National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

ARTIFICIAL INTELLIGENCE IN THE OODA-LOOP

Major Bayo Ajayi

JCSP 45

Service Paper

Disclaimer

Opinions expressed remain those of the author and do not represent Department of National Defence or Canadian Forces policy. This paper may not be used without written permission.

PCEMI 45

Étude militaire

Avertissement

Les opinons exprimées n'engagent que leurs auteurs et ne reflètent aucunement des politiques du Ministère de la Défense nationale ou des Forces canadiennes. Ce papier ne peut être reproduit sans autorisation écrite

Canada

CANADIAN FORCES COLLEGE/COLLÈGE DES FORCES CANADIENNES
JCSP 45/PCEMI 45

15 OCTOBER 2018

DS545 COMPONENT CAPABILITIES

ARTIFICIAL INTELLIGENCE IN THE OODA-LOOP

By / Par le Major Bayo Ajayi

Word Count: 2, 253

Nombre de mots : 2, 253

ARTIFICIAL INTELLIGENCE IN THE OODA-LOOP

AIM

1. The aim of this service paper is to attempt to answer, or at least clarify, aspects of two existential yet very real and pressing questions that stem from the current Techno-Digital Information Age:

   a. Is the human brain capable of handling the increased cognitive burden of the digital information age and still effectively execute Command and Control (C2)? and

   b. What would be the implications of inserting artificial intelligence (AI) into the decision-making cycle?

INTRODUCTION

2. In its quest to become more effective a professional military force continuously strives to improve its application of combat power; a key tenet of which is the effectiveness of its decision-making cycle, which can be assessed on the speed and quality of the decisions made. As such, militaries the world over ferociously seek to outmatch each other through ever leaner and more capable C2 processes. As USAF Col (ret) John Boyd put it: “In order to win, we should operate at a faster tempo or rhythm than our adversaries […]”[1]. One attempt at gaining this advantage is the relatively recent use of powerful data processing in the form of computers. All signs point to the next attempt being the use of AI.

[1] Science, Strategy and War: The Strategic Theory of John Boyd, p. 141

3. This paper will first tackle the issue of the limits of the human brain in dealing with the enormity and complexity of the Information Age data-deluge. It will then utilize the OODA-loop model to examine the concept of decision-making itself and identify fields in which AI will potentially play a future role (and arguably already has). It will then tease out legal and ethical implications, and recommend key areas of military research and investment to ensure the CAF be best postured for when (not if) it makes place for AI in its decision-making loop.

DISCUSSION

4. The first component of decision-making is *observation* and the intake of information, in other words: ISR. By now, it is commonly understood that AI already has a major role in information collection and sharing at all levels (tactical to strategic). What is increasingly becoming apparent is how advancements in machine-learning are producing algorithms that vastly outperform humans in capacities of bulk info gathering, processing power, and pattern recognition. As such, if step one is defined as data collection, then it stands to reason that the human brain, equipped with its many flaws and limitations, would be ineffective compared to AI. The EW, Sig Int, and Cyber fields are already assisted by programs and algorithms to intake, sort, categories, and graphical depict and identify suspicious patterns along the EM spectrum and Cyber domain. As AI inevitably branches out into the nebulous areas of "human behavioural" data collection vice the more Cartesian "digital domain", concerns will rise as to the relevance and validity of the deciphered patterns. For the algorithms used to produce the info/knowledge deemed *worthwhile* invariably becomes the default lens through which observations are made. Will they be rose coloured lenses, shaded glasses, or simply clear. In a world drowned in irrelevant data — clarity is power. Therefore, programming of info-collection algorithms need be as *pure* as possi-

ble, free of any and all potential human biases, safe those collectively and openly upheld by the state and its population, which the military serves.

5. “The second O, orientation, [is often thought of as] the most important part of the OODA-loop since it shapes the way we observe, the way we decide, and the way we act.”[2] It is at this crucial step that options or COAs (courses of actions) are formulated and from which one is selected as preferred and acted upon. Just as AI is involved in the *observation* step, so too (although in limited fashions for the time being) is it already utilized to orient many of our decision-making cycles. As a quite literal example, given a permissive AOR, military entities attempting to orient themselves about the ground will often use a tool such as Google Maps (or similar). The Google algorithm intakes the positional information of the entity and that of the desired destination, computes the various potential routes, and presents a few options from which to choose from. Granted, most often the present options turn out to be preferable to the numerous other *unpresented* ones, but what of less simplistic examples where the subtleties of human behaviour, on the individual and collective scales, are the inputs? What of matters of much more consequence such as life and death?

