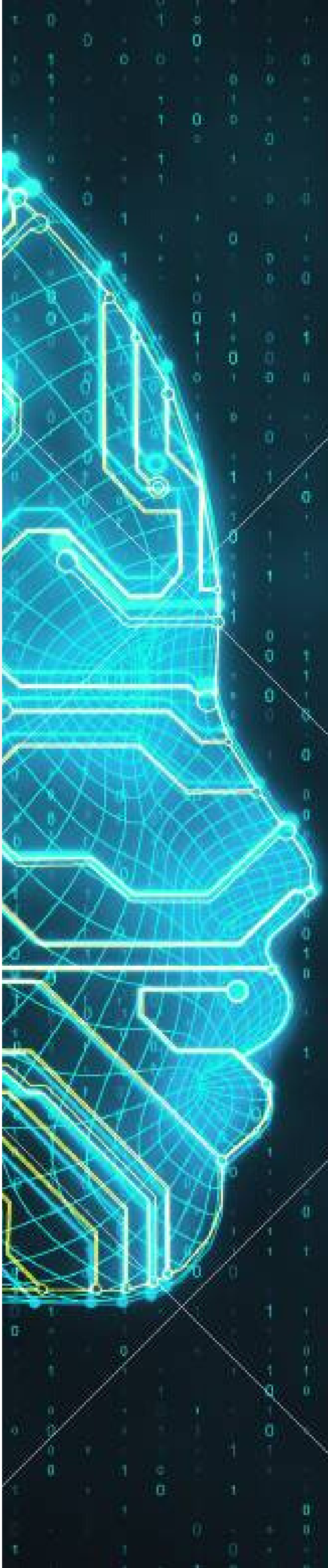
iesd
Institut d'études de stratégie et de défense
Faculté de droit
Université Jean Moulin - Lyon III



OCTOBER 2019

Artificial intelligence and defense: What is at stake?

Renaud Bellais

RESEARCH PAPER

Analyse technico-capacitaire

Image : ©Daniil Peshkov

About IESD

The **Institute of Strategic and Defense Studies (IESD)** is an academic research centre created in 2018 and specializing in strategic studies. The IESD is supported by the Université de Lyon (UdL) and belongs to the **Law School of Université Jean Moulin – Lyon III**. The institute consists of a multi-disciplinary team of researchers (Law, Political Science, Management, Economy) and unites a network of experts, researchers, PhD students and master students specialised in strategic studies.

The IESD is currently a candidate for selection as one of the Defense Ministry's (DGRIS)"National Centre of Defense Excellence" focusing on: "*Interconnection of high strategic functions (air power, space, nuclear deterrence, missile defense): political and operational implications of high intensity capability interactions in homogeneous spaces and contested commons*."

Director of IESD: **Olivier Zajec**

Collection: **Defense capabilities analysis**

Site web : https://iesd.univ-lyon3.fr/
Contact : iesd.contact@gmail.com

IESD – Faculté de droit
Université Jean Moulin – Lyon III
1C avenue des Frères Lumière – CS 78242
69372 LYON CEDEX 08

Institut d'études de stratégie et de défense
Faculté de droit
Université Jean Moulin - Lyon III

RESEARCH PAPER

Analyse technico-capacitaire

Renaud Bellais, « Artificial Intelligence and Defense: What is at Stake? », *Note de recherche IESD*, coll. « Analyse technico-capacitaire », n°1, October 2019.

Abstract

Artificial intelligence is currently a "hot topic" in defense matters. This new technology simultaneously creates fears and sets high expectations. Despite the large amount of literature written about AI and defense, it is difficult to distinguish its true impacts and estimate when they could occur. This policy paper aims to provide a comprehensive assessment, which goes beyond prejudices and misunderstandings. It underlines how AI constitutes a general-purpose technology with huge potential that could turn defense and warfare upside down. However, we must keep in mind its advantages and limits while considering its growth potential on different time scales. In addition, the military adoption of AI-based systems should not be considered a guarantee. The integration of technology is a complex process that ultimately affects how AI would change the art of war.

Résumé

L'intelligence artificielle est aujourd'hui un des sujets les plus brûlants pour la défense. Cette nouvelle technologie induit à la fois de nombreuses craintes et de très hautes attentes. Malgré une littérature foisonnante sur l'IA et la défense, il n'est pas aisé de comprendre les impacts réels de cette relation, ni même de distinguer le moment où ils pourraient produire des résultats concrets. Cette note de recherche a pour objectif d'aller au-delà des préjugés et des exagérations. Elle souligne que l'IA constitue une technologie polyvalente avec un immense potentiel qui pourrait transformer la défense et les formes de la guerre contemporaine. Il est néanmoins nécessaire de garder à l'esprit ses avantages et ses limites et de considérer son évolution potentielle sur plusieurs échelles de temps. De plus, l'adoption de systèmes d'IA au sein des armées ne devrait pas être considéré comme allant de soi. L'intégration technologique suppose des mécanismes d'adaptation relativement complexes, qui affectent la manière dont l'IA transformerait effectivement l'art de la guerre.

About the author

Renaud Bellais is an associate researcher in economics at ENSTA Bretagne and at CESICE, Université Grenoble Alpes. He graduated from Institut d'Études Politiques de Lille (1994), PhD in economics from Université du Littoral (1998) and accredited research director from Université Grenoble-Alpes (2004). After being lecturer at Université du Littoral, he worked at the French defense procurement agency (DGA) before joining EADS, now Airbus, and MBDA since 2017. He has teaching commitments in universities and military academies.

The views expressed in this article reflect solely the author's opinion.

Table of Contents

Artificial intelligence and defense: What is at stake? 5
Artificial Intelligence as a general-purpose technology 6
A multi-level “game changer” for defense? 7
Strategic dimensions 8
Operational features of AI systems 10
AI and effective autonomous systems 13
Trusting AI-based systems, a technical challenge 16
International regulations, a hindrance to AI deployment? 20
Defense innovations: the human factor 22
Conclusion 28

Artificial Intelligence and Defense: What is at Stake?

This Note aims at identifying how artificial intelligence (AI) can affect the creation of defense systems and military operations as a means to communicate between defense stakeholders. It does not look at core technical issues, but only at conceptual and operational ones. It proposes a comprehensive review of related topics, stakes and issues, and relies solely on open sources.

There are many fears and prejudices related to the use of AI in defense systems. For instance, a coalition of NGOs launched the "Campaign to Stop Killer Robots" in 2012. However, it seems very improbable that systems like Skynet[1] or Ava[2] could soon be deployed. Even though the potential implementation of advanced AI (sometimes defined as Artificial General Intelligence) into defense systems appears as a very distant possibility for technical, architectural and military reasons explored here, it is indisputable that AI has achieved major progress over the past decade. Therefore, exploring its military potential constitutes a legitimate objective.

After decades of ups and downs, the so-called "AI winters", AI has clearly made progress in recent years because three major obstacles have been overcome since the early 2010s: high-performing computational power, massive databases, and improved algorithms associated with machine learning (Cardon et al. 2018). Recent successes of AI performances has nurtured high expectations, in particular in the realm of defense capabilities where techno-centrism remains, more than ever, a core paradigm.

In February 2019, for instance, the White House and Pentagon unveiled their respective AI strategies. President Trump signed an executive order enacting the "American AI Initiative" that identifies AI as a priority for government research and development. The next day, the U.S. Department of Defense released its own AI strategy, centred on the newly created Joint Artificial Intelligence Center (JAIC). The DoD is poised to spend nearly $1 billion on artificial intelligence in Fiscal Year 2020 while DARPA has announced a multiyear $2 billion program to deliver game-changing AI solutions.

Simultaneously, AI has become a hotter and hotter topic for major arms-producing countries in Europe. Recent official statements on defense innovation, e.g. French MoD's strategic innovation policy paper[3], have increasingly brought the criticality of IA for defense matters to the forefront. Therefore, it is not surprising that AI was a major topic on the agenda of the informal meeting of EU defense ministers in August 2019. With the objective to forge new ties between the defense sector and the private tech industry in this field, these ministers met with members of the Global Tech Panel[4] consisting of tech industry leaders, investors and civil society representatives.

As the interest of the defense community is (once again) very strong for AI applications all over the world, this Note aims at understanding the nature of AI, its effectiveness and growth potential as well as its possible impacts on the way of war.

---

[1] In the series of "Terminator" movies, Skynet is an artificial neural network-based conscious group mind and artificial general intelligence.

[2] A female humanoid robot with artificial intelligence featuring in the 2014 British psychological science-fiction movie "Ex Machina", which is centered on the ability to pass Turing test (but who is testing who?).

[3] Imaginer au-delà, Document d'orientation de l'innovation de défense [Looking beyond, Defence innovation policy paper]. Paris, French Ministry of Armed Forces, July 2019.

[4] https://eeas.europa.eu/topics/global-tech-panel_en

Artificial Intelligence as a general-purpose technology

Since artificial intelligence emerged in the 1950s, innovators and researchers have filed applications for 340,000 AI-related inventions and published over 1.6 million scientific publications. The pace has significantly increased in recent years and resulted in major breakthroughs: over half of AI-related identified inventions have been published since 2013 (WIPO 2019: 13). This surge certainly reveals an in-depth transformation, in which AI could become a game-changer throughout the economic world and society. For instance, the ratio of scientific papers to inventions has decreased from 8:1 in 2010 to 3:1 in 2016. This trend indicates a shift from theoretical research to the use of AI technologies in operational products and services.

Additionally, AI is not just another new technology. Its impacts go far beyond a given product or sector. Notwithstanding its intrinsic performances, AI has the potential to transform many activities and products in depth. Kevin Kelly, the founder of Wired magazine and a renowned futurologist, clearly sums up how we need to apprehend its potential: "Like all utilities, AI will be supremely boring, even as it transforms the Internet, the global economy, and civilization. It will enliven inert objects, much as electricity did more than a century ago. Everything that we formerly electrified we will now cognitize." (Kelly 2014)

What does GPT stands for?

As the technologies in the first and second industrial revolutions allowed the creation of machines replacing human physical labour and as electricity connected the world, AI had the potential to provide capacities to replace human cognitive activities – at least for certain tasks. Scharre and Horowitz (2018: 3) notes: "The integration of AI technologies across human society could also spark a process of cognitization analogous to the changes wrought by industrialization."

