Artificial Intelligence Within the Military Domain and Cyber Warfare

Bil Hallaq[1], Tiia Somer[2], Anna-Maria Osula[3], Kim Ngo[4] and Timothy Mitchener-Nissen[4]
[1]University of Warwick, Warwick, United Kingdom
[2]Tallinn University of Technology, Tallinn, Estonia
[3] NATO CCD COE and Tallinn University of Technology
[4]Trilateral Research Ltd., London, United Kingdom
bh@warwick.ac.uk
Tiia.Somer@ttu.ee
Annamaria.osula@gmail.com
kim.ngo@trilateralresearch.com
tim.nissen@trilateralresearch.com

Abstract: The potential uses of machine learning and artificial intelligence in the cyber security domain have had a recent surge of interest. Much of the research and discussions in this area primarily focuses on reactive uses of the technology such as enhancing capabilities in incident response, aiding in the analysis of malware or helping to automate defensive positions across networks. In this paper, the authors present an overview of machine learning as an enabler to artificial intelligence and how such technology can be used within the military and cyber warfare domain. This represents a shift in focus from commercial, civilian machine learning applications that include; self-driving vehicles, speech/image/face recognition, fraud prevention, the optimisation of web searches, and so forth. While the underlying technological process remain, what is altered is the focus of application; i.e., applying machine learning to create Intelligent Virtual Assistants for the battlefield, automated scanning of satellite imagery to detect specific vehicle types, automating the selection of attack vectors and methods when conducting offensive cyber warfare, etc. machine learning solutions offer the potential to assist a Commander make decisions in real-time that are informed by the accumulated knowledge of hundreds of previous engagements and exercises that are assessed at computational speeds. With these potential use cases in mind, the authors highlight some of the legal and ethical issues that the application of weapons enhanced with artificial intelligence, machine learning and automated processes. As the authors highlight, however, there are conflict views over the ethics of weaponising these technologies. Critics question the compliance with International Humanitarian Law of automated weapon systems the exclude human judgment, charging them with threatening our fundamental right to life and the principle of human dignity. Conversely, others view this progress in weapon development as inevitable, whereby attempts to ban autonomous weapon systems would be both premature and insupportable.

Keywords: machine learning; artificial intelligence; cyber warfare; cyber weapons; intelligent virtual assistant

1. Machine learning as an enabler to artificial intelligence

Artificial intelligence (AI) should be considered as either a smart concept, an intelligent solution or mimicking human decision-making for a corresponding application, rather than a technical component. An AI solution could be a device (machine, computer, robot) capable of either intelligent behaviour or the simulation of human decision-making processes, that could be used to solve specific problems in an application faster and more accurately than humans. Typically, AI is designed to solve day-to-day tasks performed by humans, i.e. planning, problem solving, speaking, understanding language, recognising objects (face, image, voice), or performing social or business transactions. If the objective of these devices is to learn human behaviour and decision-making, then Machine Learning (ML) is designed such that the device learns from data, i.e. first finds patterns in the data and then learns independently how to perform a task.

This means that technologies such as ML, Natural Language Processing (NLP), Internet of Things (IoT), and High Performance Computing (HPC), combined with the era of big data, can be considered as enablers or pathways to achieve AI (making the device intelligent). ML operates by applying algorithms to data sets to discover patterns of interest. It has been applied in diverse fields including self-driving cars, speech/ image/ face recognition, fraud prevention, e-commerce recommendations, and optimisation of web searches. Machine learning basically enables the devices (machines, computers, robots, etc.) to exploit the data, such that the device will start the learning process. If the [human end user] target is to communicate and interact (written or spoken) with a device, then NLP is applied as part of the AI solution. On the industrial side, AI can be applied to

predict when maintenance is needed, or to analyse manufacturing processes for efficiency improvements. On the consumer side, AI can be used for automating requests instead of, for example, manual clicking, typing, and searching.

