Military Innovation and Artificial Intelligence

Amy Ertan - Royal Holloway, University of London

Landscape

Consequences

1. Background

Artificial intelligence is used in a range of applications in the military, however how AI is implemented in defence contexts is poorly understood and under-researched. The present work aims to bridge this gap by asking: what potential security threats emerge through the implementation of AI technology in the military?

2. Landscape: Current Military Applications of AI

Michael Horowitz highlights **three** applications of AI in a military context:

- Machines acting **without human supervision**, (e.g. UAVs – drones)
- Enabling the **processing** and **interpretation** of large volumes of data (e.g intelligence)
- Aiding / Conducting the **command and control** of war (e.g decision-assistance platforms)

Current AI tech can **exceed** human task-based capabilities, offering opportunities to increase productivity and accuracy, and remove humans from physical harm. **However**, implementation often takes place in silos, without debates on accountability or long-term impact analysis. As one example, researchers have raised significant concerns relating to autonomous weaponry, in terms of how the technology is used but also on fears surrounding how an adversary may **compromise** or **repurpose** weaponised AI technology.

3. Landscape: The United States and AI Innovation

In 2014 US announced the **Third Offset Strategy**: a response to perceived erosion of military technical superiority to **China, Russia and Iran.** Subsequently, the US has invested hugely in military innovation, securing themselves as a global leader in military AI capabilities.

Oct 2016 — **Defense Innovation Board highlighted need for AI applied research**
Impact: Groundwork set for creation of US military and national security structures

April 2017 — **Launch of Project Maven**
Impact: Demonstrated speed of procurement, development and implementation, and private-public collaboration.

Feb 2019 — **Department of Defence AI Strategy**
Impact: First military AI strategy globally, highlighted US view of AI rapid-prototype implementation,

June 2019 — **Launch of the Joint Artificial Intelligence Centre**
Impact: JAIC aims to accelerate delivery of AI-enabled capabilities. The JAIV is also responsible for ethical, legal and safety concerns.

Global Activity: Most cutting-edge military innovation is kept **classified** – though in 2019 the UK MoD created an 'AI Lab' while France revealed their own AI military defence strategy, highlighting **state interest in military AI capabilities**. US activity widens the capability gap between itself and European NATO allies. Competition between global leaders may lead to **democratization (and proliferation of weaponized AI** as states attempt to catch up.

"The Department of Defense should not buy another weapons system without AI" – Jack Shanahan, *Head of JAIC, 2017*

4. Consequences: Security Threats

My research identifies and analyses the **unforeseen** and **unintended** security consequences of current implementation practices, categorized into three themes:

(I) Technical Vulnerabilities

How AI systems may be compromised and adapted for malicious gain

- **Weaponised AI**: Including technology repurposed / developed by malicious actors
- **Attacks targeting AI systems:**
  - Algorithms and training data sets - vulnerable to data poisoning, subsequent interference
  - May be misled through adversarial AI techniques

(II) Human-Machine Teaming

Examining the relationships between human and machine agents.

- **Inappropriate Trust**
  - Overreliance on machines
  - Humans lack of trust
- Employee De-skilling
- **Unexpected Complications** where goals are not achieved (manual work increases / humans are further exposed to harm)

(III) Strategy and (Geo)Politics

- An AI Security Dilemma: Willingness to use AI may escalate conflict and lead to the proliferations of offensive AI technology
  - Competition theory and the proliferation of AI technology – democratizing AI in conflict
- The changing nature of warfare: how AI impacts conflict strategy in terms of speed, tactics, and decision-making.

5. Future research

1. Taking a critical approach to dynamics in defence innovation and AI
2. Mapping the dynamics between military AI and responsible AI security mitigation planning.
3. Understanding how AI *impacts and* influences security strategy

Further Reading

1. Allen, Greg, and Taniel Chan. *Artificial intelligence and national security*. Cambridge (MA): Belfer Center for Science and International Affairs, 2017.
2. Burton, Joe, and Simona R. Soare. "Understanding the Strategic Implications of the Weaponization of Artificial Intelligence." *2019 11th International Conference on Cyber Conflict (CyCon)*. Vol. 900. IEEE, 2019.

EPSRC Engineering and Physical Sciences Research Council

ROYAL HOLLOWAY UNIVERSITY OF LONDON
For further information:
Email: Amy.Ertan.2017@rhul.ac.uk
Twitter: @AmyErtan

Information Security Group
Centre for Doctoral Training in Cyber Security
Royal Holloway, University of London