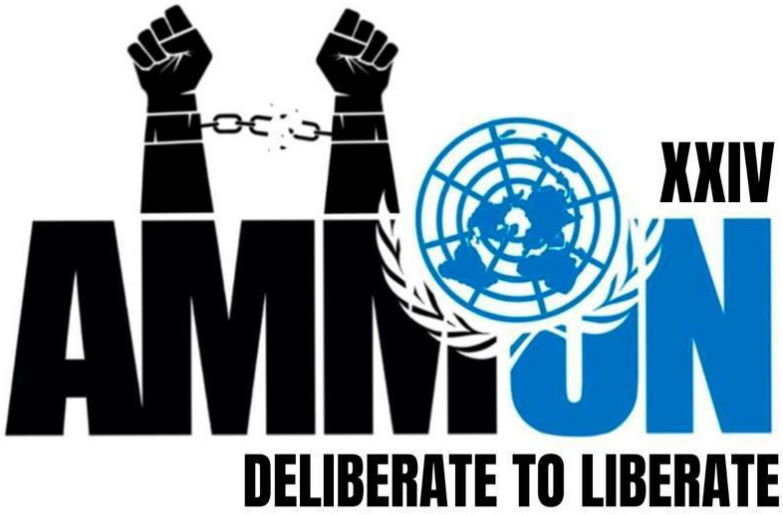

Forum: Disarmament Commission

Topic: Addressing the Risks of Cyber Warfare and Autonomous Weapons Systems

Haya Saket / Sebastian Nemeh / Jana Khalifa

Introduction

The proliferation of technological advancements along with the expansion of technology to incorporate artificial intelligence into all aspects of our lives, has generated a progression of modern-day threats to global peace and security. Due to the fact we live in a digital age where technology and artificial intelligence play a critical role in every aspect of our being, the threat they create to our safety are real. The biggest threats to contemporary peace and security are the challenges created by cyberwarfare and autonomous weapons systems (AWS) as structures of modern-day warfare. These threats to global peace and security rely heavily on the constant advances in technology as weapons and have altered how conflicts are experienced and handled worldwide.

In the past couple of years, we have seen how cyberattacks have grown into weapons of modern war. An example of this is the Stuxnet worm. It was allegedly used to disrupt Iran's infrastructure and cause physical damage to Iran's nuclear infrastructure. This was done without even stepping onto a battlefield. These attacks blur the already thin line between war and sabotage, making cyberattacks extremely dangerous.

The use of autonomous weapon systems (AWS) has grown rapidly over the past few years. This rapid growth in AWS has sparked a multitude of intense debates on whether AWS should be allowed in conflict, due to the ethical and legal implications they pose. Autonomous weapon systems are automated weapons that are able to identify a target, then proceed to strike it without any human input. In recent years, it has been clear that AWS is trusted more than it should be and that it lacks the human oversight which should be required. This has raised huge ethical and legal concerns among the international community. The unregulated and unchecked development and use of AWS and cyber weapons are a huge threat, not just to global stability, but also to global peace.

To date, the world has experienced multiple cyber-attacks that have had a huge impact on private and public systems. Autonomous weapon systems (AWS) have completely changed the traditional rules of war by demolishing the need for human intervention or input. By removing human decision making for lethal actions, these machines have become extremely risky to

operate. These risks demonstrate the need for international cooperation, legal clarity, and ethical standards.

To properly address these issues about this new era of technology, it is very important for all nations to properly communicate and prioritize monitoring, regulating and intervention. Global standards must be created and set to have clear guidelines for accountability. It is extremely crucial that the abuse of cyber capabilities is prevented and regulated, and that human oversight can be guaranteed to help keep global security and peace. This could prevent catastrophic humanitarian harm and global destabilization due to the fact that if this technology is not properly regulated, nations and states will abuse it.

