BRIEFING NOTES

BN-73-The role of AI-Aug2021

DATA RESTRICTION FOR AI-BASED DUAL USE TECHNOLOGIES AND AI DEFENSIVE MEASURES

Authors: Reza Bahrevar[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

- 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 Canada, US and EU.
- The question is how one can regulate potentially dangerous AI-based applications that have non-transparent data policies?
- One needs to mainly focus on and analyze how Canadians should be concerned with non-transparent AI-based applications.
- Advances in AI technologies have now been transformed into an arms race between Western democracies and China, and the next nuclear capable country, and/or who has it first and who becomes more advanced.
- While ethics and privacy may be perceived as a natural barrier to development of certain AI cyber-offense modalities, it should also push one to preserve security, privacy, and right of civilians through AI cyber-defensive capabilities.
- One needs to highlight areas that require consideration of policy development for AI-based technologies that may enhance the defensive capabilities of the Canadian Armed Forces.

CONTEXT

- In each century, people's view of what is ethical is changing, therefore rules and regulations have been updated based on what the general population perceives as an ethical or a moral behavior. At times a catastrophic event may lead to new regulations, and in other instances to foresight and proactiveness.
- It is important to regulate AI-based technologies that can potentially be used and fall under both military-civil applications.
- Policies that require 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 reduced power from the hardliners. It suggests that collaboration will lead to familiarizing one with others intentions while having significant economic benefit [1].
- Furthermore, due to restrictions on privacy of consumers, countries with transparent policies can be deemed to be at a disadvantage in terms of development and advancement of AI-based applications in the areas such as facial recognition systems [2].

- The next generation of warfare is perceived to be enhanced with AI-based technologies. The tools that are based on C4ISR, whether the efficiency is currently sufficiently high or not, will imply that the countries that possess AI-based warfare technologies are deemed to be superior in terms of futuristic arm race, due to factors such as sensory capabilities and fast decision-making functionalities [5].
- Cyber-threats against nuclear and sensitive military systems, ISR (Intelligence, Surveillance, Reconnaissance), and robotic/autonomous systems warfare are some of the areas that will become more advanced/threatening with the further integration with AI-based technologies [6].
- Investing in AI-offensive warfare may seem to be a simpler and more convenient approach, although there can be humanitarian, privacy, and other ethical barriers that may prohibit the development of certain types of such technologies (e.g. image recognition-based surveillance systems).
- The absence of robust defence policies is a significant contributor to further uncertainty in case of AI-powered confrontation scenarios and capabilities.
- For example, AI-based robotic/autonomous systems warfare can provide a cheap counter against advanced technologies such as submarines or fighter jets, but how should they be stopped? [5].
- Furthermore, the threat is not always international and individuals and non-state actors with malicious intentions may use such systems for their malicious intents. Therefore, AI defense can cover a broader and more imminent class of adversarial threats, especially now, with easy and cheap access of the malicious adversaries to AI-empowered technologies.

CONSIDERATIONS

- Security and privacy considerations for vehicular cloud computing with respect to advancements made in IoT, edge-cloud and 5G should be further investigated.
- Developing counter AI capabilities [3], and establishing AI safety organizations, ability to ban certain applications with treaties can be considered as some of the suggested policies [4].
- In [5], they categorize AI-enhanced capabilities to:
    - Digital security: against threats such as phishing, impersonation, and data poisoning.
    - Physical security: swarm attacks by drones for targeted assassinations.
    - Political security: such as surveillance, breaching, and deception.
- Investing in cyber-defense tools [6]:
    - Analyzing classification errors, and
    - Automatic detection of vulnerabilities.

- For dual-use AI applications that can be potentially dangerous to the society one can consider:
    - Promoting usage of data centers that are located within a safe-zone to the domestic AI developers. For example, data centers can belong to countries that possess transparent AI policies.
    - Risk assessment to provide stricter measures for AI-based application that pose greater threats.
- Setting a standard non-discriminative rule that demands transparency from AI developers in case of AI technologies that have high risk of military-civil capabilities.
    - The rules prevent any AI developer from using non-secure data centers,
    - Sharing data to unauthorized third parties, and
    - Banning access to non-essential data for the AI application.
- Promoting Edge computing. Edge computing prevents the need for data to travel across the continent and improves consumers data security.
- A number of important areas of security against the AI-based warfare tactics are as follows:
    - Secure cyber-space:
        - Using identity authentication methods in data transfer.
        - Promotion of secure data centers for data transfers such as AZURE government and AWS government to limit the capability of outsider threat by enhancing local data centers.
        - Promotion of robust AI-based intrusion detection systems:
            - Adversarial awareness, by investing in determining and examining possible breaches into the security systems before it occurs. In other words, the offense must be a way to examine the defensive measures.
            - Explainable: Investing in methodologies that provide a traceable record of the event that has happened. Who? What? Where? When? And Why? [7]
    - Investing in cognitive security analytics.
    - Examining technological warfare through understanding and analyzing the counters to technological threats that will make one alerted for possibilities:
        - Categorizing the dual use nature of AI technologies such as UAVs, packaging, or assassination?
        - Finding effective ways for countering advanced warfare such as AI-based swarm attacks, for example, one can build a playbook based tactic and invest in AI-based methodologies that can counter them:
            1. Electromagnetic-based AI weapons,
            2. Communication jammers, and
            3. Hijacking the swarm of drones with data injection cyber-attacks

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.

[5] Johnson, J., 2019. Artificial intelligence & future warfare: implications for international security. Defense & Security Analysis, 35(2), pp.147-169.

[6] Johnson, J., 2019. The AI-cyber nexus: implications for military escalation, deterrence and strategic stability. Journal of Cyber Policy, 4(3), pp.442-460.

[7] Szczepański, M., Choraś, M., Pawlicki, M. and Kozik, R., 2020, July. Achieving explainability of intrusion detection system by hybrid oracle-explainer approach. In 2020 International Joint Conference on Neural Networks (IJCNN) (pp. 1-8). IEEE.