S'MUN2030

SINGULARITY MODEL UNITED NATIONS

DISEC

Regulating the use of AI in warfare

SMUN2030

DISEC

SINGULARITY FOUNDATION

St PETER'S SCHOOL
Barcelona

0. Table of contents

1. Introduction

Face recognition, voice assistants, interactive filters for social media, house management systems… artificial intelligence (AI) has become a constant in our daily lives, playing a crucial role in most technological advances and shaping how we conceive some of our most daily routines. Its uses, however, go beyond what we see, and AI is currently applied in fields such as healthcare, industry, retail or politics.

One of the most unknown yet polemic fields in which artificial intelligence is applied is in the military: the development of AI has had a decisive influence on the way modern warfare is conceived, and this new paradigm opens the door to a new nature of armed conflicts with possible consequences never seen before (deep violations of human rights, unforeseen actions, derived from the misuse of these technologies, massive deaths, negative effects on the environment and societies…).

Artificial intelligence (AI) generally refers to the ability of a digital computer or computer-controlled robot to perform tasks commonly associated with intelligent beings, such as reasoning, generalizing, learning from precedents or associating concepts with a determinate action. As mentioned before, AI has been deployed in many different fields that directly and indirectly affect our daily lives, with the military being one of them.

The use of artificial intelligence for warfare purposes has led to the creation of lethal autonomous weapons systems (LAWS), which are defined by the Red Cross as “any weapons that select and apply force to targets without human intervention”. These weapons, also known as “killer robots”, are designed to chase certain profiles targeted beforehand, and as soon as the weapon is deployed on the battlefield and identifies the mentioned profile (through AI), it proceeds to attack.

The use of LAWS has changed the way modern warfare is conceived, mainly due to the appearance of modern weapons with new functionalities by-product of AI, but also because of the emergence of a whole new bunch of fields in which this technology can be used (civil

surveillance, training, capacity-building, crisis prevention and anticipation…). As a result, we are advancing towards a new and more sophisticated war scenario in which engines and authomatized weapons (instead of humans) will be the main fighters, and where new tactics and strategies will be implemented. Nonetheless, it is important to mention that the uses of AI for military purposes go beyond these weapons, as nowadays it is used in many other situations, among which we find cyberwarfare, predictive analysis, data gathering, training or battlefield simulations.

Nowadays, the use of AI for military-related purposes is still not regulated at a global level, mainly due to the complexity of finding common ground among the wide variety of positions global powers hold regarding how these regulations should look like. This has raised many issues in relation to aspects such as defining who should be ultimately responsible for the actions committed by LAWS, the role of humans in the control of these weapons, how to ensure the protection of basic human rights and other ethical dilemmas.

Bearing in mind previous precedents such as nuclear weapons or weapons of mass destruction, the international community is expected to focus its efforts on creating a legal framework that regulates the use of LAWS and AI in military activities, that is able to solve all the issues mentioned before and that can protect the world from undesired consequences derived from the poor handling of this powerful yet dangerous technology.

2. Current situation

The use of AI in warfare is a rapidly developing field with numerous ongoing projects and applications. To simplify all the uses that artificial intelligence can provide to warfare, we have classified five main categories:

- ***Autonomous weapons***

Several countries are developing autonomous weapons that can select and engage targets without human intervention. However, there is an ongoing debate about the ethics and risks of using such weapons. The use of autonomous weapons in warfare is a controversial topic, with arguments for and against their deployment.

Proponents of autonomous weapons argue that they can reduce the risk to human soldiers, increase the speed and accuracy of military operations, and provide a deterrent to enemy forces. They also argue that autonomous weapons could potentially reduce the overall number of casualties in a conflict by avoiding collateral damage and minimizing the risk of friendly fire incidents. Opponents of autonomous weapons argue that their deployment could lead to unintended consequences, such as the loss of civilian lives and property damage, and the

potential for such weapons to be hacked or malfunction. There are also concerns about the legal and ethical implications of using weapons that operate without human intervention and are capable of making life-and-death decisions.

