BRIEFING NOTES

BN-79-The role of AI-Aug2021

PUBLIC AND DEFENCE POLICY CHALLENGES AND INNOVATIONS ON ARTIFICIAL INTELLIGENCE, AUTONOMOUS SYSTEMS, AND CYBERSECURITY
PART 2: DEFENCE POLICY CHALLENGES OF ARTIFICIAL INTELLIGENCE

Authors: Neshat Elhami Fard [1], Rastko R. Selmic [2], 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) is a fast-growing branch of science that has significant implications for national defence [1].
- AI creates unique challenges for integration with the military, especially since a significant part of AI development for the military occurs in the commercial sector [1].
- Three countries that are fiercely competing in integrating AI and military activities are the United States, Russia, and China [1].

CONTEXT

There are diverse AI applications for the defence category which are classified as follows [1]:

- **Intelligence, Surveillance, and Reconnaissance:** AI in the defence category can be beneficial in analyzing large volumes of data. AI has automated the workforce of data analysts who have to spend a lot of time analyzing various data to make essential decisions. In this field, multiple projects have been developed that are integrated with AI and generate analytical tools. These projects are developing algorithms for multilingual speech recognition and translation in noisy environments, fusing 2-D images to create 3-D models, geo-locating images without the associated metadata, and building tools to infer a building's function based on pattern-of-life analysis.

- **Logistics:** In the field of military logistics, the use of AI has been welcomed. In the military, AI is used to predict aircraft maintenance instead of repairing damaged parts. Information is extracted from various aircraft parts, such as the engine, through real-time sensors and entered into a predictive algorithm. By focusing on the input data, this algorithm detects which parts of the aircraft should be inspected or which parts should be replaced. The AI scheduled maintenance program is another method to inspect different parts of an aircraft by schedule.

- **Cyberspace Operations:** Since the standard cybersecurity tools seek to find pre-known matches to detect malicious codes, malicious users only need to change a small part of the code to disrupt the defence. In contrast, AI cybersecurity tools are trained to find irregularities in wider patterns of activity within a network and strengthen the protection. AI cybersecurity tools must be able to "detect, evaluate, and fix software vulnerabilities" within seconds so that military systems are able to

perform tasks and defence simultaneously. This operation must be completed before an attack can take place.

➕ **Command and Control:** In command and control, the United States military seeks to centralize operations in the air, space, cyberspace, sea, and ground with AI. In this project, the information collected by different sensors are gathered in one place by AI and used centrally to control the systems.

➕ **Semiautonomous and Autonomous Vehicles:** The United States military seeks to find a way to combine AI with autonomous and semi-autonomous systems. These autonomous and semi-autonomous systems are unmanned aerial vehicles (UAV), unmanned ground vehicles (UGV), fighter aircraft, unmanned naval vessels (UNV). Integrating AI with autonomous and semi-autonomous systems aims to understand the surrounding environment, identify obstacles, navigate, and interact with other agents as a single agent in a multi-agent system.

➕ **Lethal Autonomous Weapon Systems (LAWS):** These weapons utilize sensor suites and computer algorithms to recognize the target, independently and autonomously. Afterward, they use an onboard weapon system to damage the target. All control steps in these weapons are performed without human intervention. These weapons are used in high-risk and degraded environments, the environments where old weapons cannot be used, or environments where the direct presence of people is not possible.

CONSIDERATIONS

The integration of AI and Military has created challenges that include [1]:

➕ **Technology:** The challenges of military vehicles in combination with AI in the field of technology are:

➕ These vehicles must be able to move and operate in places where map data is fragile and very weak due to security issues.

➕ A trap set by the enemy may disable the GPS of these vehicles.

➕ These autonomous and semi-autonomous military vehicles must be able to navigate off-road, unlike their commercial counterparts.

➕ **Process:** The challenges of military equipment in combination with AI in the field of process are:

      ❖ Processes such as standards of safety and performance.
      ❖ Acquisitions.
      ❖ Intellectual property and data rights.