In the field of defense, Wunische (2018) proposed a similar assessment of its comprehensive integration on military capabilities: "AI is not a wholly revolutionary idea to be applied to the military domain, and it is merely the next logical step in the digitization and mechanization of the modern battlefield." Such pervasiveness constitutes a very feature of AI and places it apart from many technologies. Contrary to many defense-related technologies that have characterised arms production in the past, AI is not defense-specific. It presents two specific features:

- AI is not a unified, clearly identifiable technology (like nuclear fission), but a methodology to design algorithms for various purposes, based on various knowledge components.
- AI development is not limited to defense systems (contrary to stealth), even in the short run (like semiconductors or composite materials), but is applicable to inputs from all possible sectors and could provide benefit to almost all of them.

This constitutes a major difference when considering path-breaking defense technologies, which, at least for a certain time after having emerged, were very limited to defense or high-end applications close to defense like space and high-performance computing (Bellais 1999). In fact, AI can be considered as a general-purpose technology (GPT), which is defined as being able to constitute an influential driver of long-run technological progress by representing "the invention of a method of invention" as Griliches explained in his seminal 1957 paper[5]. If AI is not fully a GPT for the time being, it is highly possible that it becomes one in the foreseeable future.

From an economic perspective, GPTs constitute core inventions that have the potential to significantly enhance productivity, performances or

[5] Griliches, Z. 1957. Hybrid Corn: An Exploration in the Economics of Technological Change. Econometrica 25(4), 501-522.

quality across a wide number of fields or sectors. For instance, the invention of the combustion motor brought about enormous technological and organizational change across sectors as diverse as manufacturing, agriculture, retail, and residential construction (which go well beyond purely technical dimensions). GPTs usually meet three criteria that distinguish them from other innovations (Cockburn et al. 2017: 5):

- They have pervasive application across many sectors;
- They spawn further innovation in application sectors;
- They themselves are rapidly improving.

Thus, if we consider AI as a GPT, we can expect that many sectors will benefit from AI applications, especially since the emergence of deep learning thanks to multi-layered neural networks.

Defense stake

On the positive side, defense can leverage on broader and massive investments from commercial and civilian stakeholders to mature this technology for nurturing its own needs. This is especially true regarding broad-spectrum AI where a defense investment would duplicate similar R&D efforts already engaged throughout the commercial world. Defense spending should rather focus on specific needs and applications, in particular at both ends of the R&D spectrum:

- At the lowest technology readiness levels (TRLs), exploratory research like DARPA's can help crack down on issues and topics for which commercial companies may have neither incentives nor interests to invest or do not possess the appropriate level of effort to deliver expected advancements in a given timeframe.
- At the highest TRLs, defense can support the adaptations of component knowledge previously funded and matured by commercial companies for specific military needs.

On the negative side, it is unlikely that arms-producing countries would be able to keep AI from proliferating across sectors and, what is more challenging, across countries. Hence, a strong concern regarding the ability of countries to invest in and master IA technology in order to keep pace with potential enemies. The US Department of Commerce insisted on such dual nature of AI through its request for comments in November 2018 regarding the emerging technologies that are essential to the US National Security. Some observers even perceive an "AI arms race" between China and the United States that goes far beyond defense topics.

In addition, AI could be considered as a GPT in the field of defense too. AI will not become a defense capability per se, but act as an enabler for developing several capabilities. AI as a GPT can also improve the systemic effectiveness of several existing capabilities as well as the whole defense architecture, notably by reducing the "fog of war" through better intelligence, coordination and information (what the Chinese call "intelligentized war") and by increasing the operational added value of assets and soldiers.

A multi-level "game changer" for defense?

The previously underlined characteristics of AI are the reason why major military powers expect that AI is likely to change the balance of power in their favour. As Stuart Russell[6] notes, "technologies have reached a point at which the deployment of such systems is — practically if not legally — feasible within years, not decades. The stakes are high: LAWS[7] have been described as the third revolution in warfare, after gunpowder and nuclear arms." (Russell 2015: 415) The main drivers for developing AI-based defense applications are strategic, operational, and budgetary dimensions.

[6] Professor of computer science, University of California, Berkeley.

[7] Lethal autonomous weapon systems.

Strategic dimensions

The United States places AI at the highest strategic priority for their defense transformation (notably since the launching of the Third Offset Strategy few years ago). Leveraging on AI aims at avoiding a level playing field with contesting military powers, since China or Russia are catching up with regard to major defense capabilities.

When he was Deputy Secretary of Defense, Bob Work regularly underlined the critical role of AI, considering it as part of both the solution and the issue. The emergence of defense AI could be identified as another "Sputnik moment" in international relations.

A year ago, Eric Schmidt[8] summarised the American assessment of AI potential: “AI has the power to affect every corner of DoD, from personnel and logistics to acquisition and multi-domain operations; and to create and sustain the asymmetric advantage required to outpace our adversaries. In the long run, AI will profoundly affect military strategy in the 21st century.”[9] Trying to maintain a significant military edge is the reason why the United States massively invests in AI.

On the opposite, China, Russia and other countries expect to overcome the obvious military superiority of the United States, in both quantitative and qualitative dimensions, by leveraging AI to bridge the gap, to “offset” or even to undermine the current military advantages of the United States (and its allies). AI is perceived as a game-changer that could turn international relations upside down, requiring a sustained defense effort from all major players, including Europeans, in this field to maintain the global stability (Bellais 2019).

The Chinese People’s Liberation Army aims at achieving an advantage in the course of the ongoing Revolution in Military Affairs. Among emerging technologies, AI appears as a critical dimension. Chinese military strategists anticipate a transformation in the form and character of warfare and conflicts, since they anticipate an evolution from today’s “informatized” (信息化) warfare to tomorrow’s “intelligentized” (智能化) warfare (Kania, 2019b). AI is particularly identified as a means to to leapfrog current American capabilities in order to invert the balance of power with the United States (Allen 2019).

Indeed, major military powers consider AI as the means to dramatically increase the potential of their existing defense capabilities. They could thus avoid entering into a technology-based arms race with the United States, which could lead them to a military and economic exhaustion (and to the fate of the USSR). Indeed, AI can improve not only the performances of individual capabilities but also, and above all, the effectiveness of armed forces thanks to systemic effects on military operations.

Operational dimensions

Military planners believe that AI and the resulting greater autonomy of systems could enable defense systems to achieve greater speed, accuracy, persistence, reach and coordination on the battlefield. For instance, former Deputy Secretary of Defense Bob Work noted: “Learning machines (…) literally will operate at the speed of light. So when you are operating against a cyber-attack or an electronic warfare attack, or attacks against your space architecture, or missiles that are coming screaming in at you at Mach 6, you're going to have a learning machine that helps you solve that problem right away.”[10]

---

[8] Former chairman of Google and Alphabet, Eric Schmidt was appointed by Secretary of Defense Ashton Carter as chairman of the DoD Innovation Advisory Board in 2016.

[9] Statement of Dr. Eric Schmidt, House Armed Services Committee, U.S. House of Representatives, April 17th, 2018, https://docs.house.gov/meetings/AS/AS00/20180417/108132/HHRG-115-AS00-Wstate-SchmidtE-20180417.pdf

[10] Deputy Secretary of Defense Bob Work’s speech at the Reagan Defense Forum: The Third Offset Strategy, Reagan Presidential Library, Simi Valley, California, November 7, 2015 (as delivered) https://www.defense.gov/Newsroom/Speeches/Speech/

AI is likely to improve intelligence by processing large batches of information through big data in order to speed up threat assessment (thus reducing the “fog of war”) and to reshuffle in-theatre resources to optimise the effectiveness of operations.

AI can help develop autonomous systems that overcome the physiological and psychological limits of human beings (stress, tiredness, low concentration, etc.). “Automation could improve safety and reliability in nuclear operations in some cases, notes Horowitz[11]. Simple and repetitive tasks where human fatigue, anger and distraction could interfere are ripe for the use of algorithms.” (Boulanin 2019: 83)

Additionally, AI can improve to some extent the interpretation of massive flows of data (imagery, sonar, signal intercepts, videos…). The quantity of images and data is well beyond the capacity of existing analyst communities (Feickert et al. 2018). This lack of resources creates huge backlogs of data, which cannot be processed in due time to provide the expected level of support to boots on the ground. Due to the inability to recruit enough analysts and to the cost of dealing with such quantities, most of collected data can never be reviewed.

Moreover, due to the heterogeneity of data streaming in from several kinds of platforms and sensors, quite often it is impossible to exploit such data directly. Often times, it must be adapted, integrated or fused to ensure accurate, comprehensive situational awareness. These operations still rely heavily on human operators, inducing delays, mistakes, labour shortages and high costs.

Nevertheless, aside from the impressive performances of AI, we should take into consideration the fact that current AI is not able to provide all cognitive tasks, which still require a human operator for the most advanced ones. AI can support operations to alleviate the burden of human beings, not fully substitute them.

Budgetary dimensions

AI can also improve the cost-effectiveness of operations and missions. Deploying AI throughout defense constitutes a means to relieve budget constraints without compromising the level of ambition.

In addition, AI can level the playing field even more for contesting powers, since they can expect to achieve a balance of power despite lower military expenditures. Per se, this impact represents a true game-changer, since countries leveraging on AI would no longer need to engage an arms race in a budgetary perspective.

This is particularly useful for countries like China or Russia, which cannot invest as much as the Pentagon for their defense. Rather than dramatically increasing their military spending, they can leverage AI to magnify their defense resources. For instance, it can be less expensive to develop an AI-based anti-access/area-denial air defense than trying to develop an aircraft that can match the performances of F22s and F35s (that is, falling into the “Top Gun” syndrome).