Definition of Key Terms

Cyber Warfare

Cyber Warfare occurs when a state, organization, or non-state actor digitally attacks another entity by damaging, destroying, or controlling the entities infrastructure, data, or communication systems. These attacks commonly target military systems, power grids, and hospitals. Cyber Warfare involves the use digital operations to attack or disrupt a nations critical system. It is becoming more common in conflicts between nations and is extremely difficult to regulate.

Autonomous Weapons Systems (AWS)

Autonomous Weapons Systems (AWS) are weapons that can select and engage targets without any human input or intervention. AWS rely on artificial intelligence to operate, and they can be used in land, air, and ocean-based platforms. Due to the fact AWS don’t require human intervention, numerous ethical, legal, and humanitarian concerns have been raised by their application. AWS’s are relevant and significant to this topic as they lead to the development can challenge international laws, and their use can result in unintended harm without accountability.

Artificial Intelligence (AI)

Artificial Intelligence (AI) is a simulation of human intelligence via non-human technological apparatuses. Machines are trained and programmed to preform like humans and to match their behaviors and mindsets. Military AI refers the artificial intelligence being used in a state's army. Usually, AI in the military is used to identify threats and notify individuals to intervene. AI is the driving force behind the rise of modern military technology, making it essential and a central part of disarmament discussions

Cyber Attack

A Cyberattack is a digital attack by an entity or person that aims to intentionally damage, destroy, or steal data or software through a bug or unauthorized access to a system. Cyberattacks are relevant to this topic because they can cause disruption to military and civilian infrastructure at a large scale.

International Humanitarian Law (IHL)

The International Humanitarian Law (IHL) are the standardized rules and regulations designed to protect civilians and restrict certain practices in times of war. The IHL emphasizes principles such as distinction and proportionality. The IHL is relevant to this topic because AWS do not possess the human input needed to make ethical decisions during combat which could result in unlawful killings.

Group of Governmental Experts (GGE)

The Group of Governmental Experts (GGE) are a group created by the United Nations to study and provide specific recommendations on extremely specific topics and situations that are related to international security and disarmament.

Certain Conventional Weapons (CCW)

The Convention on Certain Conventional Weapons is a treaty that aims to ban or restrict the use

of weapons that are considered to cause unnecessary suffering in conflict.

General Overview

Modern warfare has changed dramatically during the 21st century. It has increasingly moved into the digital and automated sectors, making cyber warfare and autonomous weapons systems (AWS) some of the biggest threats to global peace and security. These technologies represent a new phase of conflict that challenges traditional understandings of warfare and disarmament. While this new technology offers huge tactical advantages for the nations using them, its lack of regulation poses significant risks to civilian lives and contributes to escalating international tensions. Another issue with AWS and cyber warfare is their anonymity — it is extremely difficult to trace the origins of attacks or the development of such technologies. The continued use of this new era of digital warfare calls for updated frameworks to regulate and govern the deployment of these technologies.

Cyber warfare can be tracked back to the 1980s and 1990s, when governments and militaries began to connect critical infrastructure to emerging technologies, creating new vulnerabilities. In 2007, Estonia experienced one of the first large-scale cyberattacks in the world, where its banking, media, and government websites were frozen by a Russian group — yet no entity was ever convicted. By 2023, over 6 billion malware attacks were recorded globally, showing the scale at which digital threats are evolving.

Following Estonia, digital attacks became more frequent and were given the name “cyberattacks.” In 2010, the Stuxnet virus targeted Iran’s nuclear facilities, marking the first time malware was used to physically damage infrastructure. The attack, believed to be developed by the United States, revealed the devastating potential of cyberattacks. Around the same time, autonomous weapons systems began to emerge. While drones had already been used in military operations, the development of machines capable of making lethal decisions without human intervention sparked growing concern. AWS began to be developed in the early 2000s, and as artificial intelligence advanced, countries began exploring systems that could automatically carry out lethal operations.

Despite warnings from experts and activists, little progress has been made toward international treaties regulating cyber warfare or AWS. Countries continue to develop and test these technologies in secrecy. As a result, both cyberattacks and autonomous weapons have become defining features of modern conflict, enabled by their ability to be deployed anonymously and remotely.

