BRIEFING NOTES

BN-25-The role of AI-Oct2020

DUAL-USE TECHNOLOGY POLICY FOR AI

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) and machine learning are among the most important technologies being innovated. There are controversial topics regarding the possible benefits and drawbacks of artificial intelligence based on its dual-use nature.
- In this report, some technical aspects of the dual-use concept in artificial intelligence technologies domain are described. The different features of AI's dual-use technologies can be the first essential clues to get insight for policy making.

CONTEXT

- Artificial intelligence (AI) represent technologies that are based on the launch of intelligent software and hardware and that are skilled to learn and solve problems. The dual-use nature of AI technology requires more attention due to adverse utilization of designed tools in nefarious targets such as weapons besides other beneficial both military and civilian purposes.
- The fast-evolving AI technologies and applications will lead to several dual-use applications that may put security of individuals, governments, businesses, and academia in danger as well as the basic human safety. The AI's expansion, extension, and capabilities will result in major public security concerns.
- AI products do effectively facilitate our everyday lives, be it in for example, smartphone location data which determine traffic movement speed in applications of the Google Maps, the price of a ride while using ride-sharing applications such as Uber or AI autopilot in commercial flights.
- In addition to considerable benefits that are delivered by AI systems, there are certain threats that they pose to the public security. For instance, advanced weapons systems and facial recognition technologies, where decision-making algorithms could be employed for adversarial and terrorist purposes [1-3].
- Autonomous weapons that are powered by machine learning and AI systems need careful assessments based on AI's capabilities. Image processing, data collection, and fire control are the main tasks of AI and machine learning in autonomous weapons.
- The elementary AI applications are coded by humans which 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. It follows that this programming manner is established on human's ability of understanding the environmental features and modeling the problem that in most cases are limited and simplified.
- On the other hand, machine learning can assist in nonlinear cases and complex deep learning concepts and methodologies. To overcome the above limitations, a machine can be taught as to how 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 the machine learning literature could be seen as one of the most noticeable revolutions on the future of warfare. Autonomous systems with deep learning capabilities can easily navigate and work in complicated situations and these systems can predict and adjust to different evolving and uncertain environments [4-5].

CONSIDERATIONS

- One of the main concerns about AI technology is accountability given the possible risks that may cause harm to individuals when wrong decisions are made by an AI autonomously.
- Since AI systems are trained based on defined data sets, it could be employed for discriminatory purposes with biased data. Controllability, explainability, and transparency should be taken into account since most of the deep learning applications are assumed as “black-boxes” and their performances cannot be explained and interpreted.
- It should be pointed out that one of military uses of AI (dual-use application of AI) is lethal autonomous weapons systems (LAWS) that are sometimes called “killer robots”. Moreover, there is no common description of laws and all definitions with respect to utilizing robotic systems have different degrees of autonomy for selecting and targeting with lethal results.
- Ethical principles on AI consist of various codes of conduct and among them are beneficence, human dignity, privacy, human autonomy, fairness, and explainability. For autonomous systems which are used in the military, 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 also be taken into consideration.
- Administrators have critical roles in making decisions for the above mentioned dual-use enhancements and should pay particular attention to the algorithm’s controllability that provides further public interest in the long term.
- Dual-use concept needs security measures since many designers are not aware of the possible risks of dual-use technology and many commercial corporations are not considering this important issue given that they are confronted with intense competition. Furthermore, the misused application of AI by non-state actors result in national security risks and financial losses.
- Some secure and protected programming environments that cannot be easily accessed may reduce risks of unintended usage of AI algorithms. On the other hand, in all development procedures ethical codes of conduct should be considered for study of all possible scenarios as in design faults or poor safety techniques [6-15].

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