The fundamental key to AI is the learning processing, adaptation, and consumption of data. The contrast to both AI and ML is, for example, rule-based systems where the aim is to program the device with hand-coded routines and instructions for a specific application. In ML, the device will be trained to consume data and learn how to perform tasks. In an AI perspective, ML algorithms are designed to improve through self-learning without any human intervention. Rule-based systems could potentially be developed into an AI solution given that the routines and instructions could be updated through data and/or experiences while performing the pre-defined tasks. However, without using ML to learn the rule-based system, requires massive amounts of coding, routines, and instructions to achieve an AI solution.

While ML has been recognised as the enabler to achieve AI, the evolution of deep learning (DL) has been the main force to drive many practical applications which has been inspired by Artificial Neural Networks (ANNs). It is well-known that deep learning requires the processing of massive amount of data to enable AI solutions, which is where IoT and HPC have their value. Assuming data can be processed fast enough, DL offers advanced solutions for recognising patterns, responding to request, and supporting improve decision-making. HPC especially has been a great contributor in the move away from more traditional ML algorithms, such as decision tree learning, clustering, and Bayesian networks. In addition, the more widespread up-take of AI will drive the development technologies including ML, DL, IoT, and HPC.

2. Machine Learning in the Military & Cyber Warfare domains

The potential for ML to be applied within the military has already been recognised, with national defence science and technology laboratories across multiple countries running open competitions for ML applications. The ability of ML to extract insights from both existing and live streaming data, for the purposes of improved decision-making, offers obvious value in a battlefield environment. Nevertheless, compared to other military technologies, ML in defence is still relatively nascent, with the true cope of applications yet to be fully realised.

Current military ML competitions and applications often focus on automation processes, optimisation processes, or some combinations of the two where the speed of processes and the amount of data to be used cannot be handled by humans without considerable automation (Tyogu, 2013). For example, ML can assist in the automated scanning of satellite imagery to detect specific vehicle types thereby reducing the burden on military analysts by sifting large volumes of data. In this situation, a data analytics platform that incorporates machine learning and an interactive dashboard will provide insights that will help to identify threats in advance and can be used for planning different scenarios. Other applications include robotic for hazard scene assessment, intelligent autonomous resupply to reduce risk and burden on military personnel, and unmanned aerial vehicle (UAV) for real-time data collection, site exploration, and surveillance. These applications have especially been exploiting the era of graphics processing units (GPUs)/field programmable gate arrays (FPGAs) to parallelise computational operations to enable the device to learn at a speed, accuracy, and scale that is required. Depending on the use case these devices can be designed to work with or without the cloud but the key concept is to process, analyse, and learn fast enough to take decision in real-time. Furthermore, real-time visualisation solutions using GPUs offers high quality and resolution streamed live from the devices.

Enhanced value of ML is realised when multiple processes are combined to produce decision support systems. An example use-case is a Commanding Officer (CO) employing an Intelligent Virtual Assistant (IVA) within a fluid battlefield environment. The automation of specific underlying processes shields the CO from unnecessary distractions, while the ability of an AI/ML solution to quantify enemy intent, and compare situational data to a stored database of hundreds of previous wargame exercises and live engagements, provides the CO with access to a level of accumulated knowledge that would otherwise be impossible to accrue. Such IVAs would enable this CO to make better informed, optimised decisions at a faster rate than their opponent, and could be developed specifically for an array of situations. This point is further validated by the work from Kallberg and Cook (2017) from the Army Cyber Institute at West point, where they state “[c]yber-relevant strategies are likely to become increasingly reliant on artificial intelligence and pre-set action items, such as computational speed in execution and a situational awareness that assesses contested cyber space in real time”.

These applications are not restricted to the physical battlefield, with ML offering great potential within a cyber warfare environment, both as a defensive measure but also as an offensive tool. Given the speed of cyberattacks, the automation of defences is a rational response; indeed, this approach has been pervasively employed throughout personal, corporate and defence environments with the use of firewalls, virus detection and SCADA systems that rely on automated processes. Given this environment, AI/ML possess obvious offensive value with the automation of cyber-attacks. The ability to automate attack vectors in response to the actions of defenders provides the necessary speed of decision making for an agile digital attacker to prevail over an agile digital defender. In this regard, the potential effectiveness for offensive ML cyber warfare capabilities is enhanced by the massive amounts of data continuously being generated by ongoing cyber-attacks globally, offering rich Big Data datasets to mine for insights and as tools for iteration when learning.

