NOTE FOR NATIONAL DEFENCE: Artificial Intelligence: National Security and Policy Considerations

Authors: M. R. Nematollahi [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

- Apart from the beneficial uses of AI for providing higher levels of security, there is always the possibility that this technology can be used by adversaries and cybercriminal groups that may put a nation's digital, political, and physical security at risk. Such threats will constantly evolve alongside the ongoing advancements in AI.

- The emergence and growth of smart cities, interconnected critical national infrastructure, and the Internet of Things (IoT) generate new risks and vulnerabilities. Terrorists could take advantage of such weaknesses to disrupt the security of nations. Therefore, government agencies must predict and provide proactive approaches to prevent AI-enabled security threats before they become more serious and possibly become out of control.

- Although the use of weaponized AI systems has not yet reached practical and widespread levels, it is becoming a concern among experts. The currently commercial AI systems have the potential to evolve into hazardous weapons by terrorists and adversaries. For example, it is possible to use drones and autonomous vehicles to carry out kinetic attacks—a process that can be performed by low-skill individuals with little effort.

- According to legal and ethical frameworks that have been suggested and devised for the use of AI, any analysis of data obtained through intrusive techniques must be subject to the required ongoing human rights proportionality assessment. Moreover, regulations regarding AI must not operate in isolation from the present regulatory regimes. AI regulations and norms need to be developed within the perimeter of existing regulatory frameworks.

- While AI can be employed as an efficient tool for diminishing the possibility of intrusion and data evasion through reducing the volume of data that needs to be studied by human operators,

it also might be utilized to act as a twofold tool by increasing the risks of privacy intrusion throughout the collection, storage, and analysis processes and retention of personal data that would constitute as an infringement of human rights.

- In comparison to human operators, AI has the capability to cross analyze massive data-sets at high speeds and to detect the underlying patterns and anomalies much more effectively and efficiently. Therefore, it allows and enhances defence systems to comprehend situations in complex, evolving, unknown, and interdependent areas of operation more deeply and thoroughly. Moreover, it gives the Canadian Arm Forces the advantage of anticipating adversary's manoeuvres through maximising the exploitation and dissemination of intelligence.

CONTEXT

- Since malware attacks have been growing rapidly in volume and frequency, it is necessary that more advanced forms of AI-based antivirus be used in order to detect such threats without the need to rely on a pre-defined list and to respond in real time. In other words, AI must be able to spot the subtle signals of never-before-seen cyber-threats without the need for a direct human decision-making process.

- Cyber-attacks rely on algorithms which frequently change the identifiable features and in doing so they might be able to attain a level of adaptability that makes it virtually undetectable to antivirus software. Also, such AI-based malware can recognize the most vulnerable targets and adapt to their environment for the purpose of self-propagation through autonomous decisions.

- Moreover, among the possible issues that may arise are the automation of social engineering attacks as well as the supply chain attacks on training data. The former can go so far as to the development of chat-bots gaining human trust during longer and more creative online dialogues. And the latter could make AI systems to behave erratically and unpredictably.

- There has been growing concern regarding the creation of "deep-fake" synthetic media in the field of political security. It involves the use of ML algorithms which combine and modify an existing piece of media such as an image of an individual's face onto genuine content. Such technology may have disruptive impacts on democratic processes as videos of a person speaking can be made using only a single photo.

- Although it is possible to recognize the fake nature of such data through the work of media forensic experts, the problem is that in case of a time-sensitive situation the identification process might take time and one will not be able to prevent the adverse impacts. Besides, data tends to spread online quite rapidly and such mistruth can push individuals in positions of power to take reactive decisions without having adequate information and instead being exposed to misinformation.

- A significant concern is the possible loss of accountability of the overall AI decision-making process due to the 'black box' nature of specific ML methods. In other words, it is impossible

for human users to fully comprehend deep learning methods as they cannot assess and understand all the factors that were considered during the computational steps. Also, it increases the risk of human operators relying on AI systems and the insights derived from them while overlooking their own professional judgement.

- As far as the armed forced are concerned, AI must be employed as a means to perform missions but not as an end to all. Military AI applications have been developing to aid strategists and commanders in their operational and organizational responsibilities. AI incorporates aspects such as distributed intelligence and semantic analysis to help gain speed and room for manoeuvre for the purpose of recognition and detection of targets in the field, while ensuring compliance with the laws of war.

- AI offers several advantages within the defence criteria. For instance, it can improve the comprehension of situations by optimizing the time and speed needed for the assessment of a possible threat along with the response to it. Also, when planning and conducting operations, AI helps saving time in accessing and processing data that allows more scope and minimizes the element of surprise.

- Furthermore, AI can monitor and process massive health data of the personnel to identify risk factors related to the environment and working conditions of armed forces. Consequently, it can provide the personnel with enhanced protective measures to minimize the unwanted and adverse impacts of combat on their health.

- Moreover, through simulation AI is capable of improving the individual training, as well as the training of units. It is beneficial to personnel as they will engage in combat at a distance and are better protected. For instance, individuals will not have to be fully present in situations such as contaminated environments or mine clearance on land.

- Among the benefits of using AI for defence and military purposes are: “1) improved discrimination between combatants and non-combatants, 2) enhancing proportionality by controlling the effects of weapons according to the threat, 3) guaranteeing that action is determined strictly by need”. In other words, in case AI is managed and employed properly, it will lead armed forces to follow and apply the fundamental principles of laws of armed conflict.