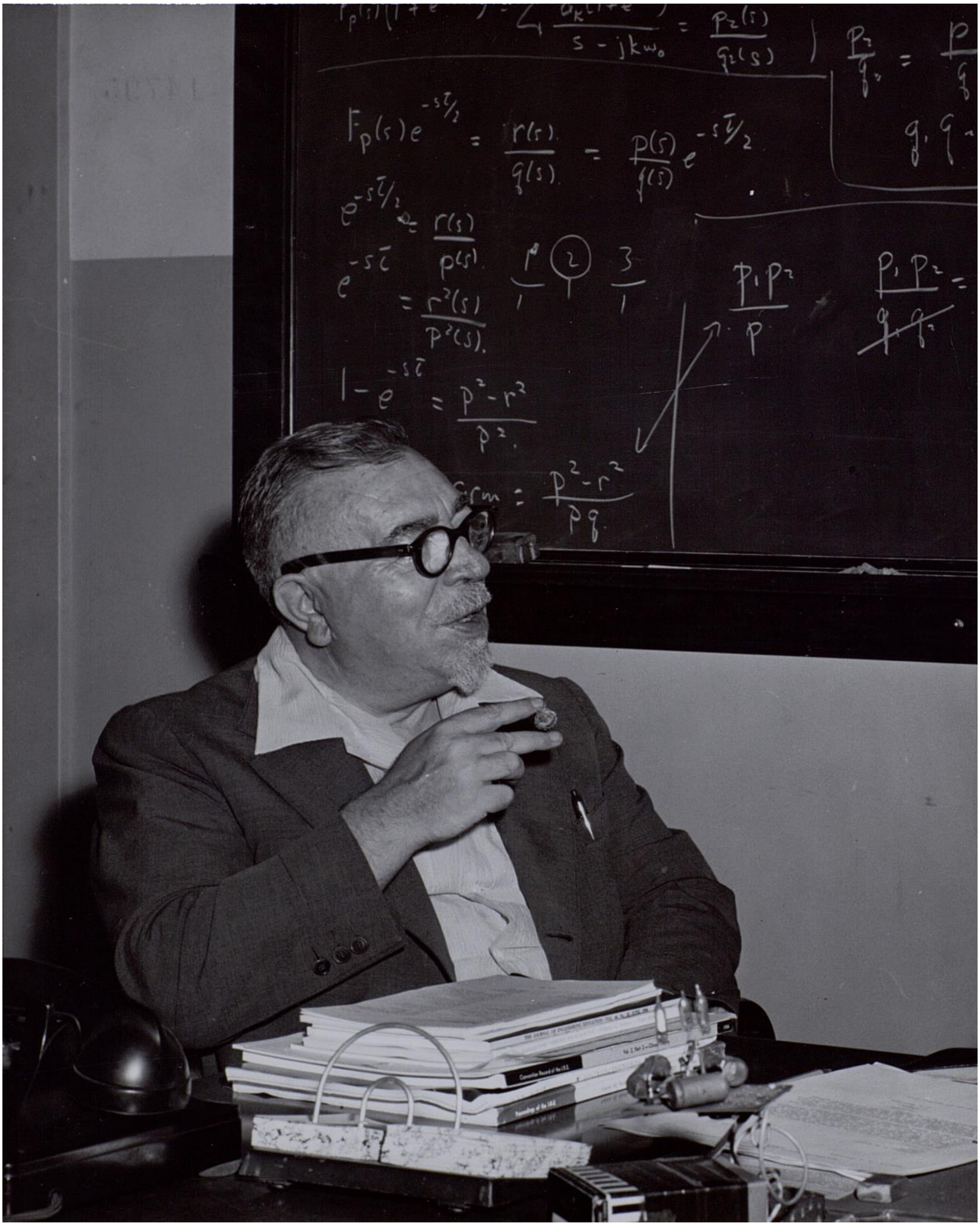
Autonomous and automated systems are believed to provide opportunities for reducing the operating costs of weapon systems and the need for soldiers, in particular by decreasing the ratio of deployed soldiers per square kilometre. Thanks to man-machine teaming, AI can favour a more efficient use of work force and reduce the likeliness of casualties. It could help armed forces cover larger areas with a limited number of soldiers and platforms.

AI is likely to improve the interoperability between soldiers and manned systems, on one side, and unmanned systems, on the other. In the medium and, more certainly, long run, man-machine teaming will help concentrate soldiers on missions that human beings can best achieve.

Article/628246/reagan-defense-forum-the-third-offset-strategy/

[11] Horowitz, M. Artificial intelligence and nuclear stability. In: Boulanin (ed. 2019), 79-83.

Norbert Wiener (1894-1964)



Founding father of the field of cybernetics, a field of research at the root of issues related to Artificial Intelligence
Norbert Wiener. F. 26/11 1894 d. 18/3 1964.

Operational features of AI systems

There is a biased understanding about what AI systems can and cannot do. We must depart from phantasms as well as prejudices that prevent many people from really understanding what we can expect from AI. Its performances must be assessed with regard to the complexity of tasks and the heterogeneity of the environment in which operations take place.

Up to now, most AI systems are specialised, meaning they are dedicated to one or several tasks that have been clearly defined ex ante. They perform very well at specific tasks in a given, homogeneous environment. These specialised AI systems must be distinguished from artificial general intelligence (AGI). AGI would constitute the ground for fully autonomous systems but it does not exist in operational features today (and could never become a reality).

Specialised AI

Given the state of the art, specialised AI (also referred to as "weak AI") is the only kind of operational AI technology today. Specialised AI can be defined as Perception AI, which is based on a probabilistic, quasi-mechanical approach. A system with specialised AI can manage complex decisions based on reasoning and previously analysed sets of data, but it needs to be trained and pre-programmed for specific applications.

In "The Organization of Behavior" (1949), Donald Hebb suggested that learning specifically involves strengthening certain patterns of neural activity by increasing the probability (weight) of induced neuron firing between the associated connections.

If task-oriented AI systems can deliver impressive results, these latter depend heavily on the quality of data and the homogeneity of the environment. Biased or even solely too heterogeneous data can mislead the AI processing. Unexpected or impure environments can create edge effects that dramatically diminish the effectiveness of otherwise performant AI systems.

Such systems cannot be considered as comparable to the human brain, since they have no capability to "think" beyond the scope of their programming. Marsh (2019) puts into relief that our understanding of AI is marred and there are too many anthropomorphic representations that mislead people on the true abilities of such algorithms. AI systems do not "learn" in a human sense. "Intelligence measures a system's ability to determine the best course of action to achieve its goals in a wide range of environments." (Scharre and Horowitz 2018: 4)

The human brain continuously triages information, that is, "natural data" from its ever-changing, noisy and unpredictable surroundings in real time, without any assistance. The current AI is far from presenting such ability, since it can only evolve within a predefined representation of the world (Cardon et al. 2018).

Rather, as John Borrie[12] underlines, AI systems are conceived in order to recursively improve their ability to successfully complete pattern recognition or matching tasks based on sets of data (which usually need to be carefully curated by human beings first). Such AI applications deal with issues when they are manageable through a tree-structure analysis (response function). In other words, specialised AI succeeds when it is subjected to a vectorised world. According to Yann LeCun's own wording, the ambition of the designers of connectionist machines consists in "placing the world into a vector (world2vec)" (Cardon et al. 2018).

Today, specialised AI appears very optimal for carrying on a given task in a given context. Nevertheless, its effectiveness requires a structured environment, homogeneous data, cooperative context… many criteria that are hardly met in most military operations. AI systems need to

[12] Borrie, J. Cold war lessons for automation in nuclear weapon systems. In: Boulanin (ed. 2019), 41-52.

be more adaptive to operate safely and reliably in complex, dynamic and adversarial environments so as to become fully supportive to military operations. New validation and verification procedures must be developed for systems that are adaptive or capable of learning.

Artificial general intelligence

In the AI community, the concept of artificial general intelligence (AGI) (or "strong AI") refers to a general-purpose AI that would be as smart as, or even smarter than, human beings. An AGI-based system would be able to understand the world itself through a comprehensive representation, not defined ex ante but created by the AI itself. Thus, it could develop its own meaning for the environment it encounters and the ways to achieve its objectives (by opposition to delimited tasks). What defines AGI is learning and reasoning abilities across multiple domains with broad autonomy (Kuncic 2019).

AGI represents the theoretical objective to achieve an effective and efficient symbolic AI, which relies on a truly cognitive approach coming closer to the core features of human intelligence. In 1957, Allen Newell and Herbert Simon summed up the top-down approach in what they called "the physical symbol system hypothesis". This hypothesis states that processing structures of symbols is sufficient, in principle, to produce artificial intelligence in a digital computer and that, moreover, human intelligence is the result of the same type of symbolic manipulations.

If such ambitious (and still theoretical) objectives can be achieved, AGI would overcome the identified limits of Perception AI, especially for systems operating in complex, heterogeneous and changing environments – which characterises the essence of military missions and operations.

However, for the time being, AGI remains in the realm of science fiction or of theoretical possibility. Even though it was the ideal of the first-wave AI designers, this approach encountered many theoretical, technical and operational stalemates and resulted in what is often called an "AI winter". AI research was able to escape from this by abandoning these ambitious objectives and by exploring non-linear solutions through what some researchers[13] called the "deep learning conspiracy" (Cardon et al. 2018).

A real substitute to human intelligence does not exist today and we are far away from it. We do not know if this is even possible, especially if the objective consists in creating a "conscious system". As the neurosurgeon Henry Marsh explains, the complexity of the brain resides in the way in which the nerve cells are connected. "Nerve cells are not, in fact, simple electrical switches (…) Neuronal networks are dynamic, they are constantly changing. They weaken or strengthen in accordance with how much traffic is passing through them (…) Furthermore, neurons come in a wide variety of shapes and sizes (…) Neural networks only resemble brain networks in a very loose way." (Marsh 2019: 1-2)

Machine intelligence

The Oxford mathematician Marcus du Sautoy takes a different perspective. He argues that AI can compete with human intelligence as long as we consider that being creative consists of "super-smart synthesis" rather than the flash of inspiration or genius. Indeed, much of creativity takes place in a continuum because it is exploratory, combinatorial and transformational (even though this latter can be erratic and thus unpredictable through AI).

While this approach does lead to an AI system comparable to human brain, his perspective holds out the prospect for very advanced AI technology. It is important to take into consideration the intrinsic limits of AI. Bob Works prefers to qualify these algorithms as "machine intelligence" rather than artificial intelligence, which can be a misleading terminology. This is the reason why synthetic

[13] Yann LeCun, Yoshua Bengio and Geoffrey Hinton (Nature 521, 436-444, May 28th, 2015).

intelligence represents a possible alternative approach to trying to improve deep learning technics.

As Kuncic (2019) notes: "Decision-making is a distinguishing point of difference between AI and synthetic intelligence. Because AI is algorithm-based, decisions are made in a deterministic way based on hard-wired sequential instructions. This is crucial for reliable number-crunching computation. In contrast, decisions made by synthetic intelligence are less predictable, reflecting the non-digital nature of the underlying network. For this reason, synthetic intelligence could never replace AI. Indeed, even the human brain is incapable of replicating AI-driven computation. But what synthetic intelligence could deliver is machines whose responses to unpredictable environmental cues are both reason-based and flexible — like humans".