6. Despite the plethora of poetic military quotes offering comfort to those desperately holding on to days gone by, the realities of the Techno-Digital Info Age have not only caught up to the times — they are here to stay. That said, assuming the AI-outputted options are shown to a single individual (or perhaps a select few), it will be near impossible when presented with COAs A, B, and C, for a person (or group) to pick D — not to mention extremely difficult to justify. Such usage of AI to pump out options would imply strict engineering, trials, and vetting processes to ensure that its outputs adhere to military laws and ethics. The legal aspect of the *orientation*

[2] Ibid, p. 197

step seems straight-forward, a mere matter of programming of set rules (an algorithm) into a given form of AI. Once entered, there is a reasonable expectation that the rules will always be adhered to. If and when laws change, simply change (update) the program — case closed. However, as will be addressed in the *decide* and *act* steps, the murkiness of the legal field rears its ugly head after decisions have been made and actions result in very real consequences having the potential for legal ramifications.

7. The ethical aspect lends itself better for examination when considering the *decide* step of the OODA-loop. First, let us acknowledge the inherent conflicting nature of the term “decision-making”. It is commonly agreed upon in military circles that decisions (or answers to a given problem) are best when derived (or arrived at) vice made (or personally chosen). Early on in their careers, militaries indoctrinate and teach its soldiers the value of following sound reasoning and processes (one could say almost mechanically) as opposed to following their own biases and proverbial *gut instincts* when confronted with a given situation. Nevertheless, assuming for now a case where a human would be charged of making a decision, i.e. a selection from a buffet of COAs… The *ethicalness* of a decision would rest squarely on the shoulders of the *decider* and depend greatly on his or her interpretation of the CAF Defence ethics policies — in many cases, an unenviable burden in this increasingly complex Techno-Digital info Age. Another option would be to assist (or outright replace) the human in the loop by AI. Enter the ethics-elephant in the room. How to ensure AI selects the most ethical option amongst the myriad of possibilities? At its very core, this implies a defining of (at best) abstract terms such as morals and values, as well as their reduction into mathematical form in order to be inserted into an AI’s algorithm. Admittedly, many soldiers have a hard time defining what CAF Defence ethics are, and rarely are those definitions identical, never-mind converting them into the universal language of pro-

gramming. To tackle this daunting task, the CAF ought to give consideration to major investments in the fields of ethics and morality — not very appealing on a recruiting poster perhaps, but indispensable if the CAF is to enter the age of AI integration in the decision-making loop.

8. The last step of the OODA-loop, *act*, is where combat power is brought to bear in accordance with a given set of directions and instructions. When all goes according to plan, the fallout is typically predictable and minimal. But when things go wrong, the questions mount and the finger-pointing begin. The current state of affairs sees humans issuing orders to other humans to execute, but as with the other steps of the decision-making cycle, AI will undoubtedly rattle the status quo. In such a scenario, the legal implication of accountability and responsibility are likely to be areas of heated debate. In the instance where orders are given from human to AI to carry out, it can be argued that the lines of accountability can easily be drawn back to the human. This view point rests its case on the argument that AI (assuming it has no *will* of its own) is merely executing what it has been programmed to do. It did not *decide* to destroy target “x” killing “y” number of enemy combatants and “z” number of civilians; no more than did the battle-axe of medieval times *choose* to slice open heads of rival foot soldiers. After all, “guns don’t kill people — people kill people”. It follows logically that the human *behind the gun* (or AI) should be the one responsible for his/her actions, i.e. answer for the issuance of flawed or dangerous orders, etc., as well as for the associated fallout and consequences. But what if orders were indeed sound and the desired outcome merely the source of faulty AI vice faulty human input? Can lines be drawn back to the original programmers of the AI itself? Akin to a present-day CAF member holding Colt Canada responsible for the result of an issued C7 riffle jamming at a critical moment in a firefight; could the manufacturers of the AI in question be held accountable for its shortcomings? Assuming AI can’t be held to account; this conundrum is at the heart of the legal

accountability matter. The notion of whether responsibility lies with its human programmers or with its human users is further muddied when nations around the globe are beginning to covert sayings such as “Corporations are people” into official legislation: “[…] corporation will have the same rights and obligations under Canadian law as a natural person”.[3]