Subtopic 1:Legal Challenges of Autonomous Weapons Systems

Autonomous Weapons Systems (AWS) have created huge legal and ethical dilemmas under current international law, specifically the International Humanitarian Law (IHL). AWS operate without any human input or intervention and rely solely on artificial intelligence to identify and eliminate targets. This raises a multitude of serious concerns about their ability to comply with IHL, specifically with the principles of distinction and proportionality.

Since AWS do not require any human judgment, there is an extremely high risk of these weapons misidentifying a target and hurting innocents. Another issue with AWS is accountability. Accountability with AWS is extremely unclear. If an autonomous weapon makes a mistake and innocent lives are lost, it is hard to determine who is the person to blame.

Subtopic 2: Importance of Cyber Warfare Protection Infrastructure

National systems are very reliant on digital platforms and automated systems, which makes them extremely vulnerable to cyberattacks. Cyber warfare protection infrastructure is critical to keeping these systems safe and secure, ensuring that they are ready in times of crises.

A strong cybersecurity framework should include encrypted communication protocols, intrusion detection systems, secure data storage, and real-time monitoring of any threats that may appear. A lack of these protections allows state actors, terrorist organizations, or hackers to easily access and disrupt critical defense networks. Cyber threats are only growing in complexity and frequency, so it is extremely important that the infrastructure to fight these threats is available.

Subtopic 3: Recognizing the Potential Impacts of Cyber-Attacks on National Defense Systems

Cyberattacks targeting national defense systems can have catastrophic consequences. Military communication networks, satellite guidance systems, weapon control software, and digital intelligence databases are all potential targets for cyber sabotage. A successful attack could result in the interruption of military operations, exposure of classified data, or even unauthorized control over weapons systems. For example, disabling command-and-control systems during an armed conflict can leave a nation unable to respond to threats or coordinate strategic actions. Additionally, the theft of sensitive data gives adversaries detailed insights into a state's military assets and vulnerabilities, which could alter the balance of power. As modern warfare continues to digitize, defending against these threats is critical to preserving national sovereignty and international stability.

National dense systems include systems such as communication networks, satellite guidance systems, weapon control software, and digital intelligence databases, if these systems are targeted by a cyberattack the consequences could be catastrophic. One successful attack could mean an interruption in military operations or even control over weapon systems. As technology continues upgrade and modernize warfare continues to evolve and digitize, it is essential to defend against these threats to preserve national sovereignty and stability.

Major Parties Involved

The United States of America (USA)

One of the most advanced countries in deploying autonomous weapons systems (AWS) and cyber capabilities. The USA invests heavily into military artificial intelligence and has been involved in numerous cyber operations globally, defensively and offensively.

The Russian Federation

Has been accused of numerous cyber-attacks targeting infrastructure, elections, and defense systems.

Russia is one of the top developers in military artificial intelligence and is against autonomous weapons systems, favoring state-level control and strategic use.

The People's Republic of China

Has been rapidly growing its military artificial intelligence and cyber warfare operations. China has been linked to multiple cyber espionages against other states and is growing their autonomous systems as part of their military modernization, while resisting outside regulation of cyberspace.

The Democratic People's Republic of Korea

Has been heavily involved in state-sponsored cyber warfare. North Korea has conducted multiple major cyberattacks on foreign governments and companies. It uses cyber operations as a low-cost tool for conflict, disruption and to steal money. North Korea does lack development in autonomous weapons systems.

North Atlantic Treaty Organization (NATO)

A military alliance that has recognized the cyber space as a new category of warfare. NATO encourages cyber defense cooperation among members to defend against cyberwarfare and autonomous systems. NATO is currently assessing the ethical and legal risks of autonomous weapons on international peace and security.

