sciendo International Conference KNOWLEDGE-BASED ORGANIZATION
Vol. XXVI No 1 2020

USING WEAPONIZED MACHINE LEARNING IN CYBER OFFENSIVE OPERATIONS

Constantin NICA*, Tiberiu TĂNASE**

***European Commission, Brussels, Belgium**
****Romanian Academy of Science - CRIFST, Bucharest, Romania**
constantin.nica@gmail.com, tiberiutanase26@gmail.com

Abstract: *Using Machine Learning in cyber defensive operations has proved to be highly efficient especially for fast pattern detection. There is yet an application in using Machine Learning in cyber offensive operations in order to improve existing skill set of human operators, or enable large scale offensive operations, otherwise hard to do, without extensive manpower. Machine Learning can be a solution to the complexity of present-day world structure, it can support full autonomous work mode operations and can support asymmetric operations by being the perfect invisible enemy. Having a fully autonomous system that can launch multiple attacks in multiple domains (social, infrastructure, telecoms) simultaneously, can be valuable in a world of interconnected networks. For military operations, it's obvious that in the era of 4th generation warfare, such solutions might give an advantage over the other combatants. Furthermore, Machine Learning can become a formidable weapon if used right in the era of 5th generation conflicts, where it can target the individual itself, escalating effects to groups of people. The paper presents a generic framework in using Machine Learning in offensive cyber operations as a solution to the present-day expansion of cyber operations on foreign and national territory.*

Keywords: Weaponized Machine Learning, 4th Generation Warfare, 5th Generation Warfare, Offensive Security, Red Team

1. Introduction

Present days show that extended warfare in open theatres of operations is almost extinct, unless fighting a more superior adversary. One exception to this is the domain of cyber. Lots of theories emerge on types of warfare [1][2], but it is visible that in an unitarian world, the war of the future is that of the proxy, or inside the cyber space, where an unlimited number of operations can be executed with minimal risk of open retaliation. Surgical strikes, like the one executed recently against Qasem Soleimani [3], shows some expectation of an open conflict to be executed, even if international relations diplomats may find ways to stay various potential conflicts. 5th generation warfare, and then 6th generation warfare is starting to revolve around research that manipulate every fabric of the environment, including that of human thought, and even how time is perceived [4][5]. 6th generation warfare is a war on the individual itself, to bend perception and will, in order to win fights long before they are even started. This is done with the help of massive data gathering of information. In order to cope with the amount of information to be processed, some metadata is generated and classified in various structures: spheres [6], levels of interaction or layers [7]. The final

DOI: 10.2478/kbo-2020-0014

layer that was added, was that of the human factor itself. Manipulation of societal factors, human perception and awareness has been named cognitive warfare [8]. The cognitive warfare includes not just influence operations, but rather an entire set of tools to be employed to change political contexts of countries to the advantage of an attacker. This requires swaths of data, fast processing and specialized knowledge into labelling that data into something meaningful (data to intelligence process). The events of Cambridge Analytica [9], have shown that the capacity of automated systems into producing meaningful and high impact results, are almost limitless. One discriminator keeps appearing in all of the above presented events and evolution: machine automation. Going back to the 6th generation warfare subject, the current developments into the application of artificial intelligence in various layers of interaction, leads to a natural result of delegating human tasks to machines. US military is already using AI to analyse footage and collect data from a battlefield and help select targets to bomb [10]. Regardless of the backlash coming from the public society, the defence industry will continue its trend, like a natural evolution. 4th generation warfare has already passed, so is the 5th generation, as interoperability and black ops are now preferred action methods and are part of present-day military operations. A war gets won not by prolonging it, versus weaker adversaries, and it can't be won against adversaries that sit remotely close in terms of technology and capacity to wage it. Breaking the will of the people to support an idea is much more efficient and turns equal adversaries into a more level playing field. Bringing Machine Learning into military operations, turns the multi-domain warfare [11] into a single domain war, that is highly fluid and adaptable to outside factors in an instant. Human thinking process takes time and can risk windows of opportunity, due to indecision and lack of speed.

One conclusion can be drawn right from the start of the study, that is, machine automation speed and decisiveness is king, over single human perception.
Of course, complementing human deep perception with the speed of a machine, is even better.