Currently, there is no international agreement on the use of autonomous weapons, and various countries are at different stages of development in this area. Some countries have called for a ban on autonomous weapons, while others are investing heavily in their development. The United Nations is also discussing the issue of autonomous weapons, intending to establish a global framework to govern their use.

- ***Cyberwarfare***

Cyberwarfare refers to the use of digital technology to attack and defend against other nations or groups. Cyberattacks and defences are key aspects of modern warfare, and AI is increasingly being used to detect and respond to cyber threats. The current situation of cyberwarfare is characterized by increasingly sophisticated attacks by state-sponsored hackers, criminal groups, and other non-state actors. Some of the key trends and developments in cyberwarfare today include nation-state attacks, ransomware attacks, cyber espionage, and, obviously the increasing use of AI.

Several countries have been implicated in cyberattacks against other countries, including attacks on critical infrastructure such as power grids, water systems, and transportation networks. Moreover, criminal groups have increasingly been using ransomware attacks to extort money from companies and organizations, causing significant disruption and financial losses. Apart from this, many countries are using cyber espionage to gather intelligence on other countries, including their military capabilities and strategic plans.

Governments and international organizations are responding to the growing threat of cyberwarfare by investing in cybersecurity measures and developing new policies and regulations to address the issue. However, the constantly evolving nature of technology and the increasing sophistication of cyberattacks means that the threat of cyberwarfare is likely to continue to grow and evolve in the years ahead.

- ***Drone warfare***

Drones are unmanned aerial vehicles that can be remotely controlled or can operate autonomously. They are being used for a variety of military applications, including surveillance, reconnaissance, and targeted strikes. AI is being used to enhance the capabilities of drones, such as enabling them to fly autonomously and navigate through complex environments. They have become an increasingly important tool in modern warfare, providing military organizations with

a range of capabilities that were previously unavailable, such as targeting strikes, logistic support, electronic warfare, swarm tactics, etc.

One of the main abilities that they have is what is called ISR (Intelligence, Surveillance, and Reconnaissance). Drones can nowadays be equipped with a range of sensors and cameras to gather intelligence on enemy movements and activities. This information can be used to plan military operations and target strikes. Moreover, they can be armed with missiles or other weapons and used to conduct targeted strikes against enemy targets, including individuals and vehicles. Drones can be used to transport supplies and equipment to troops on the ground, reducing the risk to human transport crews. Furthermore, they have the possibility to be equipped with electronic warfare equipment to disrupt enemy communications and other electronic systems. Apart from this, military organizations are exploring the use of swarms of drones to overwhelm enemy defences and conduct coordinated attacks.

All in all, the use of drones in warfare has raised ethical and legal concerns, particularly when it comes to targeted strikes and the potential for civilian casualties. There is an ongoing debate about the appropriate use of drones and the extent to which they should be allowed to operate autonomously. Nonetheless, drones are likely to continue to be a key tool in modern warfare, providing military organizations with new and powerful capabilities.

- ***Predictive analytics***

Predictive analytics involves using machine learning and statistical techniques to analyze large volumes of data and identify patterns and trends that can be used to predict future events. In the context of warfare, predictive analytics is being used to analyze data from a variety of sources to gain insights into enemy capabilities and intentions and to make better-informed decisions about military operations.

Predictive analytics can be used, for example, to analyze social media, online forums, and other sources of data to identify potential threats, such as terrorist groups or enemy combatants. This information can be used to help plan military operations and to prevent or disrupt enemy activities. In addition, it can be used to analyze data on weather patterns, supply chain disruptions, and other factors that could impact military logistics. This information can be used to help plan for contingencies and to ensure that troops have the supplies they need.

The use of these predictions is able to analyze data on enemy troop movements, weapons systems, and other factors to determine where to allocate military resources. This can include deciding where to deploy troops and equipment, as well as making decisions about the use of weapons systems. Moreover, it can register and interpret data from sensors and other sources to detect potential threats, such as incoming missiles or enemy troop movements. This information

can be used to trigger early warning systems and alert troops to potential dangers. Finally, by considering the predictions, it is possible to simulate different military scenarios, allowing military planners to test different strategies and assess their likely outcomes.