- **Personnel:** The challenges of the military and defense industry while using military equipment in combination with AI in the field of personnel are:
- There is a challenge related to the salaries of skilled AI personnel. The recruitment and retention of AI personnel in the defense industry are lower than that of companies and commercial industries due to lower wages.
- There is a challenge related to the quality of life of skilled AI personnel. These employees believe that working in industries outside the government and the defense industry will bring about significant and better changes in people's lives.

- **Culture:** The intra-structural cultural factor of the defense industry is one of the significant challenges in combining AI with military equipment. Combining AI and military can change standardized procedures within the organization, which can change staff roles or eliminate them.

The opportunities and challenges that AI has created in the military are [1]:

- **Autonomy:** Autonomous systems have a kind of AI that allows them to be reinforced to replace humans in some high-risk, dirty, and dull environments, for instance, environments contaminated with chemical weapons. The characteristics of these systems are to reduce costs as well as reduce potential risks to combatants.

- **Speed and Endurance:** Military systems combined with AI, have the power to respond to any situation at a speed of GHz.
- **Challenge:** However, this increase in speed should not go beyond human perception and control because it will destroy the entire system if it goes beyond human control.

- **Scaling:** AI can multiply cheap military systems and create robust AI multi-agent systems to pressure enemy systems and make significant savings.
- **Challenge:** However, the development of AI in military systems may separate the military power of countries from the economic power and size of the country so that small countries can use the effects of AI scaling to create a significant impact on the battlefield.

- **Information Superiority:** AI in military systems provides the ability to analyze more data. For example, analyzing high-quality videos recorded by 11,000 drones

daily requires advanced equipment as well as many experts that AI can meet these needs. Therefore, AI can be considered a war advantage by improving the quality of information and analyzing more data with high speed.

- **Challenge:** However, this type of AI development in military systems is significantly expensive.

- **Predictability:** AI algorithms often generate unconventional and unpredictable outcomes in such a way that these results are very innovative and surprising. The creation of these innovative results is due to the ability of AI algorithms to analyze and examine each operation entirely before performing it. This capability is such that it has surpassed human performance.
- **Challenge:** However, as much as these algorithms produce unpredictable positive results, they can also fail unexpectedly, and this is a significant challenge for militaries in using AI algorithms.

One of the challenges that AI may pose in military programs is the lack of recognition of the environment and considering hypotheses different from human assumptions. This challenge may cause AI equipment to have lethal effects due to misdiagnosis of the environment and various assumptions. Therefore, in AI applications in the military, the ability to adapt between two different environments is one of the factors that should be highly considered.
Another challenge in using AI systems is that the error of one agent causes the error to be scaled throughout the multi-agent system, which causes the whole system to be disrupted simultaneously, whereas in a human military team, a human may make a mistake individually and not cause the team to fail and disrupt simultaneously.

- **Explainability:** Not all sophisticated AI algorithms are able to explain their processes due to their internal complexity. One solution to understanding the intricacies of these algorithms is to reverse-analyze them.
- **Challenge:** The ambiguity of the argument in military contexts can be a significant challenge because explanatory power can challenge the military's ability to validate the performance of an AI system.
- **Exploitation:** Increasing the number of AI systems enhances the number of hackable and exploitable items. However, if all AI systems components

have the same exploitable vulnerability, the vulnerability increases to the number of existing AI systems. Moreover, software-based AI systems are vulnerable to theft and exploitation by the enemy. Enemies may deliberately generate predictability in AI systems and disrupting the AI systems so that they can take advantage of those systems.

AI has had significant effects on war and combat. These effects are described in three ways, including [1]:

- **Minimal Impact on Combat**
- **Evolutionary Impact on Combat**
- **Revolutionary Impact on Combat**

NEXT STEPS

The next report will review the work done by the military of different countries in the research and development of AI systems in war weapons.

REFERENCES

[1] Hoadley, D. S., Lucas, N. J. "Artificial Intelligence and National Security," Congressional Research Service Washington, DC, November 10, 2020.