BRIEFING NOTES

BN-55-The role of AI-May2021

DUAL USE ASPECTS OF ARTIFICIAL INTELLIGENCE (AI) AND AUTONOMOUS SYSTEMS

Authors: Bita Afshar[1] and Kash Khorasani[2]
1 Graduate student, Department of Electrical and Computer Engineering, Concordia University, Montreal, Canada
2 Professor, Department of Electrical and Computer Engineering, Concordia University, Montreal, Canada

SUMMARY

- Artificial Intelligence (AI) is one of the most important technologies that are being extensively investigated and developed. There are controversial discussion and opinions regarding possible benefits and drawbacks of artificial intelligence based on its dual-use nature.
- A growing presence of autonomous systems and robots as assets (drones) in warfare has caused many risks and concerns for human lives where concrete legal and ethical issues and concerns have been raised. The human control and authority over autonomous military assets should be further discussed as part of developing appropriate public and military policy frameworks.
- Autonomous robots and vehicles can bring about a number of advantages such as assisting disabled people, and for war robots performing different types of duties such as target attacks, inspect hideouts, defuse bombs and many other tasks.
- Four main concepts are required to be considered in using war robots and autonomous vehicles (drones), namely (1) decision of firing, (2) discrimination, (3) responsibility, and (4) proportionality.
- Autonomous weapons and drones that are operating by utilizing machine learning and AI software and technologies need careful assessment based on the AI's capabilities.
- The development of kinetic robotics and autonomous systems need a comprehensive supervisory and monitoring plan. One of the main concerns of AI technology is related to accountability, given the possible and potential risks that are conceivable and may harm people when a wrong decision is made by an AI system autonomously.
- The dual-use concept needs security measures given that many designers may not be fully aware of all the possible risks of dual-use technologies. Many commercial enterprises are not deeply involved in and concerned with these important issues given that they are mostly focused on intense competitions from other competitors.
- The misused application of AI by non-state actors would result in national security risks and financial losses. By specifying clear limitations on the military exploitation of AI, certain threats could be avoided however the question that still remains is what should be the best approach against exploitation of AI and autonomous systems by terrorists and malicious adversaries. For the above reason, technical and scientific remedies should be highlighted to avoid the misuse of AI and autonomous systems development.

CONTEXT

- The world around us is surrounded by fully autonomous systems and Artificial Intelligence systems (AI). The dual nature of AI technology requires more attention due to the adverse utilization of designed tools in targets such as weapons besides other beneficial civilian purposes [1-3].

- The fast-evolving AI technologies and applications will lead to several dual-use applications that may put the security of individuals, governments, businesses, and academia in danger [1-3].
- A specific algorithm can be used for commercial applications while it has also a crucial role in weapon systems. For instance, autonomous weapons systems, facial recognition technologies, decision-making algorithms could be employed for military purposes [1-3].
- Autonomous weapons that are powered by machine learning and AI need careful assessments based on AI's capabilities. Image processing, data collection and processing, and fire control systems are the main tasks and responsibilities of AI and machine learning in autonomous weapons [4-5].
- The basic AI applications are coded by humans that are rule-based methodologies. These kinds of programming need problem statements and the exact accuracy of the software results. This approach is suitable for tasks with well-defined variables and a small number of unknown variables. This programming methodology is established on the human's ability of understanding the environmental features and modeling the problem which in most cases are limited and simplified [4-5].
- On the other hand, machine learning can assist in case of high dimensionality and complexity of the problem by using deep learning concepts as well as methodologies. To overcome those limitations, a machine can be taught on how to deal with novel situations instead of being programmed to act in a pre-determined manner. Deep learning as one of the most advanced techniques and methods in machine learning could be considered as one of the most dominant and fundamental advances on the future of warfare [4-5].
- Autonomous systems with deep learning capabilities can easily navigate and work in complicated situations and these systems can predict and adjust to different fluctuating environments. Such progress needs a large volume of streaming big data with a wide variety of data types that are stored in the big, enhanced data storages for collecting and processing procedures [4-5].