One should keep in mind that AI research considers that hybridisation between both Connectionist and Symbolic AIs could deliver the most promising approach for developing advanced operational solutions. As Andrew Ng noted, "we still have a long way to go in the field. For example, a toddler can usually recognize a cat after just one encounter, but a computer still needs more than one example to learn. We need to find ways to train computers on training datasets as small as 100, or even 10 […] Effective 'unsupervised learning' – learning without labelled data – remains a holy grail of AI." (WIPO 2019: 8). AI potential remains important but developing it is an uneasy way and we should remain aware of its possible limits.

AI and effective autonomous systems

AI is intrinsically linked to autonomous systems, nurturing prejudices and phantasms. However, when considering the current maturity of AI and its foreseeable evolutions, what can be delivered is far from what science-fiction describes in movies like "Terminator" or "Screamers"[14].

Autonomy can be defined as the ability of a machine to execute a task, or tasks, without human input, using interactions of computer programming with its environment. Once activated, an autonomous system is expected to perform some tasks or functions on its own. Even though AI can help increase the autonomy of defense systems, technology is currently insufficient to achieve fully autonomous systems.

Levels of autonomy

Paul Scharre[15] divides degrees of autonomy into three categories:

- The human-machine C2 relationship;
- The sophistication of the system's decision-making process;
- The types of decisions or functions being made autonomous.

AI systems that require human interaction at some stage to execute a task can be referred to as semi-autonomous. This can be associated to automatic tasks, e.g. mobility (homing, following, navigation, take-off and landing), intelligence, interoperability or health management. Such dimension reflects the development of autonomy for specific functions of weapon systems, which are delegated to an AI application to relieve the human operator, rather than the development of autonomous systems as a whole.

AI systems that can operate independently but under the oversight of a human being, who can intervene if something goes wrong (e.g. malfunction or system failure) or who keeps the ultimate control over the delivery of force, correspond to automated tasks.

Automatic and automated tasks can discharge human beings from operating specific dimensions

[14] "Screamers" is a 1995 dystopian science-fiction movie, based on Philip K. Dick's 1953 short story "Second Variety", where humans face AI-based, self-evolving robots.

[15] Center for a New American Security.

of the system and let them focus their cognitive abilities on more essential or appropriate tasks.

Systems that operate completely on their own and where humans are not in a position to intervene during a mission are considered as fully autonomous. Here, AI helps to carry on a mission rather than a task.

The place of human operators

This classification regarding the degree of autonomy shows that the level of implication of human beings in the implementation of tasks or the functioning of systems can vary. A standard classification of human interaction and supervision is defined by three categories:

Human-in-the-loop systems can select and deliver action or force only with a human command.

Human-on-the-loop systems can select and deliver action or force under the oversight of a human operator, who can override the system's actions.

Human-out-of-the-loop systems are capable of selecting targets and delivering force without any human input or interaction.

Even though a fully autonomous system may be possible, such conception is not necessarily compatible with the military doctrine and how armed forces want to operate. The concept of "sliding autonomy" is sometimes used to refer to systems able to switch back and forth between automated and autonomous functioning, depending on the complexity of the mission, external operating environments and legal/regulatory frames.

From this classification, it appears that some functions in defense systems can become autonomous without presenting significant ethical, legal, operational or strategic risks (e.g. navigation or countering foes' defense systems), while others raise greater concerns and question international regulation (e.g. targeting, objective management or determination). One difficulty regarding weapon systems can result from the fact that different levels of autonomy are likely to be implemented in the same capability, at least with regard to the first two levels.

Stratus Augmentet Reality Interface for soldier MBDA

On-board vs off-board AI systems?

While the Chinese speak about "algorithm wars", one major challenge is to combine AI software and dedicated hardware to improve its effectiveness. This software-hardware combination appears essential to deliver the highest performances of AI. Thus, one question pops up: Where should the hardware layer be placed? Embedded into a deployed capability or at a node inside the defense architecture? This question is far from trivial but it is neglected most of the time.

Embedded AI

The embeddedness of AI raises the question of related hardware. Indeed, processing capacities are essential to deliver expected performances from AI applications. This is the reason why China tries to develop its domestic microprocessor industrial base, and why the United States wants to restrict the export of AI-specialised chips. The criticality of this dimension is well understood by Chinese decision-makers, since the focus of its national AI strategy now includes the build-up of a comprehensive domestic semiconductor industry (Allen 2019: 16-20).

On-board AI capacities lead to challenges in terms of design, energy, system architecture... and significant costs, even though operational benefits can represent a game-changer. The design of the actuators and end-effectors will affect the hardiness, endurance and cost of the systems. This option can favour more autonomous systems, being able to pursue their missions despite weakened or disrupted communications.

Due to the required computing capacities and the network-based effectiveness, there is no obvious solution where to position AI capabilities in the military architecture. If the NGOs fear the emergence of "Terminator-like" systems, this would require embedding sophisticated AI capacities inside a given platform. Nevertheless, this approach would need very advanced AI systems that do not exist today and that are quite complex to design.

Network-based AI

An alternative solution consists in developing off-board AI applications. A network-based AI supporting distributed capabilities can deliver higher effectiveness and eventually efficiency, since it creates the opportunity to gather the critical mass of resources (processing power, comprehensive capacities, data gathering and fusion, etc.) with reduced constraints in terms of space or energy for a given capability. In this perspective, the Chinese expect to benefit greatly from quantum computing to exploit the potential of networked AI and to achieve higher speed and accuracy in managing military operations.

A network-based AI approach could also reduce the risks that biased data could trick a given platform, due to limited access data or the lack of cross-checking databases, in order to prevent any kind of misinterpretation. Such more powerful AI solutions are nevertheless highly dependent on resilient, dense and secured communication networks to deliver its output to in-theatre systems. Any network-based AI requires relying on advanced cryptography and cybersecurity (the more complex and interconnected systems become, the more vulnerabilities they present to cyberattacks) as well as high performing communication architecture.

These different features question the conception of defense systems and organisation with regard to desired outcomes. One can expect that an effective approach would consist in combining embedded and network-based layers of AI. In addition, an effective use of AI requires accessing a strong telecommunications infrastructure in order to be able to manage huge flows of data. This is the reason why the mastering of 5G capacities has become a strategic issue. 5G networks are likely to constitute a critical resource for achieving the full potential of defense-related AI.

One reason why distributed AI could prevail over on-board Ai results from the huge quantity of energy that AI needs. As Julia (2019) remarks, DeepMind consumes more than 440,000 watts per hour to play go game when a human brain only needs 20 watts per hour. Even though one can expect to develop less energy-intensive microprocessors than today's GPUs[16], remote capacities linked to deployed platforms could achieve a good balance between the self-governance of deployed capabilities and several technical constraints (unit cost, size, stealth, embedded energy, etc.).

Resilient defense architecture

One major stake consists in increasing the resilience of AI systems against adversarial capabilities, in particular when these latter are based on AI too.

Chinese strategists have fully understood that this is a key feature for future capabilities. For instance, Li Minghai (researcher at PLA's National Defense University) underlines that China expects to achieve military superiority by switching from systems confrontation to algorithms competition. This approach requires achieving superiority in algorithms: "In future warfare, the force that enjoys algorithm superiority will be able to rapidly and accurately predict the development of the battlefield situation, thus coming up with the best combat-fighting methods and achieving the war objective of 'prevailing before battle starts'." (Gertz 2019)

Freedberg (2019) describes a new emerging field known as "adversarial AI". The objective consists in training AI to confront adversarial forces through dynamic virtual battle experiments. For instance, generative adversarial networks place two machine-learning systems together in a virtual cage, each pushing the other to evolve more sophisticated algorithms over thousands of rounds. Generative adversarial networks aim at confronting one side to fake data that the other system constantly generates so that it can learn to detect counterfeits. What ensues is a kind of Darwinian contest, a survival of the fittest in which duelling AIs replicate millions of years of evolution on fast forward.

Such virtual tournaments allow identifying weaknesses and optimising against them. This constitutes the only way to keep pace with potential enemies in the AI arms race. For instance, Chinese researchers Shen Shoulin and Zhang Guoning clearly explain that China wants to acquire capacities to "take the cognitive initiative and damage or interfere with the cognition of the enemy based on the speed and quality of the cognitive confrontation" (Eastwood 2019).

The emergence of adversarial AI could favour a combination of different layers of AI both on board and off board to increase the resilience of capabilities and the whole defense architecture.

Trusting AI-based systems, a technical challenge

AI-based systems are elaborated around a theoretical view of the world that is often a simplification of physical reality in terms of mathematical models[17]. An autonomous system always has a model of its universe, or design space, which mathematically describes the system's relationship to its environment. This latter relies on the interpretation of signals from its sensors. Therefore, a system is intended to act effectively and efficiently only within its design space. It is likely that its behaviour outside of the initially defined design space becomes unpredictable, since the system has no description of his environment to which it can refer and on which it relies.

This is the reason why AI differs from human intelligence, and such a conceptual approach leads to two main issues. First, the mathematical model relies on estimated parameters, which may vary with time, be insufficiently precise or provide incomplete information, notably because the operational domain is only partially observable. Second, AI is very likely to access incomplete information. Thus, autonomous systems face difficulty to deal with real-life environments.

[16] Graphics processing units.

[17] The mathematical model is a description of the interaction between the system and its universe.

Issues of mathematical modelling

As Dimitri Scheftelowitsch[18] explains, "even given perfect observation, perfect situation awareness, perfect modelling and perfect computational decision-making capabilities, the actions of an autonomous system are defined by its goal statement." (Boulanin 2019: 29) The effective functioning of a given AI system requires that such a goal can be identified and formulated in machine-readable terms.

These issues linked to the mathematical modelling and implementation of AI are even more problematic regarding defense capabilities because of specific dimensions:

It is difficult to perfectly model all possible environments in which a given capability could be deployed (no pre-recorded data) and to predict their evolutions once the battle has started (difficult to perform real-life measurements).

Adversaries are likely to introduce biases in AI analysis by providing erroneous data in order to trick its algorithm (even if the environment was a priori predictable).

They will try to disrupt communications so as to prevent the system to confirm its own assessment by implementing a benchmark with other friendly defense systems.

Goals are hard to define ex ante and are likely to change in the course of operations because of interactions with (friendly and adversarial) platforms inside the theatre and because of the dynamics of battle.

Learning and black boxes

Thus, using AI for autonomous systems leads to promote self-learning that has become possible thanks to neural networks and deep learning, which contributed to greatly improved performances of AI over recent years. However, these systems tend to operate as black boxes.