Overall, predictive analytics is providing military organizations with new and powerful tools for decision-making and planning. However, the use of predictive analytics in warfare also raises concerns about privacy, ethics, and the potential for unintended consequences.

- ***Training and simulation***

As briefly mentioned before, AI simulations for warfare involve the use of artificial intelligence to create realistic and complex simulations of military scenarios. These simulations can help military organizations train soldiers, test new strategies and tactics, and evaluate the effectiveness of existing systems and equipment.

AI simulations can be used to train soldiers in a wide range of scenarios, from basic combat training to complex operations involving multiple units and equipment. By creating realistic simulations of combat scenarios, soldiers can be better prepared for real-world situations. At the same time, they can serve to test new weapons systems and equipment, allowing military organizations to evaluate their effectiveness and identify potential weaknesses or limitations.

Moreover, they can be used to model and simulate different military scenarios, allowing military planners to test different strategies and assess their likely outcomes. This can include planning for specific missions, as well as evaluating the potential impact of broader geopolitical events. Apart from this, when having large volumes of data, AI is able to identify patterns and trends that can be used to predict future events and to inform military decision-making and planning.

In a nutshell, AI simulations are providing military organizations with new and powerful tools for decision-making, planning, and training. However, the use of AI simulations in warfare also raises concerns about privacy, ethics, and the potential for unintended consequences.

Overall, the use of AI in warfare is still in its early stages, and the ethical, legal, and strategic implications of its use are still being debated. However, AI is already having a significant impact on the way wars are fought and the capabilities of military organizations. It is in all nation’s hands to tackle all the issues that arise from its use, as it is currently starting to be implemented in some conflicts.

3. What to tackle

As seen in current battlefields such as Ukraine (where Russia is using Iranian-made kamikaze drones against the Ukrainian army) or Syria (which has become a laboratory for may global

powers to try its newest technological advances, and where military AI technologies have substantially increased the risk for mass atrocities), but also in other contexts aside from war (such as in Estonia, where in 2007 the national parliament and several banks, ministries, newspapers and other public institutions suffered a huge wave of cyberattacks that threatened the security and functioning of the whole country) the use of Artificial Intelligence for modern warfare purposes is quickly evolving, and its presence is growing due to an overall reduction of costs and easier access to these technological advances. In this sense, this growth is not expected to stop, as AI is set to acquire major relevance in future military applications.

As mentioned before, the use of AI in warfare is currently characterized by the lack of international legally-binding instruments that are able to ensure a rational and human-based use of these technologies. Therefore, efforts should be directed towards designing a common and global legal framework for the development, production and use of this technology for military and warfare purposes. Ultimately, negotiations should lead to the creation of a new convention or protocol specific to AI that can resemble others such as the Convention against Anti-personnel Mines or the Convention on Cluster Munitions.

One of the main points this regulation must tackle is the role and responsibility of humans. Many countries and experts agree that the application of AI for military or warfare purposes should always be supervised and ultimately controlled by humans in order to prevent potential mistakes and avoid unwanted actions. Those in favour of this approach also believe any kind of technology implementation lacking human control should be banned.

Regarding this matter, in 2021 the European Parliament adopted a report on “Guidelines for military and non-military use of Artificial Intelligence”, which established that the “decision to select a target and take lethal action using an autonomous weapon system must always be made by a human exercising meaningful control and judgement, in line with the principles of proportionality and necessity”. The report also stated that “AI-enabled systems must allow humans to exert meaningful control”, in order to promote accountability and facilitate the assumption of responsibility.

Another important aspect to tackle could be defining who would be liable or responsible for the consequences of actions carried out by AI or autonomous weapons. The production chain of these engines is usually long, and it involves many professionals: from developers to producers and operators. All of them contribute in some way or form to the creation of the product, but there is a need for legislation on who would ultimately be held accountable. As of now there is no consensus at an international scale on who should this responsibility rely on, and different stances emerge: some think it should go to the ultimate operators (mainly the State, since most of this technology is State-owned) due to the fact that they decide what uses to give to this

technology and how to deploy it; others think it should fall on the developers of the technology, arguing that they are the main responsible for how this technology is conceived; and some argue that it should rest with the producers of the weapons themselves, since they are the ones who implement AI in these objects.