CONSIDERATIONS

- The above emerging and disruptive technologies are moving forward exponentially while technological developments such as kinetic robotics automation systems need a comprehensive supervision plan. One of the main concerns about AI technology is accountability due to its possible risks which may harm individuals when a wrong decision is made by an AI autonomously [6-15].
- Since AI systems will be trained based on defined data sets, it may be employed for discriminatory purposes with biased data. Controllability, explainability, and transparency should be taken into account because most of the deep learning applications are assumed as "black-boxes" and their performances can not be explained and interpreted [6-15].
- One of the militaries uses of AI (dual-use application of AI) is lethal autonomous weapons systems (LAWS) which are sometimes called "killer robots". It should be noted that there

is no united description of LAWS and all definitions regard utilizing the autonomous/robotic systems with different autonomy degrees for selecting and targeting the lethal results [6-15].

- Ethical principles on AI consist of different codes of conduct and among them are beneficence, human dignity, privacy, human autonomy, fairness, and explainability [6-15].
- For autonomous systems that are used in military fields, further ethical considerations are added such as human control and accountability of designers and operators. On the other hand, in case of autonomous systems, predictability and explainability should be taken into consideration [6-15].
- Policy makers and administrators have critical roles in making decisions for the above dual-use enhancements and should pay more attention to the algorithm's controllability which provides more public interest in the long term. Launching commercial products quickly without adequate due process and entering products into the military domain may lead to them being used for unethical applications [6-15].
- The dual-use concept needs security measures since many designers are not aware of the possible risks of dual-use and many commercial corporations are not sufficiently invested in this important consideration given they are experiencing intense competitions [6-15].
- Secure and protected programming environments that cannot be easily accessed may reduce the risk of unintended usage of AI algorithms. On the other hand, in all development procedures the ethical codes of conduct should be considered and incorporated to study all possible scenarios such as design faults or poor safety measures [6-15].

RECOMMENDATION

- One of the promising approaches to prevent transcending AI in comparison to the human intelligence is to produce AI devices having restricted and limited capabilities. This implies one should avoid to employ multi-task AI systems. It should be pointed out that each AI system should be designed to concentrate on its own specific set of tasks. In addition, AI systems should not be capable of improving and extending their codes as they should demand more processing and RAM resources.
- Limiting AI systems to extend their original code in order to overcome the control by the manual user could be achieved by employing compiled version of the codes instead of using interpreter programing languages to execute the codes.

REFERENCES

1-https://www.forbes.com/sites/cognitiveworld/2019/01/07/the-dual-use-dilemma-of-artificial-intelligence/#706f72f26cf0

2-https://emerj.com/ai-sector-overviews/everyday-examples-of-ai/

3-https://www.forbes.com/sites/bernardmarr/2018/11/19/is-artificial-intelligence-dangerous-6-ai-risks-everyone-should-know-about/#72160c812404.

4- http://bwcio.businessworld.in/article/The-Double-Edged-Sword-of-AI/10-02-2020-183770/

5-Haas, M. C., & Fischer, S. C. (2017). The evolution of targeted killing practices: Autonomous weapons, future conflict, and the international order. *Contemporary Security Policy*, *38*(2), 281-306.

6-de Ágreda, Á. G. (2020). Ethics of autonomous weapons systems and its applicability to any AI systems. Telecommunications Policy, 101953.

7- https://towardsdatascience.com/solving-the-ai-accountability-gap-dd35698249fe

8-Jason Millar, et al (2018). Discussion Paper for Breakout Session Theme 3: Accountability in AI Promoting Greater Societal Trust. G7 Multistakeholder Conference on Artificial Intelligence.

9- Board, D. I. (2019). AI principles: Recommendations on the ethical use of Artificial Intelligence by the Department of Defense. *Supporting document, Defense Innovation Board*.

10- Clarke, R. (2019). Regulatory alternatives for AI. *Computer Law & Security Review*, *35*(4), 398-409.

11- Allen, G., & Chan, T. (2017). *Artificial intelligence and national security*. Cambridge, MA: Belfer Center for Science and International Affairs.

12- Kant, L., & Mourya, D. T. (2010). Managing dual use technology: it takes two to tango. *Science and engineering ethics*, *16*(1), 77-83.

13- Williams-Jones, B., Olivier, C., & Smith, E. (2014). Governing 'dual-use'research in Canada: a policy review. *Science and Public Policy*, *41*(1), 76-93.

14- https://emerj.com/ai-future-outlook/weaponized-artificial-intelligence/

15- https://www.aiin.healthcare/topics/privacy-security/4-recommendations-combat-malicious-use-ai