Rapid changes in technology, as well as adaptive behaviour of attackers, defenders and users, are characteristic of cyberspace. Planning of military operations in cyberspace poses challenges – having more information does not equate having more knowledge (U.S. Military Academy, 2016). Many cyber intelligence planning tools are therefore of forensic nature, with intelligence being available to decision-makers after the event, not before the event. Intelligence agencies of today, have greater technical ability to gather information on a much larger scale than their predecessors, which can then be used for a variety of purposes including tactical support to military operations (Weedon, 2015).

3. Legal and ethical issues in employing AI in cyber warfare

Employing AI in warfare raises several legal and ethical questions. Notwithstanding whether we address cyber warfare or traditional warfare, these questions reflect the same core principles.

Currently, the fundamental issue that is being debated focuses on the feasibility of an overall ban of AI in warfare. The supporters of such a ban have submitted an open letter to the United Nations (UN), signed by more than 17000 individuals, urging a general ban on the offensive autonomous weapons beyond meaningful human control and disapproving a military AI arms race (Future Life Institute, 2017). Similar sentiments have been echoed by different States and other stakeholders at the series of UN Convention on Certain Conventional Weapons Group of Governmental Experts on Lethal Autonomous Weapons Systems (Biontino, 2016). One of the arguments raised on that front is that even if we agree that autonomous weapons like all weapon systems must comply with International Humanitarian Law (IHL), it is debatable whether fully autonomous weapons (without including any human judgment) would be capable of meeting IHL standards at all, while they would threaten the fundamental right to life and principle of human dignity (Human Rights Watch, 2017).

On the other hand, there are experts convinced that the development of such weapons is inevitable (World Economic Forum, 2016). Some argue that an overall ban on autonomous weapon systems would be premature, underestimate the regulatory capability of international law and generally “insupportable as a matter of law, policy, and operational good sense” (Schmitt, 2012). Rather, it is suggested that possible future regulation of AI in warfare should be guided by an international dialogue between involved stakeholders (Anderson & Waxman, 2013). Such international cooperation would help to develop a common framework for developing and using such weapons, and ensuring their legality under international law. However, it remains to be seen in what format these discussions would be held, and to which extent private sector, who is reportedly in a much more advanced position in developing automated systems (Chatham House, 2017), would be engaged in these talks.

There are numerous IHL issues which have been raised in regard to using autonomous weapons in warfare. For example, notwithstanding the weapons being used, an attack needs to distinguish between combatants and non-combatants and therefore attacks that are not directed at lawful targets are prohibited (ICRC, 1949). Also, any attack needs to be proportional, i.e. it must be ensured that incidental loss of civilian life, injury to civilians or damage to civilian objects which would be excessive of the anticipated military advantage in prohibited (ICRC, 1949). This is closely related to a number of precautions foreseen by IHL to spare the civilian population, individual civilians and civilian objects (ICRC, 1949). Also, no attack should unnecessarily aggravate the suffering of combatants (Additional Protocol to the Geneva Convention, 1977). However, it needs to be underlined that even an autonomous weapon system that is, for instance, completely incapable of

distinguishing a civilian from a combatant or a military objective from a civilian object can be lawful under certain circumstances, since not every battlefield contains civilians or civilian objectives therefore pointing at the need of a case-to-case analysis rather than an overall ban (Schmitt, 2012).

As a recurring argument, experts have concerns over the possibility of AI to fulfil the above-mentioned IHL principles without the involvement of human judgment (Biontino, 2016). Furthermore, given that there is a lack of a uniform standard to weapon reviews, the objectivity of the current domestic review systems is being doubted (Biontino, 2016). Another legal issue that has been identified is the accountability for the actions of these autonomous systems. For example, it is considered to be uncertain as to who would be held accountable within the chain of command or responsibility, such as the commander, programmer, or the operator of the system (Biontino, 2016) while Schmit (2012) argues that the responsibility for committing war crimes would fall on the individual who programmed the AI, and "the commander or civilian supervisor of that individual would be accountable for those war crimes if he or she knew or should have known that the autonomous weapon system had been so programmed and did nothing to stop its use, or later became aware that the system had been employed in a manner constituting a war crime and did nothing to hold the individuals concerned accountable".