While the algorithm is known for such AI systems, the process through which inputs result in an outcome is not necessarily observable or explainable on mathematical grounds. As Vincent Boulanin[19] notes: "The lack of transparency and explainability of these systems in turn creates a fundamental problem of predictability. A machine learning system might fail in ways that were unthinkable to humans because the engineers do not have a full understanding of its inner working. In the context of weapon systems (…) it makes complex the task of identifying the source of a problem and attributing responsibility when something goes wrong." (Boulanin 2019: 20)

This feature leads to many questions regarding how much trust we can have on such AI applications and how predictable their behaviour can be.

This limit of today's AI applications led DARPA to launch dedicated programmes that allow the extensive use of AI applications for defense needs: Trustworthy AI and Explainable AI. In April 2019, the independent high-level expert group on AI set up by the European Commission published a report entitled "Ethics guidelines of Trustworthy AI" as a starting point for the discussion.

Explainability and observability

If one considers that the AI systems for autonomous cars face major challenges in terms of validation and verification, it appears even tougher for defense capacities. Autonomous cars would travel within a quite predictable space (thanks to 3D mapping) and with "engagement rules" that could be modelled up to a certain point. This is not that easy when dealing with defense capabilities. In addition, armed forces have very high standards for validation and verification procedures, since safety

[18] Scheftelowitsch, D. The state of artificial intelligence: An engineer's perspective on autonomous systems. In: Boulanin (ed. 2019), 26-31.

[19] Boulanin, V. Artificial intelligence: A primer. In: Boulanin (ed. 2019), 13-25.

and reliability cannot fail when soldiers are actually fighting.

Specialised AI is very effective to manage a given task. It can analyse through a probabilistic approach, implementing routines. However, their behaviour cannot be fully understood, since results sometimes rely on parameters differing from what a human being would use, usually uncovered once the AI application delivers unexpected – revealing ex post the limits of the system's trustworthiness.

The learning curve of an AI system is contingent to a given environment with quite homogeneous parameters. As Boulanin and Verbruggen (2017: 15) note: "A computer's lack of contextual understanding derives from the fact that it remains very complex for engineers to represent in a model the abstract relationship between objects and people in the real world."

If the environment in which an AI system is deployed diverges from these ex ante criteria, its effectiveness and thus trustworthiness are bound to decrease rapidly. We can fear that enemy forces will try to trick or defeat it through erroneous data, inducing biases in the system's assessment, understanding and/or behaviour. These potential limits of current specialised AI systems would reduce significantly their benefit for armed forces.

Additionally, when a learning process is involved, one can wonder if it is necessary to freeze its evolution once it enters into service. Indeed, unless a system's learning process is stopped when being deployed, it is difficult to predict how it would behave as it might learn or do things beyond what we can expect from it.

Thus, the validity of such systems is based on the guarantee that it does what we expect from him, only what we expect, and all we expect.

Validation and verification

Nevertheless, observability should be distinguished from predictability and explicability. In a true black box, the algorithm is not observable. If it is observable, we can explain its functioning (on a mathematical basis). In fact, one can consider two different process:

- Formal verification is achieved at the mathematical level, which is meant to cover all cases.
- Testing is carried on at empirical level, which involve only a limited number of representative cases.

One should keep in mind that empiricism is the ground for a large share of science. The ability to reproduce a process is key, and it is different from a mathematical demonstration. This perspective could open an alternative approach to validate some systems, but it requires reaching the critical mass of experimentations. Is it achievable in the field of defense?

Verification and validation process is a methodological issue, since there are not yet well-established methods to verify and test machine-learning systems. Even though deep learning can lead to a black box, patterns are not explainable per se but parameters are known. So one can consider that a verifiability is possible, notably thanks to a sufficient number of experimentations (still to be defined). This leads to define the appropriate process to experiment enough a system so as being able to trust it. However, this remains a very difficult research issue up to now.

While commercial industries can expect to implement such verification and validation process (based on huge volume, acceptability of failure, low risk environment…), it appears more complex to do so in the field of defense, ceteris paribus. In defense, there is a limited recurrence of implementation (limited fleets, low rotation rate, limited deployments, etc.) and, the acceptable rate of failure is much lower for any kind of capability (hence higher costs for comparable civilian systems).

In a longer perspective, technological advancement could provide AI technology able to explain by itself the process and resulting decisions it delivers. Such self-assessment would constitute an alternative approach to observability. However, this seems to represent a long-run prospect today.

AI systems must also be able to identify fake or erroneous information that aim at generating dysfunctional behaviours. This requires adaptive systems, which is far from the case today. This is the reason why in 2018 DARPA launched a $2bn investment programme called "AI-Next" in order to reach a new level of advanced artificial intelligence. This programme expects to develop more adaptive reasoning and, hopefully, an ability of algorithms to determine subjective phenomena, recently explained Valerie Browning, director of DARPA's Defense Sciences Office in an interview with Nextgov[20].

C2 – Command and Control - USA

©-Inez Lawson

[20] Corrigan, J. 2019. Inside DARPA's Ambitious 'AI Next' Program. March 10th. https://www.defenseone.com/technology/2019/03/inside-pentagons-big-plans-develop-trustworthy-artificial-intelligence/155427/

International regulations, a hindrance to AI deployment?

Ongoing discussions on regulating autonomous systems result from increasing normative pressures from civil society against the conception, production or use of autonomous weapon systems. We should keep in mind that the quest for international regulation regarding AI and autonomous systems does not come out of nowhere. Since the Geneva Conventions in 1949, an international law has emerged and been consolidated to supervise the features and use of weapons.

In particular, Article 36 of the 1977 Additional Protocol I to the Geneva Conventions requires States to conduct a legal review of all new weapons, means and methods of warfare in order to determine whether their employment is prohibited by international law.

On-going discussions on how to regulate LAWS

Since 2014, the governance of lethal autonomous weapon systems (LAWS) has been discussed internationally under the framework of the 1980 United Nations Convention on Certain Conventional Weapons (CCW), which regulates weapons that may be deemed to have an excessively injurious or indiscriminate effect. Representatives from about 80 countries have been meeting on lethal autonomous weapons systems.

In 2017, these meetings were upgraded from informal "Meetings of Experts" to a formal Group of Government Experts (GGE). The GGE invites experts from civil society to partake in the deliberations alongside members of national delegations.

Despite several years of debates, the GGE has not succeeded in producing any specific policy recommendation yet. A consensus has emerged on two points: appropriate levels of human control must be maintained over any LAWS; and LAWS must remain subject to International Humanitarian Law (IHL). However, "the mechanics of applying both terms remain contentious (e.g., does IHL categorically ban LAWS?), and the limited scope of agreement provides no basis for further action" (Liu and Moodie 2019: 1).

By November 2019, they have to decide how they will continue to discuss the issue:

Keeping a group of governmental experts (GGE) with a similar exploratory mandate;

Entering into negotiations on a new treaty to regulate killer robots;

Discontinuing discussions.

This intergovernmental process resulted at least partially from the "Campaign to Stop Killer Robots", which aims at achieving a U.N. treaty banning the development, production and use of fully autonomous lethal weapons. This coalition of NGOs tries to lobby the ongoing international negotiations, to influence national policies and to raise awareness of public opinion. They use tactics that had succeeded in achieving international treaties to ban land mines and cluster munitions (for the records, outside the United Nations framework).

Implementing International Humanitarian Law

IHL already includes a number of obligations that restrict the use of autonomous targeting capabilities. It also requires military command to maintain, in most circumstances, some form of human control or oversight over the weapon system's behaviour. This requirement is implicit, hence the call of NGOs for a new legal instrument. IHL puts limits on how attack may be conducted through the principles of distinction, proportionality and precaution.

AI appears sensitive when it could be used to manage lethal tasks, notably identification, tracking, prioritization, selection of targets and, possibly, target engagement. Autonomous targeting may be lawful in some specific circumstances, e.g. against distinct material military targets, in an unpopulated, remote and predicable environment or in good weather conditions.

Even though these tasks are somehow lawful in a segregate space and uncluttered background, it appears crystal clear that most of engagements do not meet these criteria. Target identification can be difficult and theatres are messier and messier, with a high probability to misidentify real targets.

AI-based systems can implement certain rules and principles of international law. They may distinguish between targets, if clearly identified as military ones, but they cannot act in a proportionate way. Even when such implementation is possible, this occurs only in a very crude manner for the time being. Fiott and Lindstrom (2018: 7) notes: "Should AI-systems eventually act beyond the intended boundaries set by humans, the issue of accountability would emerge and conflict situations might deteriorate even further as a result."

Even before authorising or banning LAWS, the key stake consists in defining a lethal autonomous weapon system. Up to now, there are several and competing definitions (Boulanin and Verbruggen 2017, Liu and Moodie 2019). For instance, Vatican looks at "a weapon system able to identify, select and fire on a target without human intervention" (close to automated systems). Alternatively, France proposes a more restricted perimeter through three criteria: full autonomy, no human supervision at all, and ability to self-adapt to the environment, to target and to fire with lethal effect (focusing on truly autonomous ones).

Depending on the selected definition, the score of IHL and eventually a possible ban can vary significantly. This is the reason why it is important to be involved in ongoing discussions to avoid unwanted restrictions or bans that could include much more than solely autonomous defense systems.

Ethics and companies' involvement

As AI technologies advance, some academics and private companies might choose to "opt out" of working with DOD on AI applications that they might view as opposite to their own values (Feickert et al. 2018; Sayler 2019). This was already the case when several employees petitioned Google to exit DOD's Project Maven in May 2018. Actually, this decision was coherent with Google's decision to cancel existing government contracts for two robotics companies it had acquired—Boston Dynamics and Schaft—and prohibited future government work for DeepMind, an AI software start-up that Google acquired.

Nevertheless, not all companies share this approach. Simultaneously to Google's decision, several companies have pledged to continue supporting DOD initiatives. Amazon CEO Jeff Bezos even underlined that "if big tech companies are going to turn their back on the U.S. Department of Defense, this country is going to be in trouble", defending government contracts amid a wave of employee protests – adding ""We are going to continue to support the DOD and I think we should." (Tiku 2018)

In addition, while armed forces expect that ethics will prevail (e.g., as defined through Weinbaum's grounds for an AI code of conduct), one cannot exclude that, facing a possible defeat and overwhelmed by despair, some armed forces could be tempted to choose rogue behaviours. History provides many examples, especially since the late 19th century, where emerging technologies have served military purposes even if banning such use was already banned, e.g. machine guns, submarines and chemical weapons.

The prohibition of militarising technology at national or international level is not sufficient to ultimately prevent armed forces from using it. As Wunische (2018) underlines, "the single determinant of its use, or non-use, on the battlefield is the result of something much more straightforward—states will use it if it's effective on the battlefield."

