: Form an independent UN-led body to monitor compliance, investigate cyberattacks, and review the deployment of autonomous systems.

Introduce Bans: Encourage states to agree to a temporary pause (moratorium) on the use of lethal autonomous weapons until rules are finalized, or consider banning specific systems altogether.

Protect Civilians and Critical Infrastructure: Prohibit attacks on essential services such as hospitals, schools, power grids, or water supplies, ensuring that humanitarian principles are always upheld.

Promote Transparency: Encourage states to share information about their use and testing of autonomous systems and cyber capabilities to reduce mistrust and avoid escalation.

Implement Technical Safeguards: Require that autonomous systems include safety features such as "kill switches," fail-safes, or override mechanisms to prevent unintended harm.

Support Capacity-Building for All Countries: Provide training, resources, and technology-sharing so developing countries can strengthen their cyber defenses and participate equally in negotiations.

Encourage Public-Private Partnerships: Engage technology companies, universities, and civil society in discussions on ethics, research standards, and responsible innovation in artificial intelligence and cyber tools.

Guiding Questions

Here are some guiding questions you can use to jumpstart your research, and feel free to use the sources provided to you in the bibliography or citations listed below. These are resources to help you!

1. How should existing international law (like International Humanitarian Law and the Geneva Conventions) apply to autonomous weapons and cyber warfare?
2. Should the UN create a new treaty specifically regulating these technologies, or adapt existing ones?

3. To what extent should “meaningful human control” be required in the use of autonomous weapons?
4. How can the international community address the ethical concerns of allowing machines to make life-or-death decisions?
5. How can states be held accountable for cyberattacks when attribution is often difficult?
6. Should there be global agreements that prohibit cyberattacks on civilian infrastructure, such as hospitals, schools, or power grids?
7. What mechanisms could ensure transparency in the development and deployment of autonomous weapons?
8. Should the UN establish a monitoring or verification body to oversee compliance?
9. How can developing countries be supported in strengthening their cyber defenses and understanding new technologies?
10. What role should private companies, universities, and civil society play in shaping international guidelines?
11. Should certain uses of autonomous weapons or cyber tools be banned outright (similar to landmines or chemical weapons)?
12. How can guidelines remain flexible to keep up with rapidly advancing technologies in AI and cyber warfare?

Citations

“Biological Weapons | United Nations Office for Disarmament Affairs.” *Unoda.org*, 2025, disarmament.unoda.org/en/our-work/weapons-mass-destruction/biological-weapons. Accessed 30 Sept. 2025.

“Convention on Certain Conventional Weapons -Group of Governmental Experts on Lethal Autonomous Weapons Systems (2024) | United Nations.” *Unoda.org*, 2024,

meetings.unoda.org/ccw-/convention-on-certain-conventional-weapons-group-of-governmental-experts-on-lethal-autonomous-weapons-systems-2024?. Accessed 30 Sept. 2025.

Council of Europe. "Budapest Convention and Related Standards." *Council of Europe*, 2025, www.coe.int/en/web/cybercrime/the-budapest-convention. Accessed 30 Sept. 2025.

"Disarmament | United Nations Office for Disarmament Affairs." *Unoda.org*, 29 Aug. 2025, disarmament.unoda.org/en. Accessed 30 Sept. 2025.

"Emerging Challenges | United Nations Office for Disarmament Affairs." *Unoda.org*, 2025, disarmament.unoda.org/en/our-work/emerging-challenges? Accessed 30 Sept. 2025.

étrangères, Ministère de l'Europe et des Affaires. "11 Principles on Lethal Autonomous Weapons Systems (LAWS)." *France Diplomacy - Ministry for Europe and Foreign Affairs*, www.diplomatie.gouv.fr/en/french-foreign-policy/france-and-the-united-nations/multilateralism-a-principle-of-action-for-france/alliance-for-multilateralism/article/11-principles-on-lethal-autonomous-weapons-systems-laws. Accessed 30 Sept. 2025.

Holloway, Michael. "Stuxnet Worm Attack on Iranian Nuclear Facilities." *Stanford.edu*, 16 July 2015, large.stanford.edu/courses/2015/ph241/holloway1/. Accessed 30 Sept. 2025.

McGuinness, Damien. "How a Cyber Attack Transformed Estonia." *BBC News*, 27 Apr. 2017, www.bbc.com/news/39655415. Accessed 30 Sept. 2025.

NATO. "Kosovo Air Campaign (March-June 1999)." *NATO*, 21 Oct. 2024, www.nato.int/cps/en/natohq/topics_49602.htm. Accessed 30 Sept. 2025.

"Open-Ended Working Group on Information and Communication Technologies (2021) | United Nations." *Unoda.org*, 2021, meetings.unoda.org/open-ended-working-group-on-information-and-communication-technologies-2021?. Accessed 30 Sept. 2025.

Stop Killer Robots. “Stop Killer Robots.” *Stopkillerrobots.org*, 2018, www.stopkillerrobots.org/. Accessed 30 Sept. 2025.

“The Folly of Cyber War | Columbia | Journal of International Affairs.” *Columbia.edu*, 2022, jia.sipa.columbia.edu/content/folly-cyber-war. Accessed 30 Sept. 2025.

“United Nations Treaty Collection.” *Treaties.un.org*, treaties.un.org/pages/ViewDetails.aspx?chapter=26&clang=_en&mtdsg_no=XXVI-2&src=TREATY. Accessed 30 Sept. 2025.