In addition to these IHL concerns, the deployment of AI in warfare brings along a number of human rights (e.g. human dignity, the right to life, the right to physical integrity) and ethical questions. A principal ethical question seems to be whether the decision on life and death of human beings should be delegated to machines (International Review of the Red Cross, 2012). Also, a widespread use of AI in warfare may lead to an overall lowering of the threshold of going to war, therefore having an impact on global stability (International Review of the Red Cross, 2012). At the same time, we should not forget the possible benefits of AI systems such as the potential use of autonomous technologies in hazardous environments and for search and rescue operations, or precision in targeting (Biontino, 2016). Due to the lack of clarity of the future capabilities of such systems, it is fair to conclude that autonomy in weapon systems may positively promote the aims of the laws of war in some technological configurations and operational circumstances — but not in others (Anderson & Waxman, 2013).

4. Conclusion

It is clear that while there are significant opportunities to utilise machine learning within the military domain, including cyberwarfare, there is still a lack of maturity and general understanding of the scope of opportunities the technology can deliver.

Warfare operations today are conducted in complex joint and multinational environments. Innovative concepts, doctrine, and technologies are required to develop new planning and execution systems that are more flexible and agile in unknown environments. Traditional planning procedures require considerable time to evaluate a situation and generate adequate responses. Military decision-making must take into consideration the vast quantity of information from disparate sources that are typically required to perform complex tasks. At the same time, quickly developing crisis situations require fast and timely decisions. Use of artificial intelligence or intelligent decision-making aids in operations can help alleviate the challenges of planning complex operations

Undertaking applied research into this area is key to making tangible advancements. The authors proposal that running scalable test scenarios across cyber synthetic virtualised environments (i.e. cyber ranges and cyber testbeds) would aid in such developments.

Disclaimer: This contribution contains the opinion of the respective authors only, and does not reflect the policy or the opinion of any other entity or institution.

References

Adams, T.K., 2001. Future warfare and the decline of human decisionmaking. *Parameters*, *31*(4), p.57.
Anderson & Waxman, 2013, s.l.: s.n.
Biontino, 2016, s.l.: s.n.
Chatham House, 2017 s.l.: s.n.

Christian Czosseck and Kenneth Geers eds., 2009. *The Virtual Battlefield: Perspectives on Cyber Warfare* (Vol. 3). Ios Press.
Edward J, 2016. The Rise of Artificial Intelligence in Cyber Defense. www.enterpreneur.com.
Epstein, Z., 2014. How to find the Invisible Internet. *BGR*.
International Committee of the Red Cross (ICRC), 1949, August. *Geneva Convention Relative to the Protection of Civilian Persons in Time of War (Fourth Geneva Convention*, 75 UNTS 287.
Future Life Institute, 2017 s.l.: s.n.
Kallberg, J., 2016. Strategic Cyberwar Theory-A Foundation for Designing Decisive Strategic Cyber Operations.
Rios, B., 2009. Sun Tzu was a Hacker: An Examination of the Tactics and Operations from a Real World Cyber Attack. *The Virtual Battlefield: Perspectives on Cyber Warfare*, *3*, p.143.
Kallberg, J. and Cook, T.S., 2017. The Unfitness of Traditional Military Thinking in Cyber. IEEE Access.
Schmitt, M.N., 2013. *Tallinn manual on the international law applicable to cyber warfare*. Cambridge University Press.
Tyugu, E., 2011, June. Artificial intelligence in cyber defense. In *Cyber Conflict (ICCC), 2011 3rd International Conference on* (pp. 1-11). IEEE.
U.S. Military Academy, 2016. Mad Scientist Conference 2016: the 2050 Cyber Army. New York, U.S. Military Academy.
Weedon, J., Beyond Cyber War: Russia's use of Strategic Cyber Espionage and Information Operations in Ukraine. *Cyber War in Perspective: Russian Aggression Against Ukraine*, pp.67-77.