Timeline of Events

Date	Event
2007/4/27	Estonia suffered the first massive attack that disrupted government systems and national banking systems.
2008/5/14	NATO opens its Cooperative Cyber Defense Centre of Excellence in Tallinn to strengthen allied cyber defenses.
2010/6/17	Stuxnet virus was uncovered. This virus targeted Iran's nuclear faculties and destroyed the facilities centrifuges by alternating their speeds. This was the first known malware used that caused physical damage.

2014/8/17	The U.S Air Force tested and deployed Perdix, a micro-drone swarm from F-16's over Alaska. This was the first public test of autonomous weaponized drone tech.
2015/12/23	Russian hackers shut down power to approximately 230,000 Ukrainian citizens. This was the first time a cyber-attack was able to successfully cause a blackout.
2017/4/26	U.S department of defense launched a project labeled "Project Maven" to integrate artificial intelligence into drones.
2022/2/24	Russia begins an invasion on Ukraine. Hackers launch numerous DDoS/Malware attacks on over 70 different Ukrainian government and bank websites in an attempt to destabilize the country further.
2025/4/30	Vienna hosts first conference that discusses AWS rules. The conference is called "Humanity at the Crossroads" and had 144 states pushing for legally binding AWS regulations.
2024/7/10	NATO launches its Defense Innovation Accelerator that funded 44 startups with €100k each to protect critical infrastructure.

Attempts to solve the issue

Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 14 July 2015 (A/70/174)

In 2015, a GGE report was created. This was the first ever official agreement among member states that UN law applies to everything in the Cyberspace. It highlighted specific standards that should have already been in place, such as avoiding damaging critical infrastructure. This report was very important in shaping the international cyber norms nations follow today. The issue with this agreement is how voluntary it is. The agreement did not have a way to enforce punishment on member states who violated the agreement. This meant states could completely disregard its recommendations without any consequences.

Developments in the Field of Information and Telecommunications in the Context of International Security, 8 December 2018 (A/RES/73/27)

To properly address the rising threats that were created by the misuse of information and communication technologies in internation security, the UN General Assembly adopted this resolution. This resolution pushed Member States to collaborate together and to build trust by encouraging transparent communication, the sharing of best practices, and the development of voluntary norms for responsible state behavior in cyberspace. The resolution emphasized confidence-building measures between different states to reduce the risk of misunderstandings or escalation in the event of cyber incidents. While this resolution helped member states open more discussions about cyber norms and promote multilateral cooperation, the resolution was missing a feasible way to enforce punishments when the resolution was violated. This limited how much the resolution could impact in limiting cyberwarfare or finding who was accountable.

Call to Ban Fully Autonomous Weapons, 23 October 2018 (CCW/GGE.1/2018/3)

During a 2018 session of the Convention on Certain Conventional Weapons, The GGE produced a report that strongly urged for international oversight of lethal AWS (LAWS). The report outlined the biggest concerns of LAWS, such as the need for human control and to follow international humanitarian law. This did not result in a legally binding ban due to military powers (USA, China Russia) voting against it. This helped raise global awareness and helped push out campaigns such as “Stop Killer Robots”. It helped carve in new norms about human responsibility on AWS.

Possible Solutions

Subtopic 1: Legal Challenges of Autonomous Weapons Systems

An effective possible solution is to establish an international treaty that clear states and

bans the use of fully lethal autonomous weapons. A complete ban on these lethal autonomous weapons would ensure that these autonomous machines will not cause any accidental conflicts or raise tensions. A clear definition of what "Autonomous" means would need to be required to reduce the risk of any potential loopholes being found. The treaty should also be specific and include detailed conditions for accountability, verification mechanisms and consistent reporting to prevent states from exploiting any loopholes that could be found. The treaty could be negotiated under the UN framework and based around the principles of the international humanitarian law, using principles such as distinction, proportionality, and precaution. These principles are extremely difficult for machines to learn and fully follow, which is why full autonomy in lethal decisions must be banned. States should also be encouraged to use a pre-approval process, where autonomous systems must be reviewed and approved by an separate international body before it can be used. This would create a lot more transparency between states and create a stronger global norm around acceptable military technology.