In addition, even though armed forces sometimes resist new technologies, this positioning usually only postpones their adoption in the medium and long rum. As Price (1995: 73) observed, "Throughout history, numerous weapons have provoked cries of moral protest upon their introduction as novel technologies of warfare. However, as examples such as the longbow, crossbow, firearms, explosive shells, and submarines demonstrate, the dominant pattern has been for such moral qualms to disappear over time as these innovations became incorporated into the standard techniques of war."

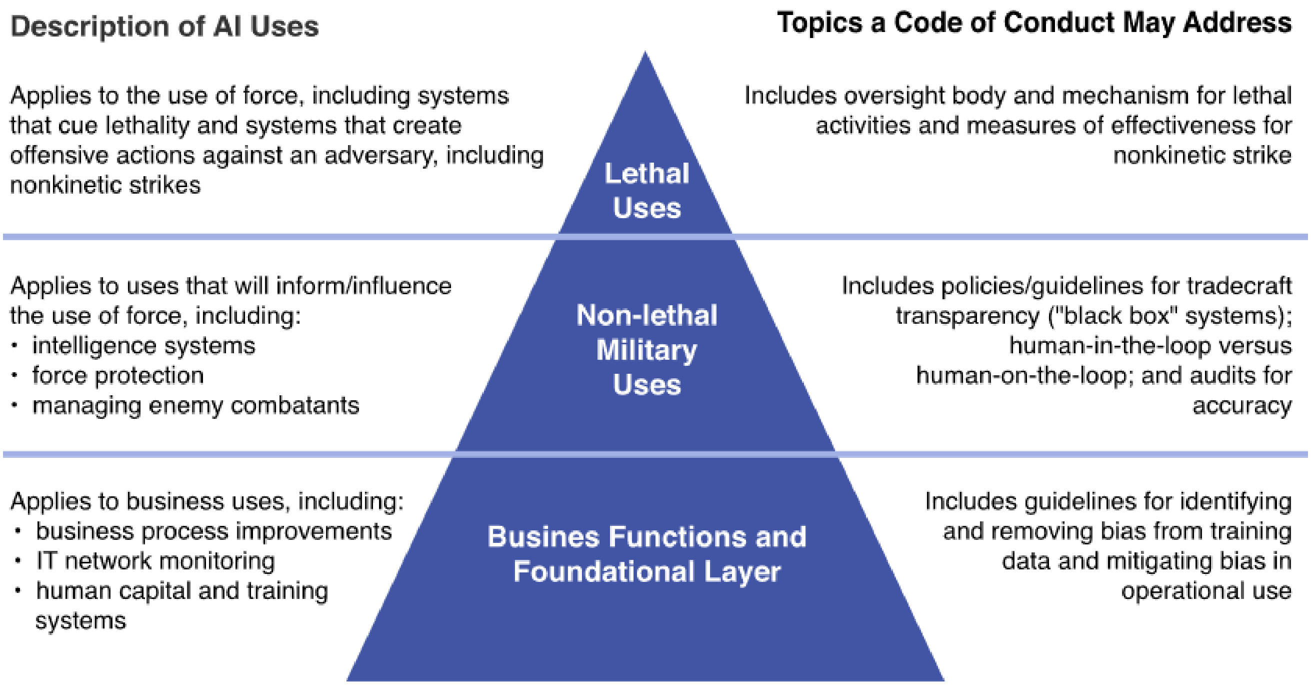
Defense innovations: the human factor

Historian Joel Mokyr's works[21] provides at least one major lesson: nothing should be taken for granted when considering the adoption of innovations that have the potential to radically transform defense. His analysis sounds a cautionary note. Ever since the dawn of the first Industrial Revolution three centuries ago, both the pessimists and optimists concerning innovation and technology have almost been proven wrong in a long-run perspective.

In fact, the adoption and diffusion of innovation do not rely only on technical dimensions (the maturity of a given technology and the availability of complementary ones if one considers the technical system strictly speaking). Most of the time, technical issues and difficulties can be overcome, to some extent at least and through appropriate efforts[22].

However, the technical feasibility of a technology or its improving performances does not necessarily lead to its desirability and spreading since political, economic, operational, sociological and ethical factors come into play, either stimulating the adoption or hindering it. As Oh et al. (2019) remark: "History is replete with examples of militaries that possessed certain technologies but failed to incorporate them organizationally to succeed in battle."

Grounds for an AI Code of Conduct for the Pentagon



Source: Weinbaum, C. 2019. Here's What an AI Code of Conduct for the Pentagon Might Look Like. June 21st.

---

[21] For instance, Mokyr, J., Vickers, C., Ziebarth, N. 2015. The History of Technological Anxiety and the Future of Economic Growth: Is This Time Different? Journal of Economic Perspectives. 29(3), 31-50.

[22] The history of missile systems in Germany from the inter-war period to the end of World War II provides a good illustration of such ability to get over challenges in terms of both science and experimentations. See, for instance, Michael J. Neufeld's The Rocket and the Reich: Peenemunde and the Coming of the Ballistic Missile Era (Smithsonian Books, 2013).

No doctrine, no capability

No new system can have military value as long as armed forces have not conceived a corresponding doctrine to understand its military value and the ways they would integrate such a system inside missions and operations. A given system should be understandable for military uses and acceptable with regard to how military forces want to carry on their duties and missions.

None of the previously mentioned technical and conceptual problems is unsolvable per se in the long run. However, as Dimitri Scheftelowitsch[23] explains, they require a deep understanding of the application domain and the mathematical foundations of current solution methods, their capabilities and limitations, and an integration of domain and technical knowledge into military doctrine. In fact, this ultimate dimension appears much more critical to the deployment of AI into defense capabilities than technical issues. The design of an appropriate doctrine is a sine-qua-non condition to give a specific technology its full military potential.

The use of AI in military operations is logical if and only if armed forces are able to understand what added value it can provide and how military operations need to be reshuffled so as AI can deliver its full benefits. Such process can only take place if armed forces accept to integrate AI and develop a sound doctrine to go along with new capabilities. Military history demonstrates that such a process is far from being granted. What is technical feasible does not automatically determine what will be accepted or developed. There is no teleological process creating an automatic runoff from technology to defense.

Even when a doctrine is available, institutional resistance can also persist, notably when soldiers consider that new capabilities are incompatible with the operational paradigm they are used to. Up to now, it appears that armed forces often lack trust in the safety and reliability of autonomous systems. Moreover, some servicemen understand the development of certain autonomous capabilities as a direct threat to their role, status, positioning or professional ethics.

Compatibility with military ethos

As Bob Work underlined: “A general AI system sets its own goals and can change them. No one in the Department of Defense is saying we ought to go toward those type of weapons.” Even Project Maven, against which Google employees petitioned their company to remove itself from the project for ethical reasons, focuses on merging human and machine intelligence in a way that improves human decision-making. It does not aim at substituting a machine decision for a human one.

Resistance results, for a large part, from a lack of trust in substituting AI-based solution to existing tools, since decision-makers fear downgrading the effectiveness their current defense capabilities. For instance, Deputy Director for CIA technology development, Dawn Meyerriecks expressed concern about the willingness of senior political and military leaders to accept AI-generated analysis, arguing that the defense establishment’s risk-averse culture may pose greater challenges to future competitiveness than the pace of adversary technology development (Sayler 2019: 18).

In its AI Strategy Review for 2018, the US Department of Defense only mentions AI in weapon systems in relation to keeping humans in the loop for any kind of lethal engagement. This report emphasises many other applications where AI would provide benefit to the operational environment such as “improving situational awareness and decision-making, increasing the safety of operating equipment, implementing predictive maintenance and supply, and streamlining business processes.”

---

[23] Scheftelowitsch, D. The state of artificial intelligence: An engineer’s perspective on autonomous systems. In: Boulanin (ed. 2019), 26-31.

While being one of the fiercest proponents of AI operational deployment, Bob Work underlined: "We are not talking about Skynets and we're not talking about Terminators (…) We're looking for narrow AI systems that can compose courses of action to accomplish the tasks that the machine is given and it can choose among the courses of action." (Boyd 2018) AI should complement and not be a substitute to human fighters. This is the reason why he talks about machine intelligence and algorithmic warfare rather than artificial intelligence. Bob Works even added: "A general AI system sets its own goals and can change them. No one in the Department of Defense is saying we ought to go toward those type of weapons." (op. cit.)

The EU's positioning is quite similar. The partial agreement for a Regulation establishing a European Defense Fund purports that the EDF shall not finance activities that involve the development of lethal autonomous weapons without the possibility for meaningful human control over the selection and engagement decisions when carrying out strikes against humans. Thus, discussions around the development of AI technologies for integration in weapons systems will affect directly the future regulatory framework for AI and defense technologies within the EU.

Fiott and Lindstrom (2018: 3) provide a comprehensive assessment of armed forces' position when they note that AI "can easily be seen as a stand-alone capability or technology when in reality it should be regarded as a strategic enabler. It is therefore more accurate to speak of AI-enabled cyber-defense, AI-supported supply chain management or AI-ready unmanned and robotic systems."

AI and autonomous systems are currently seen as a means to make human beings more powerful, not to substitute to them – even in the Chinese perspective. Bob Work underlined that "When people hear me talk about this [autonomy], they immediately start to think of Skynet and Terminator, I think more in terms of Iron Man […] A machine to assist a human, where a human is still in control in all matters, but the machine makes the human much more powerful and more capable." He also added: "We're looking for narrow AI systems that can compose courses of action to accomplish the tasks that the machine is given and it can choose among the courses of action."[24]

Man-machine teaming at stake

Maintaining a safe and meaningful interaction between soldiers and AI-based systems appears increasingly challenging as the level of system autonomy increases. Trust is essential to avoid jeopardising the life of soldiers deployed simultaneously with AI-based systems. Additionally, the differential in data management between IA systems and human beings can lead to mismatch in terms of decisions. As Boulanin and Verbruggen (2017: 67) underline, "The more autonomous a process is, the harder it is for human operators to react to a problem correctly and in a timely manner."

This constitutes a challenge for hybrid deployment of forces. This nevertheless requires a good man-machine teaming. This latter constitutes an ancient issue in computer science, and a fundamental dimension to succeed in implementing AI into any kind of system.