10. On the other hand, an even more controversial scenario is one where humans could be held to account for acting on directions derived and given by AI. Both legal and ethical “alarms” go off in this case, as it could be tempting to view the human(s) at the *pointy end* as the *tool* and the AI as the *master*. *Legal* alarms go off because the current legal systems, both military and civilian, aren’t organized or geared to deal with such scenarios. Courts are merely making due with outdated structure and tools. As AI moves into the latter stages of the decision-making cycle, the inherent inadequacies of the legal system become glaringly apparent. A complete overhaul and rethinking of the system is required in order to even attempt to offer an appropriate legal framework on which to apply the notions of accountability and responsibility.

11. *Ethical* alarms also ring in similar circumstances. If militaries begin entrusting AI to *act* (or guide humans into acting), it would presumably be based on an assumption that AI was now deemed *safe* by some measure. In other words, that there existed some form of assurance that the AI always acted as predicted as per its programming, which in turn would be in line with CAF Defence ethics policies. One only need overlay a few historical examples such as the My Lai Massacre during the Vietnam War to illustrate the quagmire. In short, the incident saw a company of US Army infantry men brutally kill approximately 500 unarmed Vietnamese villagers in mere hours. A nearby USAF helicopter crew (including a gunner) eventually witnessed the ongoings and stepped in, inserting themselves between the infantry men and civilians, saving the lives

[3] https://www.ic.gc.ca/eic/site/cd-dgc.nsf/eng/cs06641.html

of a few remaining villagers. Now replace the ethically sound USAF helicopter crew with an AI UAV equipped with similar weaponry… would the result be an AI UAV opening fire on its own US Army soldiers in an attempt to prevent a developing war crime? If so, the programming of the AI had better *up to snuff* on its ethics, as the slightest mishap would be catastrophic. In a scenario where AI would fail an ethical behaviour litmus test, the CAF would quickly reacquaint itself with the legal implications too.

CONCLUSION

12. The Techno-Digital Info Age has brought upon militaries an overwhelming amount of data for the human brain to sift through. So much so, that AI is often required to assist humans in gathering, processing, categorizing and presenting of information to human decision makers. Hence, AI has made its way into our military human decision-making cycle and is raising legal and ethical questions. As AI creeps its way into the latter stages of decision-making, more profound questions surrounding accountability and responsibility arise from AI's participation in the OODA-loop. As it currently stands, it is clear that our legal systems are ill prepared to deal with the inevitable influx of AI into these more mature phases of decision-making.

RECOMMENDATIONS

13. It is recommended that the CAF invest resources into the fields of ethics and computer programming, specifically aimed at converting its Defence ethics policies into programmable code. In addition, the CAF ought to revamp its legal system enabling it to deal with plausible scenarios where AI (or its programmers) could be held to account if required. Such updates to the military legal system are unlikely to occur without simultaneous to the civilian justice system. Therefore, as a precautionary measure, it is recommended that the CAF refrain from utilizing AI in the *decide* and *act* steps of its OODA-loop until legislation has caught up to the times.

BIBLIOGRAPHY

Boyd, John “Science, Strategy and War: The Strategic Theory of John Boyd.” (2005).

http://www.forces.gc.ca/en/about/code-of-values-and-ethics.page

Cummings, M.L. “Artificial Intelligence and the Future of Warfare.” (2017). https://www.chathamhouse.org/sites/default/files/publications/research/2017-01-26-artificial-intelligence-future-warfare-cummings-final.pdf.

Stephan De Spiegeleire, Matthijs Maas, and Tim Sweijs. “Artificial Intelligence and The Future of Defense: Strategic Implications For Small and Medium-Sized Force Providers.” (2017) https://hcss.nl/sites/default/files/files/reports/Artificial%20Intelligence%20and%20the%20Future%20of%20Defense.pdf.