

Topic: The Weaponization of Artificial Intelligence

Many people think of artificial intelligence as fully sentient robots in human form, a concept which they believe to be purely science fiction. However, artificial intelligence, or AI, represents so much more than what has classically been seen on the silver screen. Broadly defined, AI refers to “the ability of a digital computer or computer-controlled robot to perform tasks commonly associated with intelligent beings.”¹ Though this may seem like quite a futuristic topic, some argue that the origins of AI can be traced back to the 1950s with famed British mathematician Alan Turing.² The ideas and concepts innovated by Turing with his Turing Machine, and in his paper “Computing Machinery and Intelligence,” still underlie many modern artificial intelligence technologies and the programs used to test their intelligence.³

While the reality of anthropomorphic robots may still remain in the distant future, many of us do not even realize the extent to which we interact with AI in our daily lives. Programs such as Apple’s Siri, or Amazon’s Alexa are prime examples of what is referred to as narrow AI, or AI with intelligence that is limited to a single task or domain of knowledge.⁴ Alexa and Siri have undoubtedly become indispensable parts of many people’s daily lives, and the risks associated with the development of artificial intelligence generally do not involve these helpful robotic assistants who reside in our devices. Rather, the issue lies in how developing AI technology is being used by militaries around the globe.

The weaponization of AI is one of the biggest threats facing the international community. Weaponized AI technologies do not face the same barriers as human soldiers, allowing them to traverse all kinds of terrain and be utilized in all areas of typical warfare. Additionally, as artificial intelligence becomes more sophisticated, its ability to engage in atypical warfare, such as that in space and cyberspace, continuously increases.

Perhaps the most well-known AI system employed by the military, the lethal autonomous weapons system (LAWS) creates complex security issues for nations across the globe. LAWS is a military system which can search, aim, and attack automatically, according to its programmed instructions.⁵ LAWS do not need human operation and at this point have been integrated into

¹ <https://www.britannica.com/technology/artificial-intelligence>

² <http://sitn.hms.harvard.edu/flash/2017/history-artificial-intelligence/>

³ Ibid

⁴ <https://undir.org/publication/weaponization-increasingly-autonomous-technologies-artificial-intelligence>

⁵ <https://www.lawfareblog.com/lethal-autonomous-weaponssystems-recent-developments>.

nearly all areas of warfare. The United States Armed Forces utilizes LAWS in both unmanned vehicles and weapons, as well as for silent cyber-attacks.⁶

Though the international community is not one to shy away from technological development, the risks associated with the weaponization of AI must be acknowledged. The proliferation of artificially intelligent weapons brings with it the prospects of arms races, security dilemmas, and the grim possibility that non-state actors may acquire such weapons.⁷ Additionally, the current technology being used by the majority of the world's militaries is vulnerable to the risk of hackers hacking into these weapons' programming, enabling them to change the intended function of the lethal systems.⁸ As such, the issue of the weaponization of artificial intelligence must be confronted, and it is the responsibility of DISEC to find an innovative solution to combat this threat.

The weaponization of AI is still a relatively new issue, and therefore there has not been much previous action taken by the United Nations on the topic. While delegates are encouraged to research previous resolutions and programs which have been adopted relating to this issue, they are urged to be creative in their thinking and to prepare concrete and actionable plans to confront the weaponization of AI.

Some questions delegates may wish to consider include:

- How can a balance be struck which allows the positives of AI to continue to be enjoyed by civilians, while still combating the threat of this technology being weaponized?
- If an error occurs while a LAWS is in use, who should be responsible for it?
- How can hackers and/or terrorists be prevented from interfering with the functioning of weaponized AI systems?
- Should a set of guidelines, such as those found in the Geneva Convention, be set in place to govern the use of AI weapons? Would doing so help in preventing (or, at this point, slowing) an AI arms race?

Please keep in mind that you are representing your country's views, not your own. In addition, all papers will be submitted through Turnitin, so do not plagiarize!

⁶ <https://doi.org/10.23919/cycon.2019.8756866>.

⁷ Ibid

⁸ Ibid

If you have any questions, please feel free to email me at adauerba@mail.yu.edu. I am looking forward to reading your work.

Best of luck,
Adam Auerbach
Chair, Disarmament and International Security Committee
YUNMUN XXXII