Another possible solution is to create an ethical and legal framework that requires all nations to implement new laws that ensures a human can be held accountable for any decision made by an AWS. This could include a licensing system for the engineers and developers that created it, human oversight being mandatory, and court liability standards when AWS does cause accidental or civilian harm. This will ensure that AWS can hold a human accountable incase the system does make an accident. Additionally, states could be required to publish transparency reports about how their autonomous systems are being used, who is responsible for them, and what oversight is in place. Being clear with who is responsibly is essential and would reduce the risk of abuse while improving trust between member states. These steps will help guarantee that even as technology advances, accountability and international law remain central to warfare.

Subtopic 2: Importance of Cyber Warfare Protection Infrastructure

A suitable solution would be to create an international cyber defense cooperation body that is supported by the UN. This body would help countries build up strong cybersecurity infrastructure for defense. This is especially useful for developing countries who lack resources for self-defense, and it will promote more political stability in their regions. This body could

also include cyber security toolkits, and training workshops for members in the government that work in the security sector to ensure that they are well educated on cyber warfare defense systems and their use. This will also help nations conduct national risk assessments and ensure there are not any vulnerabilities that hackers could exploit within their infrastructure. Overall, this solution ensures that all member states are better prepared for any cyberattack and can respond accordingly.

Another solution would be for member states to create a mandatory minimum cybersecurity standard for critical infrastructure, which, if it goes down, could cause the country to suffer significantly. This includes important infrastructure such as energy grids, military defense systems, and communication networks. These systems are extremely important for a country's stability and security. A major cyberattack on these systems could severely disrupt a country's stability and important services, such as first responders, which, in turn, would make the nation extremely vulnerable. These minimum cybersecurity standards could be created by a UN task force that sets and creates these standards while overlooking them to make sure all member states comply and are fair. The task force could also offer technical support and provide recurring system audits. Additionally, this task force could create a general global response framework, along with global cybersecurity drills and simulations that would help prepare countries for threats and test the nation's strength.

Subtopic 3: Recognizing the Potential Impacts of Cyber-Attacks on National Defense Systems

A possible solution would be to develop a system that detects and warns nations about cyber threats that target critical systems, a system similar to an early missile detection system. Through AI global monitoring and intelligence sharing between trusted states this system could alert countries of any suspicious activities that target their nations critical systems. While an international system may be unfeasible and even unsafe in the worlds current geopolitical state due to trust and sovereignty concerns, regional implementation among trusted partners could

serve as a viable framework to begin with. By implementing machine learning and behavioral analytics this system could be able to detect unusual activity and identify potential threats. This helps give nations a chance to fight cyberattacks more efficiently and maintain stability.

Another solution is to strengthen international norms and standards around cyber non-aggression. This could be done by expanding the 2015 GGE voluntary norms into legally binding commitments between nations, where states make a pledge to not target another state's critical infrastructure unless in wartime and under strict legal review. To help in building trust and promoting enforcement, regional workshops and capacity-building programs could be hosted around the globe and remotely to help train cyber officials, promote transparency, and encourage cooperation. By slowly building trust and promoting transparency, these efforts will prevent any cyberattack from escalating into threats against critical infrastructure, further promoting long-term international stability.

Guiding Questions

1. What are the main dangers that cyber warfare brings to national defense systems and global security?
2. How have recent major cyberattacks affected how nations view cyber threats?
3. What new development in technology have helped create autonomous weapons systems (AWS), and how are they used today?
4. What legal and ethical problems do autonomous weapons systems (AWS) create under international law?
5. Why is it so difficult for autonomous weapons to follow rules like identifying civilians and taking responsibility for mistakes?
6. How have countries used cyber warfare in past conflicts to gain advantages or defend themselves?
7. What do the P5 countries think about banning or regulating autonomous weapons?
8. What actions has the United Nations taken to control cyber warfare and autonomous weapons through discussions or resolutions?
9. How do non-government groups (like hackers or terrorist groups) use cyber weapons, and why is this dangerous?