The fast development of AI and its use as a tool for mass surveillance or predictive analytics for military purposes also poses substantial threats related to the respect for basic human rights, human dignity and respect for privacy in bellic contexts. In this sense, many voices agree with the fact that any new regulation attempts should also take into account the hypothetical affectations of the use of this technology on human rights. The European Union has been the main promoter of this human rights-based approach, suggesting measures such as banning public authorities from using AI for "highly intrusive social scoring applications" and paying special attention to the misuse of this technology for non-conventional and hybrid warfare methods such as the destabilization of societies, the spread of fake news, the manipulation of public opinion or the malicious influence of the outcomes in electoral processes.

On another note, according to Qiang Li and Dan Xie, professors at the Military Law Institute of the China University of Political Science and Law (CUPL), any legal regulation of military operations involving AI should comply at all times with the main principles of International Humanitarian Law (IHL) and, especially, with the First Additional Protocol to the Geneva Conventions. Both experts stress that the creation of this framework should take into account four main points: whether the new weapons are already regulated or explicitly forbidden by other conventions or protocols, if such weapons may cause environmental harm if there is a possibility that these weapons have the effects of indiscriminate attacks, and if they will comply with the principles of humanity and the dictates of public conscience.

All the debates introduced until now remark on the important moral and ethical dimension of the regulation of the issue on hand; especially when it refers to Lethal Autonomous Weapons Systems (LAWS). Artificial Intelligence cannot be equated with human intelligence, as it lacks a moral component as well as the capability to make decisions based on the context or taking into account social, cultural or political factors. In this situation, weapons based on AI are objectively programmed to reduce human beings to simple points or targets that need to be eliminated, leaving aside the particularities of battlefields, which tend to be highly volatile and unpredictable. With that being said, one question arises: in a context like this, should the decision to kill be given to machines operating under artificial intelligence? This debate has a high moral load, and as such it might be difficult to translate into legal debates, but at the same time, it is key at the time of conceiving what a regulation on the field should look like.

In conclusion, the current lack of binding and global legislation to regulate the use of AI in warfare

issues poses a great threat to international security. In this context, the international community will have to agree on a common legal framework that establishes the uses of this technology, its main responsibilities and the conditions under which its deployment will be legal and legitimate. To achieve so, past negotiations on similar topics (such as nuclear weapons, weapons of mass destruction, and biological weapons…) can be used as a starting point to build this legislation. Nonetheless, the divergence of positions over how a global regulation should look like, the wide variety of interests regarding the weaponization of AI and the lack of mutual trust among global powers such as the United States, China or the Russian Federation will hinder further progress on the matter.

In order to bring positions closer and help create the optimal conditions for a hypothetical agreement, there need to be more spaces in which both State and non-State actors can come together to debate, share points of view and exchange information and practices. There have already been several efforts in this direction, including the one made by the United Nations Office for Disarmament Affairs, which in 2019 collaborated with the Stanley Center and the Stimson in the organisation of a workshop and the drafting of several papers about the peace and security implications of the use of AI that brought together many actors involved in some way or form in the field of AI and warfare. Despite the existence of precedents, the lack of progress evinces their inefficiency and the need for different approaches and better practices.

Some voices go beyond simple regulation, and directly stand up for a complete ban of these technologies for military and warfare purposes. However, reaching this scenario is much more difficult, since the increasing availability and accessibility of AI for new actors and the interests of many global powers in weaponizing this technology make it almost impossible to work on a complete ban on a global scale.

Concurrently with international legislation, regulative frameworks at the national level are also needed. Such structures should enable States to develop their own standards and requirements, taking into account the global dimension of the issue on hand. In this sense, governments should focus on aspects such as transparency, and adapt legislation to their own contexts.

