NOTE FOR NATIONAL DEFENCE:
Data Restriction for AI-based Dual Use Technologies

Authors: R. Bahrevar[1] and K. 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

- The progress of countries with non-transparent policies in advancement of AI-based technologies is one of the main concerns of governments and regulators such as the U.S. and EU.
- Our goal is to mainly focus on how Canadians should be concerned with non-transparent AI-based applications.
- The question is how one can regulate the potentially dangerous AI-based applications with non-transparent data policies?

CONTEXT

- In each century, people's view of what is ethical changes, therefore rules and regulations have been updated based on what the general population perceives as ethical or moral behavior. Sometimes a catastrophic event may lead to new regulations, and in another instances, foresight and proactiveness.
- It is important to regulate AI-based technologies that can potentially be used under military-civil applications.
- Policies that demand AI developers to unconditionally share their data with the government can be a potential threat to the privacy of Canadian consumers, government officials, and in general national security.
- From the EU's perspective, international collaboration with such countries can lead to better transparency and getting power from hardliners. It suggests that collaboration will

lead to familiarizing themselves with their intentions while having significant economic benefits [1].

- Moreover, due to restrictions such as the privacy of consumers, countries with transparent policies are deemed to be at a disadvantage in terms of the development and advancement of AI-based applications in the areas such as facial recognition [2].

CONSIDERATIONS

- Developing counter AI capabilities [3].
- Establishing AI safety organizations, ability to ban a certain application with treaties are some of the suggested policies [4].

NEXT STEPS

- For dual-use AI applications that can be potentially dangerous:
    - Promoting usage of data centers that are located within a safe-zone to the domestic AI developers. For example, data centers belonging to countries that possess transparent AI policies.
    - Risk assessment to provide stricter measures for AI-based applications that pose greater threats.
- Setting a standard for non-discriminative rule that demands transparency from AI developers in the case of AI technologies having a high risk of military-civil capabilities.
    - The rules prevent any AI developer from using non-secure data centers.
    - Sharing data to unauthorized third parties.
    - Banning access to non-essential data for the AI applications.
- Promoting Edge computing. Edge computing prevents the need for data to travel across the continent and improves the consumers' data security.

References

[1] Stumbaum, M.B.U., 2009. *Risky Business?: the EU, China and dual-use technology*. European Union institute for security studies.
[2] Yuan Yang, Madhumitamurgia , LA TIMES https://www.latimes.com/business/story/2019-12-09/china-facial-recognition-surveillance, 2019
[3] Thomas, M.A., 2020. Time for a Counter-AI Strategy. *Strategic Studies Quarterly*, *14*(1), pp.3-8.
[4] Allen, G. and Chan, T., 2017. *Artificial intelligence and national security*. Cambridge, MA: Belfer Center for Science and International Affairs.