10. What does “meaningful human control” mean, and why is it important in the use of AI weapons?
11. Why is it hard to figure out who caused a cyberattack, and how can that lead to bigger conflicts?
12. How is the UN’s Convention on Certain Conventional Weapons (CCW) trying to deal with the risks of AWS?
13. What are the biggest challenges to creating a global treaty on cyber warfare or autonomous weapons?

Appendix

- https://www.defense.gov/Spotlights/Artificial-Intelligence/
- https://www.ai.mil/about/organization/
- https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/russia
- https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-141a
- https://www.ft.com/content/63720831-8805-497d-8145-1713e450a55a
- https://www.nato.int/cps/en/natohq/topics_78170.htm
- https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-cyber-defence-en.pdf
- https://www.un.org/disarmament/the-convention-on-certain-conventional-weapons/
- https://www.icrc.org/en/document/icrc-position-autonomous-weapons

Bibliography

Arms Control Association. “Geopolitics and Regulation of Autonomous Weapons Systems.” *Arms Control Today*, Jan. 2025, https://www.armscontrol.org/act/2025-01/features/geopolitics-and-regulation-autonomous-weapons-systems

Artificial Intelligence and Law: International and Regional Regulation. *Library of Congress*, 3 May 2024, https://www.loc.gov/law/help/artificial-intelligence/international.php

“Autonomous Weapons Systems: Current International Discussions.” *Ethik und Militär*, 2024, https://www.ethikundmilitaer.de/en/2024/1-ai-and-autonomy-in-weapons-war-and-conflict-out-of-control/autonomous-weapons-systems-current-international-discussions

ComputerWeekly. “Global Majority United on Multilateral Regulation of AI Weapons.” *ComputerWeekly*, 15 May 2024, https://www.computerweekly.com/news/366582577/Global-majority-united-on-multilateral-regulation-of-AI-weapons

Developments in the Field of Information and Telecommunications in the Context of International Security: Report of the Secretary-General. A/70/174, *United Nations General Assembly*, 22 July 2015, https://docs.un.org/en/A/70/174

House of Lords. *AI in Weapon Systems: Select Committee on Artificial Intelligence in Weapon Systems. UK Parliament*, 22 Feb. 2024, https://publications.parliament.uk/pa/ld5804/ldselect/ldaiwe/16/1608.htm

Just Security. “Scientists Call for Ban on Autonomous Weapons Systems.” *Just Security*, 27 Oct. 2015, https://www.justsecurity.org/2097/scientists-ban-autonomous-weapons-systems/

Reuters. “UN ‘Killer Robot’ Talks Drag as Regulation Lags.” *Reuters*, 12 May 2025, https://www.reuters.com/sustainability/society-equity/nations-meet-un-killer-robot-talks-regulation-lags-2025-05-12/

Resolution Adopted by the General Assembly on 5 December 2018: Developments in the Field of Information and Telecommunications in the Context of International Security. A/RES/73/27, *United Nations General Assembly*, https://digitallibrary.un.org/record/1655670/files/A_RES_73_27-EN.pdf

“Solutions.” *Campaign to Stop Killer Robots*, Future of Life Institute, https://autonomousweapons.org/solutions/

Towards a Roadmap for International Regulation of Autonomous Weapons Systems. *UNIDIR*, 2018, https://documents.un.org/doc/undoc/gen/g18/323/29/pdf/g1832329.pdf

Contact Information

President: Haya Saket

Email: haya_saket@abs.edu.jo

Phone: +962 7 7956 2200

Chair: Sebastian Nemeh

Email: sebastian_nemeh@abs.edu.jo

Phone: +962 7 9806 9000

Chair: Jana Khalifa

Email: jana_khalifa@abs.edu.jo

Phone: +962 7 9151 8888