2. Applications of Machine Learning in cyber offensive operations

Areas where Machine Learning can transform warfare in cyber operations are:

- Communications: overloading communication lines, interruption of communication lines, or even worse, the manipulation of a communication channel in order to provide for fake targets.
- Social, Political and Economic disruptions: disrupting any of these states, or all together, can cripple an adversary, even the most prepared ones. Returning to the case of Cambridge Analytica, it is obvious there that even a small amount of people changing their opinions can make a great difference. This can be achieved by using fake news generators, disruption of social networks using bots, disruption of local economical markets by using ML powered micro-transaction systems in order to destabilize markets;
- Social Engineering: disruption of normal day to day life via targeted events, conducted fully autonomous can speed an adversary to end a war. Here we can name elements like Influence Operations, targeted social engineering, fake news;
- Offensive automated cyber weapons. Machine Learning powered malnets, hive-nets/botnets that can attack local service infrastructure, utilities, communications, social services, card systems;
- Chain of command disruption: the usage of various methods, either by micro-targeting in any way (physical or non-physical), or by generic blanked social engineering operations powered by an AI engine in order to steal credentials, gain access to critical networks, theft of data;
- Force multipliers in open conflicts:

automated hive-nets that can launch attacks, can self-replicate, can generate automated virus payloads in order to disrupt military infrastructure, disturb military communication like GPS and other positioning systems, delivery of ammunition;

- Black-ops/wet-works improvement, by providing advanced tracking capabilities in an inter-connected work, and even delivery of payloads using drones/robots;

There is no limitation that Machine Learning can have in the cyber domain, as long as there is enough will and sufficient financial capacity to sustain research. In fact, the trend is to continuously adopt such technologies in various areas of military operations, where complex multi-domain missions are required. Granted the cyber domain is just a part of a greater strategy. One such example is the case of Russia's aggression on Ukraine, where it is shown the effect of combined arms application [12] to high effectiveness. The element of cyber before an actual boots-on-the-ground missions has had as an effect the substantial weakening of the Ukrainean defence structures, but more so, the social elements were substantially disrupted.

3. Machine Learning impact on the war

The main aspect of the current warfare methods is that of fusion warfare[13]. So, this means immense interaction capacity required between each actor participating for the goal. Due to this high interaction of elements, all being based on interoperability, availability, redundancy and constant communication flow, the element of cyber operations is constant in any part of the fusion warfare.

A good strategist may think that the application of similar methods and technologies with the purpose of achieving total disruption of any component inside the opponent's structures is something to be desired[14]. On a defender's side, not employing the same technologies would indeed be a mistake, as it would cripple a battle right from the start.

Regardless of the moral aspects of using Machine Learning and Artificial Intelligence to execute killing missions or disruptive operations which may result in the loss of life, the advantages of a decentralized infrastructure which is autonomous, that can run within some given limitations (rules of engagement, geographical, methods),is substantial. The attacker would suffer little or no human loss, the economic advantages would also be consistent as technology evolves to other states of perfection, as well as such an approach would make the subject of attribution to some specific actor, almost impossible. The most probable technology to achieve these goals are self-learning, unsupervised algorithms, that can be implemented in autonomous physical machines, or into cyber weapons.

The more violent a war is, the faster it can finish. The human factor in the end tires, gains a conscience of action, or simply runs out of resources. Maintaining pressure on any adversary, especially the prepared ones that can have similar technologies is a key to success. Machine Learning can support any strategy, in any time, weather or geographical confinement.

A Machine Learning fully autonomous system would be capable of maintaining pressure on all the elements of an adversary. Another important impact on the war, when using Machine Learning is that of enabling better counter operations. Knowing how your adversary gathers data, classifies that data and uses that data in the era of fusion warfare, allows for the manipulation of the environment of the adversary, its infrastructure and analytics structure. Machine Learning would be a perfect candidate of fast detection of intrusion attempts using digital methods, and employment of counter measures to disrupt or distract an adversary. Another aspect of the 6th generation warfare, war of the future, or what other denomination it may get is that of the "hyperwar" [15]. The

state of the world is that of a hyperwar, where all operations are fuelled by some form of automation, whether on domestic grounds or on foreign territory. Offensive operations are usually the best defence. The best defence is usually that of a constant pressure being kept on adversaries. Machine Learning is a system that can support another important aspect of the hyperwar, that of a constant conflict on any scale, in any time, unlimited by any border or opponent capacity. This is why states that have proficient militaries conduct constant Red vs Blue exercises, employ Red Team tactics, in order to test, assess and improve constantly, the response times, adaptability and discover potential weaknesses, before adversaries do.
Machine Learning supports simulations and environmental adaptability the best.