According to Sayler (2019: 30-31), human-machine interaction issues that may be challenged by insufficient explainability in a military context include three dimensions:

Goal Alignment. Human beings and autonomous systems must have a common understanding of the objective. As they encounter an evolving environment, goals are bound to change. Thus, human beings and systems must adjust simultaneously and they must base such adjustment on a shared picture of their environment.

[24] Quoted by Freedberg (2016).

Task Alignment. Both must understand the boundaries of each other's decision space, especially when goals change.

Human-Machine Interface. Due to the requirement for timely decisions in many military AI applications, traditional machine interfaces may slow down performances, but real-time human-machine coordination is essential to build trust.

As long as man-machine teaming issues are not solved, one can expect only a limited embeddedness of AI applications into defense capacities. This issue is far more complex than one expect. Indeed, even in a segregated space like an industrial plant, the development of cobotics ("collaborative robots") raises many difficulties to have human operators and machines operating closely.

These issues reach another level when dealing with defense capabilities that are deployed in moving, heterogeneous and hostile environments… Many uncertainties exist today regarding the fact that AI-based capabilities can work in harmony with soldiers. If this is not the case, one can consider that AI would become a source of trouble and reduce the effectiveness of military operations or even result in casualties among the friendly forces.

The effectiveness of military operations appears as the ultimate criterion when deciding which capabilities can fulfil operational requirements. Since alternative solutions exist and as long as their benefit equals or exceeds the performances and reliability of AI-based systems, it is likely that armed forces favour the conservative approach in terms of capabilities (Bellais 1999).

Reshuffling the organisation of armed forces

The integration of AI into defense capabilities is likely to modify the organisation of armed forces. Ryan (2018: 20) provides an illustration of such transformative impact: "a highly capable and sustainable land combat battlegroup in 2030 may consist of as few as 250–300 human soldiers and several thousand robotic systems of various sizes and functions. By the same token, many functions of artillery and combat engineer units, currently undertaken by humans, might be better done by robots in human-robot teams. This has the potential to reduce the size of these types of units by hundreds of combat arms personnel. This approach could free up personnel for redeployment into areas where the art of war demands leadership and creativity-enabling intelligence functions; training and education; planning; and, most importantly, command and leadership."

One should consider that relying heavily on AI-based systems also constitutes a challenge for the organisation of armed forces. Indeed, if capabilities can manage autonomously their tasks and missions, then there is no use for soldiers and, even more, officers in the loop. However, the institutional evolution of armed forces is fundamentally based on the chain of command.

In his *Principles of War*, General Foch noted that "in an army, there are only subordinate units"[25]. Such hierarchical organisation remains at the heart of armed forces today. As Caplain (2019: 11) explains: "From political decision to the implementation order up to the last soldier, armed forces rely on an operational command structure which role consists in conceiving, implementing and eventually conducting military manoeuver." Since the 18th century, the chain of command is the quintessential dimension of military organisations with staffs and the "modèle divisionnaire", inspired by Guibert and fully implemented by Napoleon.

This does not mean that decentralised, autonomous operations did not exist. There are several instances of these latter – especially in the German armed forces during World War I and II (e.g. Stoßtruppen). However, even though they can deliver good outcomes in the short run, loosely

[25] Ferdinand Foch. 1911. Des principes de la guerre. Paris: Berger-Levrault, 3rd edition, 93.

coordinated operations are unlikely to deliver the best outcomes in the long run, and thus fulfil political decision-markers' expectations.

Indeed, the hierarchical organisation of armed forces results also from the need to articulate three levels of operations: tactical, operative and strategic. Sometimes, a decision can appear irrelevant at the tactical level, but it provides a high added value at the operative one, which cannot be identified as such from a very local perspective. The ultimate outcome does not result from the juxtaposition of effects delivered by each unit locally but from the merger of all outcomes through a comprehensive approach on a global perspective. If boots on the ground can face difficulties to appreciate the reasons why they implement some actions, the ability to achieve apparently irrational operations based on beyond-the-line-of sight information can only be inaccessible to AI systems.

Therefore, the more autonomous decisions (unmanned or manned) are at the tactical level, the more fragile and loose the articulation between these three levels of war can be. The very military concept of "command and control" speaks by itself when we try to catch the core organisational principles of armed forces: understand, conceive, and command…

New mind-sets, structures, and processes

Despite the digitalisation of armed forces, command structure has not lessened but, on the contrary, been reinforced through the RMA. This is due to the ability to access information in near-real time for most situations; in addition, this information loop gives political decision-makers the possibility to prevent soldiers on the ground from engaging actions with side effects and political hazards (e.g. civilian casualties). While soldiers and officers have access to much more information, paradoxically they have a lower margin of manoeuvre to make decisions at their own level due to this control obsession.

Therefore, digitalisation tends to increase the importance of the chain of command rather to favour a more decentralised management of operations. This trend seems contradictory to the deployment of more autonomous systems even though AI would give them such ability. Artificial intelligence can help manage the complexity of military operations, but it is improbable that it could replace the hierarchical organisation of armed forces, especially at staff levels.

As Caplain (2019: 79-80) notes, AI can play a decisive role in future command structures, notably in order to gather and exploit huge volumes of information through decision-making tools. If some observers are already speaking about another revolution in military affairs, we should be cautious and consider the potential resistance of existing structures to changes, especially when they turn existing sources and structures of power upside down. "Changing any military's doctrine," pointed out by Toffler and Toffler (1993: 62), "is like trying to stop a tank armour by throwing marshmallows at it. The military, like any huge bureaucracy, resists innovation – especially if the change implies the downgrading of certain units and the need to learn new skills and to transcend service rivalries."

As Oh et al. (2019) underline, "military institutions have a deserved reputation for, at best, only a half-hearted embrace of disruptive technologies. To beat historical precedent, the joint force must take appropriate best practices from all sources, whether from inside or outside of government, to alter organizational mindsets, structures, and processes to better incorporate AI." Their point of view is even more interesting since authors of this paper are all U.S. military officers and graduates of the U.S. Army War College resident class of 2019.

Perhaps the biggest challenge for any company as well as the armed forces in incorporating AI is its organisational culture. "A company's culture can resist disruptive technology, especially if it threatens core models and processes that are engrained in the company's identity. The workforce may view these models as sacrosanct because they have led to successes in the past." (Oh et al. 2019) Initiatives that impact core business models take longer to fully incorporate (if it even succeeds) since they meet the strongest cultural resistance inside organisations.

Such resistance from military structures to game-changing innovations goes beyond the

United States. In China, Xi Jinping placed the military intelligentization and the integration of AI into defense capabilities as a top priority in the political agenda. Additionally, China concentrates important efforts of AI-related R&D. However, a military deployment of AI solutions is likely to take some time:

"The inclusion of discussion of competition in artificial intelligence in this authoritative textbook reflects a further formalization of the PLA's strategic thinking on the importance of military intelligentization (…) However, these concepts must enter the PLA's 'operational regulations' in order to act as a basis for future military operations and training, and the PLA's process of transforming concepts into doctrine requires a more formal process of evaluation and authoritative assessment, including on the basis of ideological considerations. In this regard, it would be premature to say that the PLA has a formal doctrine or framework of firm policies established for questions of autonomy and artificial intelligence." (Kania 2019b: 7)

The transformative impacts of AI require to changes in-depth the logics of national defense to deliver its full military potential. In China, these transformations could be impeded by the fact that the People's Liberation Army is a Party army, not a nation's one. Xi Jinping has consistently reiterated that the PLA must adhere to the Party's "absolute leadership" to ensure its complete obedience. The imperatives of capability and controllability could constraint and condition the Chinese approach to AI in the field of defense. The Chinese situation illustrates by its extreme features the decisive impact of non-technical factors in the possible integration of AI-based capabilities into armed forces.

A slower integration than expected?

Indeed, an AI-centric evolution of defense capacities and capabilities would put the organisation of armed forces upside down. Due to the role of officers in armed forces, a sociological resistance can limit the deployment of AI-based autonomous systems in quantitative and qualitative terms. More decentralised operations of armed forces could provide benefits (e.g. in the short run and very thick "fog of war"), but history proves the added value of operative and strategic levels, for which the role of officers and the chain of command is of upmost importance.

Therefore, a slow implementation of IA onto defense capabilities is likely to result from:

- A lack of trust among soldiers in unproven technology (learning curve)
- A priority given to proven solutions over theoretically superior ones (risk mitigation)
- The shortfall of added value from these solutions
- The inertia of organisational setup that prevents from optimising the use of new capabilities
- Inappropriate doctrines to give military/operational meaning to these capabilities
- High switching costs (depreciating existing assets, training of soldiers, creating appropriate infrastructure, support and maintenance…)
- The slow adoption by (potentially) competing countries

In addition, History proves that, in absence of conflict or rapidly intensifying tensions, the introduction and adoption of military innovations can be slow compared to the relative maturity of related technologies (e.g. radars, aircraft carriers or missile systems in the interwar period[26] or the key systems of Andrew Marshall's "revolution in military affairs").

We should keep in mind that, in many countries and even in the United States, armed forces and the

[26] See, for instance, Military Innovation in the Interwar Period. Edited by Williamson Murray and Allan R. Millett. Cambridge, Cambridge University Press, 1996.

MoD have been more comfortable investing in AI for back-office initiatives rather than capabilities that truly affect how wars are fought. Regarding the United States, Oh et al. (2019) state: "Current AI pilot projects have focused on peripheral areas like preventive maintenance and humanitarian assistance. The military has not yet invested in areas where AI can impact core warfighting functions like command and control. Such initiatives will likely challenge many cultural norms such as the role of the commander in decision making or appropriate levels of automation."

Armed forces are quite conservative when deciding what kinds of capabilities to deploy due to both hysteresis effect, institutional latency and mistrust vis-à-vis disruptions. This is the reason why we can expect that the deployment of AI-based systems could be slower than expected, but with punctuated diffusion rather than unpredictable tipping points, resulting in a non-linear adoption requiring a sustained monitoring. In addition, these dynamics of diffusion can gear up in case of emergency, for instance because of increased international tensions (in order to change the level-playing field) or of a new arms race (with AI as a general-purpose technology for defense capabilities).

Conclusion

Many expectations and fears result from the new wave of AI developments that have been occurring over the past decade. Even though AI solutions appear more and more capable, this Note underlines the technical and non-technical parameters that could promote or hinder the integration of AI solutions into defense capabilities.

One should keep in mind that, while keeping human beings in the loop or on the loop constitutes the favoured option of armed forces, the fate of ongoing battles could push some belligerents to ultimately rely on autonomous, AI capabilities as Paul Scharre[27] underlines. Decision-makers would then be confronted to Faustian dilemmas related to the costs of victory, the fate of battles, and the ways and means to win.