- Also, AI provides the personnel with the opportunity to focus on high-value tasks such as decision-making, as it performs many ancillary and repetitive and time-consuming tasks. It has been estimated that 80 percent of human errors occur while they perform mechanical routine chores. Therefore, the use of AI for such tasks will also reduce and limit such errors. Also, the predictive measures that AI offers can enhance resources, technical management and scheduling of maintenance operations.

- However, as AI will be inherent in all systems and it will be easily available due to diversion of commercial technologies, the evolving threats that might come with it will soon become much more pressing. Among these threats are: 1) the possibility that AI in the hands of adversaries will have the ability to anticipate the modes of action of defensive systems, and 2)

Through neutralization, deception or diversion of defensive technologies, adversaries will be able to paralyze the command & control capabilities.

- Moreover, AI can push the developed nations into a form of competition in the defence field, which will destabilize the existing balances and could result in technological disruption. In other words, due to the vast future scope of AI, most countries believe that employing AI will alter the military power hierarchy to their advantage. However, technological application of AI in military contexts can be beneficial only if used asymmetrically.

- Another concern that has been growing among experts is that AI has the potential to blur the lines between reality and fiction through creating deep-fakes, behavioral analysis software applied to opinion groups, or dissemination of disinformation or mistruth at high speed on large scales. Such issues can negatively affect and undermine the political credit of democracies. And as advancements in the field of AI are quite rapid, it will not give governments sufficient time to come to agreements and terms and to build trust regarding the use of AI in the military context and arms control.

CONSIDERATIONS

- There is controversy among experts and legislators regarding regulations that must be applied to the use of AI. It is believed that with the rapid expansion of AI it will be ever more complicated to realize the nature and extent of the analytical work that has been done on the data. Therefore, identifying and measuring the intrusion that has been caused by obtaining and retaining data might be difficult to achieve.

- Consequently, a necessary step that must be taken by legislators and policy makers is to reassess the potential for intrusion constantly as analytic processes change and develop. In this regard, the human rights proportionality test provides criteria that the agencies can use to assess the legitimacy of new uses of technology, including AI. However, the focus of the current authoritarian processes must shift from data collection to its subsequent analysis which is in need of further transparency.

- The current flow of communication data analysis has raised concerns regarding the insights that can exploited about an individual's personal life. Also, the process of collecting and examining bulk datasets about individuals who are not of intelligence interest has been regarded as an intrusion into individual rights which is in need of additional evaluation from an ethical point of view. Therefore, it is essential that policy makers for national security uses of AI shift their attention to problems of necessity, proportionality, transparency, accountability, and collateral intrusion risk.

- Furthermore, due to the context-dependent nature of these challenges, any policy making efforts and frameworks must be 'mission-agnostic' and principles-based, implying that legislators have to come up with standardized processes that oblige AI projects to perform

according to the established routes for empirical evaluation of algorithms within their operational context, while assessing these projects' legal requirements and ethical norms.

- Moreover, it has been argued that algorithmic analysis of data could be more intrusive than parametric keywords searches by human operators. The European Court of Human Rights claims that algorithmic analysis of data causes far greater risks of privacy violation that the automatic collection and storage of data. However, there is controversy regarding the interpretation of intrusion which argues that it should not be assumed that the use of automated processing methods is inherently less intrusive than human review.

- While the use of automated and algorithmic methods for collecting and analyzing data is prone to errors and intrusion, AI analysis could be regarded as a more proportionate alternative to human review for the purpose of identifying and mitigating threats. Yet, there is some concern as with the use of multiple AI systems that might result in a "cumulative intrusion risk". In other words, interaction of algorithmic systems could result in compounded effects and higher levels of data and privacy violation. Therefore, internal processes are required to monitor these systems and their cumulative effects.

- Another challenge that comes with the use of AI is the problem of the reliability of AI systems used to process personal data. Particularly in case of an AI system being integrated into a national security context. Under such circumstances, possible errors can lead to undesirable outcomes, specially when the AI is employed for decision making processes that may result in direct action being taken against individuals.

- To tackle this problem context-specific evaluation processes are required, through which the agencies can monitor the validity and reliability of the statistical algorithms that have been employed. It is crucial that the real-world effectiveness of such AI systems, as well as their statistical accuracy, be evaluated in a live operational context. Moreover, standardized terminology must be developed to properly communicate error rates and technical information to human operators.

- Algorithmic profiling has raised great concerns regarding the ability of ML algorithms to develop comprehensive and reliable profiles of individuals without intruding data and invading human rights through bias or discrimination. In other words, this process may expose individuals to targeting, stigma and stereotyping of particular vulnerable groups as "risk".

- Such behavioral profiling lacks transparency and overlooks consent and public knowledge. Also, the ways in which it is implemented and used will not be fully understood. It has often been claimed that such tools over-predict individuals from particular racial groups, gender, or certain neighbourhoods. Moreover, biases in historic data may result in important case-specific data being overlooked.

- Therefore, regulations and internal processes are required to safe-guard against bias in algorithmic decision-making and to provide fairness. As discussed by the Committee on Standards in Public Life, this will require ensuring diversity in AI project teams, as "a

workforce composed of a single demographic is less likely to check for and notice discrimination than diverse teams".

REFERENCES

- Babuta Alexander, Oswald Marion, and Janjeva Ardi (2020), "Artificial Intelligence and UK National Security: Policy Considerations", RUSI, Royal United Services Institute for Defence and Security Studies

- Report of the AI Task Force (2019), "Artificial Intelligence in Support of Defence", Ministere Des Armees