NOTE FOR NATIONAL DEFENCE:
Artificial Intelligence: Defense, Intelligence and National Security

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

- Artificial Intelligence (AI) has been rapidly growing within the field of defense and intelligence. Developed countries such as USA, Russia, and China have ever more become engaged in using AI's potential applications on a competitive level. However, this urge for employing AI for military and security purposes has downsides that have caused bureaucratic and technical challenges. Since AI is still an advancing technology many of its aspects remain untested and poorly understood that could result in catastrophic consequences in case of accidents or unexpected failures.

- Using AI in the military context is a twofold challenge for democratic nations. Although governments are attempting to supersede their adversaries in the competition for AI use in defense and intelligence, it is crucial that they put the safety of their citizens first by mitigating potential risks. In this regard, nations need to cooperate with their competitors to minimize the risks of inadvertent escalation and to prevent unintentional failures and miscalculations.

- Some countries such as China and Russia think of artificial intelligence as the new global arms race. It is believed that AI could be employed for defense and cybersecurity purposes while relying on the overwhelming amount of the public data that are available such as the unstructured social media data from both fringe and mainstream platforms, not to mention deep and dark web data.

- In other words, data scientists develop machine learning models capable of identifying cyberattacks, monitor on-the-ground enemy activity, and direct autonomous vehicles using

aerial photography or data from physical sensors in the field. Nevertheless, such unstructured data must be collected, curated and stored specifically for AI development.

- Since AI has the potential to drastically alter and revolutionize the global economic and military balance, it is necessary that policy makers, along with experts, estimate and assess its impact. Furthermore, in specific use cases one needs to clarify how countries and companies integrate AI into existing systems and platforms. In this regard two approaches have been recommended: the capabilities-based approach and the conditions-based approach.

- Although defense and intelligence leaders are willing to employ AI, they face certain limitations such as the problem of unreliability on the part of machine learning methods which in the field of defense could result in catastrophic failures. Therefore, it is highly recommended that such defense agencies employ machine learning systems merely in non-safety-critical settings, such as enterprise applications, and meanwhile one should focus on improving the standards of reliability, interpretability, and security of AI solutions for military applications.

CONTEXT

- Governments have been encouraging experts in the field of AI, along with advocates of civil society to attempt to better understand the nature of possible challenges of using AI technology for national and international security purposes, and to come up with actionable regulations and policies from a legislative point of view, in order to prevent future complications and downsides. In addition, governments need to go one step further by developing metrics through which they can evaluate foreign countries' AI sectors.

- In order to build a more secure and trustworthy AI which can be used for defense and intelligence purposes with minimum risks, experts have been attempting to develop AI applications that prioritize human-machine teaming and trustworthiness through testing and standardization. It is believed that AI machines should not be looked upon as fully autonomous systems and it is necessary that they perform under human supervision.

- AI can provide governments with the opportunity to establish a military and operational advantage against their adversaries. As with the field of intelligence, AI offers the possibility of using algorithms that can detect patterns and identify anomalies in large data sets. Consequently, they can provide valuable insights that improve situational awareness and support decision-making. For instance, in a military context, analysis of the imagery gained by drones helps human analysts to identify hostile activity.

- AI is a beneficial tool for building an effective human-machine teaming and coordinating between different intelligent agents and systems. Governments such as US draw on programs such as the Defense Advanced Research Projects Agency's (DARPA) Mosaic Warfare in order to collate and fuse information from various sensors and sources which allows better decision-

making based on real-time analysis. It provides the military sector with the capacity to adapt to complex events and to seize the initiative in high-stakes situations.

- Moreover, it has been claimed that integration of AI applications to streamline back-office processes, personnel management, and equipment maintenance can offer benefits such as improvements in functionality and longevity of military equipment, auditing and budgeting, as well as a rise in efficacy and a reduction of expenses.

- Also, using AI can help military forces to assess damage and to improve humanitarian response so as to reduce the disaster impact. Moreover, autonomous vehicles can drastically change the nature of military enterprise as incorporating AI into semi-autonomous and autonomous vehicles can provide ground vehicles, naval vessels, fighter aircraft and drones that can be employed to perceive and map the environment, and to detect obstacles while communicating with other vehicles with minimum human intervention, which results in better decision-makings in complex combat situations.

- Autonomous ground and aerial systems can be used for sensing and surveillance to provide reconnaissance and to improve situational awareness. Yet, as they are not fully developed technology they require further assessments, realistic experiments, testing and evaluations. As with the introduction of autonomous vehicles into the military field, the actual physical presence of personnel will be less required in hazardous and life-threatening missions such as explosive ordnance disposal and route clearance.

- However, this field is still in progress and not fully advanced and it may originate additional challenges such as fragility and lack of robustness of algorithms which can undermine the accuracy of the data collected and analyzed, as well as, unanticipated failures in performance when it comes to differences between air, ground, and underwater combat environments.