4. Use case scenario of Machine Learning application in any conflict

The best approach to explain the usage of Machine Learning into an almost automated operation (notwithstanding the obvious input of human controllers on the control end of all elements). One such scenario may be a multi-domain attack on an opposing actor, making use of various technologies like Big Data, self-learning algorithms, robotics, Influence Operations powered by mass data collection, targeted rendition of important opponent leadership and total disruption of data collection endpoints of the adversary. Some supplemental actions may include local radical group creation by supplying specific untraceable funding and support. Except the available human operations, in order to better execute the attacks and to cover for any timed gaps (humans are good, but timing is also important in order to be effective), the negative actor prepares a set of bot farms situated all across the world, ready to execute the attack at the same time. The purpose of these bot farms is primarily to flood with various attack types and overflow the defence teams and systems. Classical systems have a really hard time in determining real attacks from the ones that are there just to keep you busy. While the cyber strike gets prepared, the Artificial Intelligence engine, using the vast amounts of data available is able to identify new weaknesses in the targeted infrastructure, is able to generate targeted phishing attacks, adapted to micro-managed social profiles and is even able to generate advanced video and audio contents using text-to-speech engines, fake news, fake videos. Using local bot farms on the territory of the attacked entity, content gets to be pushed prior to the actual physical invasion. Local bot farms make traceability a time-consuming issue.
Further escalation of the scenario can result in the execution of the attack begins by first flooding information and defence channels using the bot farms, controlled by Artificial Intelligence and based on the vast amounts of collected data. So, the attack begins from multiple places, simultaneously, using various methods and even code pieces that can be attributed to diverse hacktivism groups. The cyber operations, coupled with social engineering, local actors that are being recruited for the benefit of the attacker, the speed with which this scenario gets executed and the amount of data availability, weaken the defender to such a state, that the army relies solely on old style combat, versus an attacker which is able to use all elements of the 6th generation warfare.
The kinetic operations find a territory that is almost devoid of any kind of resistance, basic operations are heavily disrupted and there is no response. The target state where the monolithic defence structure, that do not employ smart technologies, has no method of transmitting orders, can`t distribute the command to other units and can`t know the real situation in the field.
An interesting scenario would be to consider that the attacked structure really does use some basic ITC infrastructure, can have basic C3 capabilities, or even basic

C4ISR, but without the capability of decentralization. Furthermore, the population has access to digital services and can access social media, posts various content on social media, especially younger generation. The defending actors makes use of the infrastructure to interact for various services with its population. The defender uses various social media infrastructure and other tools to collect data and create its own social profiling, but it uses it for its own purposes. The attacker gets to use the actual defender infrastructure, which it got infiltrated, extracts the valuable information, then attacks said infrastructure and attempts to destabilize it, in order to reduce the trust in such structures of the local populations.

Offensive applications of Artificial Intelligence can in reality push the limits of analytics engines by flooding them with needless data, that looks real enough to warrant an analytics process. This generates the phenomenon called "dark data"[16], where there is some useful data, it gets stored, but there is not enough capacity to process it, thus crippling a defender that relies on some form of automation.

5. Conclusions

Artificial Intelligence and Machine Learning are the next leap into the permanent state of war.

Some actors may argue that building systems before a tested and proved concept may be high. The results can indeed be substantially negative if applied wrongfully. However, not making use of such technologies while potential adversaries are building similar systems and are employing such strategies can be detrimental to the "moral" thinker.