4. Questions a resolution must answer (QARMA)

- Should the international community aim for a global framework that establishes a common and binding regulation for the use of AI for military purposes, or would it be more suitable to leave it up to each country's choice?
- Should there be any limits regarding the use of AI in warfare? If so, which ones?
- Who should be ultimately responsible for the actions committed by LAWS? Developers, producers, operators…?

- Which should be the ethical or moral approach regarding LAWS or other kinds of AI-based military-related technologies? Should this component be taken into account while legislating?
- How can AI be deployed for military uses (such as predictive analysis or civil surveillance) without negatively affecting fundamental human rights? Should it be a priority?
- Given the wide variety of positions on the topic to be tackled, which strategies could be used to find common ground among actors?
- Which mechanisms could be enabled to ensure hypothetical common legislation is respected and followed by all states that stick to it?

5. Vocabulary

- **Artificial intelligence (AI):** the ability of a digital computer or computer-controlled robot to perform tasks commonly associated with intelligent beings, such as reasoning, generalizing, learning from precedents or associating concepts with a determinate action.
- **Autonomous weapons**: Weapons that can select and engage targets without human intervention.
- **Cyberwarfare**: The use of digital technology to attack and defend against other nations or groups.
- **Drone warfare**: The use of unmanned aerial vehicles to conduct military operations.
- **Lethal autonomous weapons systems (LAWS)**: any weapons that select and apply force to targets without human intervention.
- **Machine learning**: A subset of artificial intelligence that allows machines to learn from data and improve their performance over time.
- **Mass surveillance**: delivered monitoring of an entire huge group of people or a part of it, carried out it order to obtain information about its behaviour, composition and others.
- **Neural networks**: A type of machine learning algorithm that is modelled after the structure of the human brain.
- **Robotics**: The design, construction, and operation of robots for various purposes, including military applications.
- **Targeting**: The process of identifying and selecting specific targets for attack.
- **Unmanned ground vehicles (UGVs)**: Vehicles that operate on the ground without a human operator.
- **Weaponized AI**: The use of artificial intelligence in military applications, including the development of autonomous weapons.
- **Algorithmic warfare**: The use of algorithms and data analysis to make military decisions and carry out operations.
- **Ransomware attacks**: a type of malicious cyberattack in which an attacker infiltrates a

computer system or network and encrypts files, making them inaccessible to legitimate users.

6. Sources

AI in War: How Artificial Intelligence is Changing the Battlefield. The Decoder. (2022, March 1). https://the-decoder.com/ai-in-war-how-artificial-intelligence-is-changing-the-battlefield/

AI Is Rapidly Transforming Warfare. New Rules Are Urgently Needed. Centre for International Governance Innovation. (2022, February 16). https://www.cigionline.org/articles/ai-is-rapidly-transforming-warfare-new-rules-are-urgently-needed/

Araya, D. (2022). *AI Is Rapidly Transforming Warfare: New Rules Are Urgently Needed*. Centre for International Governance Innovation. Retrieved from: https://bit.ly/3EoKNT1

European Parliament (2021). *Guidelines for military and non-military use of Artificial Intelligence* [Press release]. Retrieved from: https://bit.ly/3xGMnvM

Lethal AWS (s.f.). *What are lethal autonomous weapons?*. Retrieved from: https://bit.ly/2JJ0qdQ

Li, Q., Xie, D. (2019). *Legal regulation of AI weapons under international humanitarian law: A Chinese perspective*. Humanitarian Law & Policy. Retrieved from: https://bit.ly/3lPGA4p

Marijan, B. (2022). *AI-Influenced Weapons Need Better Regulation*. Scientific American. Retrieved from: https://bit.ly/3YQleCL

Maxwell, P. (2020). *Artificial intelligence is the future of warfare (just not in the way you think)*. Modern War Institute. Retrieved from: https://bit.ly/3KnDVJE

United Nations Office for Disarmament Affairs (2020). *The Militarization of Artificial Intelligence*. Retrieved from: https://bit.ly/41g36Uo