- There is an ongoing controversy regarding the use of AI for defense purposes. While many believe that employing AI can provide protection against incoming aircraft, missiles, rockets, and artillery which leads to the reduction in civilian casualties and collateral damage, others argue that using autonomous AI for military operations must be limited or banned as it raises serious ethical concerns.

- Therefore, it has been suggested that the use of AI whether for combat or noncombat purposes must be responsible, equitable, traceable, reliable, and governable to prevent mistakes and potentially catastrophic outcomes.

- In this regard, the legislative branch must work closely with experts and academics to establish and refine guidelines for implementing the ethical principles of AI throughout the entire life cycle of AI applications and to improve the safety and reliability standards of this technology. Also, nongovernmental organizations, humanitarian groups, and civil society organizations must be informed and involved in the process in order to promote public trust and to supervise the commitment to ethical AI.

- Competition in using AI to gain defensive supremacy against other nations must not put the citizens of democratic nations at risk and safety and security must always come first. Therefore, it is necessary to establish and to promote international cooperation for a healthy and risk free competition so as to prevent unwanted accidents and to consider mutual concerns. In other words, nations must prioritize the promotion of democratic principles and the development of research collaboration and common standards.

CONSIDERATIONS

- Available online data particularly those from social, deep, and dark web sources is a valuable source for training AI algorithms. Communication channels across the deep and dark web often signal targeted cybersecurity threats. Also, a variety of online spaces are used by extremist groups to spread disinformation and plan violent attacks. In addition, AI is used by foreign nation-states to conduct information warfare both domestically and abroad.

- In this regard robust AI and national security strategy could be used to address cyber risks. However, accessing such data does not suffice and in order to overcome cyber risks properly data scientists must collect, organize, and store this data efficiently and optimally for AI applications. This process is known as making online data “AI-ready”.

- To put it differently, the transition to AI ready systems will require the implementation of methodical and highly deliberative processes for collecting and curating data. Therefore, it is suggested that relevant data needs to be aggregated efficiently through a wide variety of data sources and types. Then, it must be catalogued and a large enough database established to develop effective machine learning models.

- Yet, it is not always possible through existing commercial APIs and threat intelligence platforms and the merging technology often develops faster than the public policy. Governments need to come up with solutions that deliver AI-ready data in order to keep up with AI technologies and to integrate them into defense environments.

- While major powers compete each other to achieve strategic advantage in AI, the precise terms of competition remain overlooked under the growing competitive pressures. Also, the rapidly shifting terrain of AI makes it even much more complicated for nations to define the means and the ends of this competition.

- In this regard, any fundamental uncertainties must be recognized and assessed. Policy and research communities have to come up with more transparent and recognizable metrics and methodologies for describing and understanding how AI will relate to different regime types and how it could exacerbate political tension between democratic and authoritarian powers.

- In order to assess the global competitiveness of AI two approaches have been suggested. First, the capabilities-based approach which focuses on indicators such as public and private sector funding for research and development, publications and participation at top AI conferences such as the Neural Information Processing Systems annual meeting.

- On the other hand, condition-based approach examines the innovation ecosystem and policy frameworks that make the design, development and deployment of AI capabilities possible. This approach focuses on the domestic pool of talent available and the educational systems required to produce high-end talent in computer science. Both approaches are necessary to assess a country's relative competitiveness in AI.

- Since data, algorithms and computing power are fundamental aspects of AI systems, it is essential that these systems develop and function within policy and regulatory frameworks that strengthen the capabilities and conditions that promote the security, prosperity and core values of democratic societies.

- Therefore, relevant communities should build metrics that enable evaluation of global competitiveness in AI. Moreover, the public-private partnership must be expanded and a national science and technology center must be established to collect information and disseminate relevant findings.

- Although AI appears as a promising asset to advancement of defense and intelligence, it still has limitations that must be overcome. Machine learning systems tend to malfunction in unexpected ways when given unfamiliar input. Also, these systems process data in ways that remain opaque and difficult to understand. Hence, for high-stake defence and intelligence context AI will be an unsuitable option since it is vulnerable to intentional manipulation and it often fails to handle novel situations properly. It particularly applies to systems that depend on "deep learning" methods.

- Therefore, defense and intelligence agencies must avoid the use of AI in non-safety-critical settings and instead they need to attempt to improve standards of reliability, interpretability, and security regarding he machine learning methods. It is necessary to ensure the performance and reliability of systems through testing, evaluation, validation, and verification (TEVV).

- However, machine learning systems have not been built around human-specified rules or procedures and instead process data through inscrutable numerical functions learned from data and due to the large amount of output they produce it will be challenging if not impossible to test all this data using TEVV paradigms. Therefore, new paradigms and processes such as "CD/CI/CV" (continuous development, continuous integration, continuous verification and validation) are required to increase the reliability and interpretability of AI in defense.

REFERENCES

- CSET (Center for Security and Emerging Technology), (2020) “Artificial Intelligence and National Security” Bipartisan Policy Center.

- https://www.securitymagazine.com/articles/93692-artificial-intelligence-and-national-security-integrating-online-data