Based on the given scenario, the applications of Machine Learning may include (but not limited to):

- Autonomous war fighting capability using robots[17];
- Autonomous execution of tasks in the information sphere in order to disrupt defence capabilities;
- Autonomous execution of tasks in the area of influence operations;
- Support classical military armed operations;
- Expand an attack surface to almost limitless targets;
- Support for actions against adversaries with similar capabilities in an ever-evolving war;

Offensive applications of Artificial Intelligence in military campaigns is the embodiment of the concepts of fusion warfare or hyper war. Since the 6th generation warfare is a war on the person and what the reality is built from (disruption of social environment to the point of total societal dissolution), the human actor does require speed and decisiveness into executing operations. Artificial Intelligence and Machine Learning are giving specific opportunities to execute endless operations in time, space and targets.

Artificial Intelligence and Machine Learning can substantially increase the lethality of the conflict, but also can end a conflict well before it gets the chance to reach to an open shooting war.

Another aspect to be retained is the fact that the cyber component is just a component. So is Machine Learning. Unless they are used the right way, offensively, they will not provide a win. They can be used sometimes to send a message to adversaries and potential adversaries; they can be used as a deterrent; but they will not win wars. However, using combined arms, where Machine Learning and Artificial Intelligence augment human capacity, can indeed win wars.

References

[1] Lind, William S.; Nightengale, Keith; Schmitt, John F.; Sutton, Joseph W.; Wilson, Gary I. (October 1989), *The Changing Face of War: Into the Fourth Generation*, Marine Corps Gazette, pp. 22–26

[2] Cynthia D Ritchie, *Understanding 5th generation warfare*, Tribune (Pakistan), 6 January 2019.

[3] Cohen, Zachary; Alkhshali, Hamdi; Khadder, Kareem; Dewan, Angela (3 January 2020). *US drone strike ordered by Trump kills top Iranian commander in Baghdad*. CNN. Archived from the original on 3 January 2020. Retrieved 3 January 2020.

[4] Mary C. FitzGerald. *The Russian military's strategy for "sixth generation" warfare*. 1994. Elsevier, Orbis.

[5] Ray Alderman. *Sixth generation warfare: manipulating space and time*. http://mil-embedded.com/guest-blogs/sixth-generation-warfare-manipulating-space-and-time/

[6] Giovani Reale. A History of Ancient Philosophy II: Plato and Aristotle. SUNY Press.

[7] John Boyd. *Destruction and Creation*. http://www.goalsys.com/books/documents/ DESTRUCTION_AND_CREATION.pdf

[8] Kimberly Underwood. *Cognitive Warfare Will Be Deciding Factor in Battle*. https://www.afcea.org/content/cognitive-warfare-will-be-deciding-factor-battle

[9] Washington Post, Reuters. *Cambridge Analytica: Impact and backlash*. https://www.straitstimes.com/world/cambridge-analytica-impact-and-backlash

[10] Ben Tarnof. *Tech Workers Versus the Pentagon*. https://jacobinmag.com/2018/06/google-project-maven-military-tech-workers

[11] Shmuel Shmuel. Multi-domain Battle: *Airland battle, once more, with feeling*. https://warontherocks.com/2017/06/multi-domain-battle-airland-battle-once-more-with-feeling/

[12] Margarita Jaitner. *Russian Information Warfare: Lessons from Ukraine*. NATO CCDCOE

[13] Staff Sgt. Alyssa C. Gibson. *Fusion warfare key to C2 future*. https://www.af.mil/News/Article-Display/Article/1100441/fusion-warfare-key-to-c2-future/

[14] GLOBSEC, NATO, GLOBSEC. *NATO Adaptation Initiative: The Future Tasks of the Adapted Alliance*. https://www.globsec.org/wp-content/uploads/2017/11/GNAI-Final-Report-Nov-2017.pdf

[15] Robert K. Ackerman. *Hyperwar Is Coming Faster Than You Think*. https://www.afcea.org/content/hyperwar-coming-faster-you-think

[16] Gartner. *Dark Data.* https://www.gartner.com/en/information-technology/glossary/dark-data

[17] Derek Manky. *Rise of the Hivenet: Botnets That Think for Themselves* https://www.darkreading.com/vulnerabilities---threats/rise-of-the-hivenet-botnets-that-think-for-themselves/a/d-id/1331062