Relying too much on AI would prevent human decision-makers from stopping damaging or destructive engagements. This requires a thorough analysis of possible consequences in the medium and long run as well as a systemic understanding of resulting interactions, especially on the architecture of defense. For instance, it is important to avoid any automaticity of decisions that could put capabilities out of control like in the 1983 movie “War Games” though domino effects or misunderstandings.

The adoption of AI solutions should be based on a global cost-benefit assessment in terms of national defense and of the ability to keep war under control. As Scharre and Horowitz (2018: 14) underline: “In national security settings, unintended interactions could occur by AI systems trying to gain a competitive advantage on one another and taking actions that could be destructive or counterproductive. In settings where machines interact at superhuman speeds, such as in cyberspace or electronic warfare, these interactions could lead to harmful consequences before human users can adequately respond.”

[27] Scharre, P. 2018. Army of none: Autonomous weapons and the future of war. New York: W.W. Norton & Company.

Bibliography

Allen, G.C. 2019. *Understanding China's AI strategy: Clues to Chinese strategic thinking on artificial intelligence and national security*. Washington, DC: Center for a New American Security, February.

Bellais, R. 1999. *Production d'armes et puissance des nations*. Paris: L'Harmattan.

Bellais, R. 2019*. Le rôle indispensable de l'Union européenne comme acteur de la stabilité internationale. Défense nationale*, 821, June, 30-36.

Bendett, S. 2018. *Here's How the Russian Military Is Organizing to Develop AI*. July 20th. https://www.defenseone.com/ideas/2018/07/russian-militarys-ai-development-roadmap/149900/

Boulanin, V. ed. 2019. *The impact of artificial intelligence on strategic stability and nuclear risk. Volume 1: Euro-Atlantic perspectives*. Solna: SIPRI.

Boulanin, V., Verbruggen, M. 2017. *Mapping the development of autonomy in weapon systems*. Solna: SIPRI.

Boyd, A. 2018. *Pentagon Doesn't Want Real Artificial Intelligence In War, Former Official Says*. Nextgov, October 30th. https://www.nextgov.com/emerging-tech/2018/10/pentagon-doesnt-want-real-artificial-intelligence-war-former-official-says/152418/

Caplain, S. 2019. *La fourmilière du général. Le commandement opérationnel face aux enjeux de haute intensité*. Focus stratégique 89, Paris: Institut Français des Relations Internationales, June.

Cardon, D., Cointet, J.P., Mazières, A. 2018. *La revanche des neurones: L'invention des machines inductives et la controverse de l'intelligence artificielle*. Réseaux 211, 2018/5, 173-220.

Cockburn, I., Henderson, R., Stern, S.. 2017. *The Impact of Artificial Intelligence on Innovation: An Exploratory Analysis*. Paper prepared for the NBER Conference on Research Issues in Artificial Intelligence, Toronto, September.

Copeland; B.J. 2019. *Artificial intelligence*. Encyclopaedia Britannica, April 11th. https://www.britannica.com/technology/artificial-intelligence (viewed on April 17th, 2019).

Corrigan, J. 2019. *Inside DARPA's Ambitious 'AI Next' Program*. NextGov, March 10th. https://www.defenseone.com/technology/2019/03/inside-pentagons-big-plans-develop-trustworthy-artificial-intelligence/155427/

DoD. 2019. *Summary of the 2018 Department of Defense Artificial Intelligence Strategy*. Washington, DC: U.S. Department of Defense.

du Sautoy, M. 2019. *The Creativity Code: How AI is learning to write, paint and think*. London: Fourth Estate.

Eastwood, B. 2019. *A smarter battlefield? PLA concepts for "intelligent operations" begin to take shape*. Washington, DC: The Jamestown Foundation, February 15th. https://jamestown.org/program/a-smarter-battlefield-pla-concepts-for-intelligent-operations-begin-to-take-shape

Feickert, A., Kapp, L., Elsea, J. Harris, L. 2018. *U.S. Ground Forces Robotics and Autonomous Systems (RAS) and Artificial Intelligence (AI): Considerations for Congress*. Washington, DC: Congressional Research Service, November 1st. https://crsreports.congress.gov/product/pdf/R/R45392

Fiott, D., Lindstrom, G. 2018. *Artificial Intelligence, What implications for EU security and defense?*. Brief Issue No. 10/2018. Paris: European Union Institute for Security Studies, November.

Freedberg, S. 2016. *Iron Man, not Terminator: the Pentagon's sci-fi inspirations*. Breaking Defense, May 3rd. https://breakingdefense.com/2016/05/iron-man-not-terminator-the-pentagons-sci-fi-inspirations/

Freedberg, S. 2019. *Attacking Artificial Intelligence: How To Trick The Enemy*. Breaking Defense, February 6th. https://breakingdefense.com/2019/02/attacking-artificial-intelligence-how-to-trick-the-enemy/

Gassilloud, T., Becht, O. 2018. *Gagner la guerre numérique, nouvel enjeu de souveraineté*. Information report No. 996. Paris: National Assembly.

Gertz, B. 2019. *China developing battlefield AI for high-technology warfare*. Washington Times, January 30th. https://m.washingtontimes.com/news/2019/jan/30/chinas-military-outlines-artificial-intelligence-p/

Glass, P. 2019. *Here's the Key Innovation in DARPA AI Project: Ethics From the Start*. Defense One ,March 15th. https://www.defenseone.com/technology/2019/03/heres-key-innovation-darpas-ai-project-ethics-start/155589/

Gorriez, F. 2017. *Vers une interdiction des systèmes d'armes létaux autonomes ?*. Cahiers de la pensée Mili-Terre 47, June 30th.

Kania, E. 2019a. *Learning Without Fighting: New Developments in PLA Artificial Intelligence War-Gaming*. China Brief 19(7), Washington, DC: The Jamestown Foundation; April 9th, 15-19.

Kania, E. 2019b. *Chinese Military Innovation in Artificial Intelligence*. Testimony before the U.S.-China Economic and Security Review Commission Hearing on Trade, Technology, and Military-Civil Fusion, Washington, DC: Center for a New American Security, June 7th. https://s3.amazonaws.com/files.cnas.org/documents/June-7-Hearing_Panel-1_Elsa-Kania_Chinese-Military-Innovation-in-Artificial-Intelligence.pdf?mtime=20190617115242

Kelly, K. 2014. *The Three Breakthroughs That Have Finally Unleashed AI on the World*. Wired, October 27th. https://www.wired.com/2014/10/future-of-artificial-intelligence/

Kuncic, Z. 2019. *In search of smarter machines*. Financial Times, August 3rd/4th, page FTWeekend 18.

Liu, Z., Moodie, M. 2019. *International Discussions Concerning Lethal Autonomous Weapon Systems*. Washington, DC: Congressional Research Service, August 16th. https://fas.org/sgp/crs/weapons/IF11294.pdf

Mallat, S. 2018. *Inaugural lecture on the data sciences chair*. Paris: Collège de France, January 11th.

Marsh, H. 2019. *Can we ever build a mind?* Financial Times, 12 January, pages FTWeekend 1-2.

Oh, P., Spahr, T., Chase, C., Abadie, A. 2019. *Incorporating artificial intelligence: Lessons from the private sector*. 19 June. https://warroom.armywarcollege.edu/articles/incorporating-artificial-intelligence-private-sector/ (consulted on 21 June 2019).

Petersson, H. Wood, A. 2019. *Possible political and legal consequences of the ethical debate on Artificial Intelligence*. Scoping Paper. Brussels: ASD. April.

Price, R. 1995. *A Genealogy of the Chemical Weapons Taboo*. International Organization 49(1), 73-103.

Russell, S. 2015. *Take a stand on AI weapons*. Nature 521(7553), 28 May, 415-416.

Ryan, M. 2018. *Human-Machine Teaming for Future Ground Forces*. Washington, DC: Center for Strategic and Budgetary Assessments.

Sayler, K. 2019. *Artificial Intelligence and National Security*. Washington, DC: Congressional Research Service, 30 January. https://crsreports.congress.gov/product/pdf/R/R45178.

Scharre, P. 2015. *The opportunity and challenge of autonomous systems*. In: A. Williams and P. Scharre (eds.). Autonomous Systems: Issues for Defense Policymakers. Norfolk: NATO.

Scharre, P. Horowitz, M. 2018. *Artificial intelligence: What Every Policymaker Needs to Know*. Whasington, DC: Center for a New American Security, June.

Schmidt, E. 2018. *Statement before the House Armed Services Committee*. Washington: U.S. House of Representatives, April 17th. https://es.ndu.edu/Portals/75/Documents/HHRG-115-AS00-Wstate-SchmidtE-20180417.pdf

Sherman, J. 2019. *Don't Call It an 'Arms Race': US-China AI Competition Is Not Winner-Takes-All*, March 7th. https://www.defenseone.com/ideas/2019/03/dont-call-it-arms-race-us-china-ai-competition-not-winner-takes-all/155378/

Tiku, N. 2018. *Amazon's Jeff Bezos Says Tech Companies Should Work with the Pentagon*. Wired, October 15th. https://www.wired.com/story/amazons-jeff-bezos-says-tech-companies-should-work-with-the-pentagon/

Toffler, A.; Toffler, H. 1993. *War and anti-war: Survival at the dawn of the 21st century*, Boston: Little, Brown and Company.

Villani C. 2018*. Donner un sens à l'intelligence artificielle, Pour une stratégie nationale et européenne.* Report to the French Prime Minister, Paris, March.

Wang, H., Dotson J. 2019*. The "Algorithm Game" and Its Implications for Chinese War Control.* China Brief 19(7), Washington, DC: The Jamestown Foundation, 19-24.

WIPO. 2019. *WIPO Technology Trends 2019: Artificial Intelligence*. Geneva: World Intellectual Property Organization.

Work, B. 2015. *Deputy Secretary of Defense Bob Work's speech at the Reagan Defense Forum: The Third Offset Strategy*. Reagan Presidential Library, Simi Valley, California, November 7th (as delivered) https://www.defense.gov/Newsroom/Speeches/Speech/Article/628246/reagan-defense-forum-the-third-offset-strategy/

Wunische, A. 2018. *AI Weapons Are Here to Stay*. The National Interest, August 7th. https://nationalinterest.org/feature/ai-weapons-are-here-stay-27862

Contact : iesd.contact@gmail.com

Site : https://iesd.univ-lyon3.fr/

IESD - Faculté de droit
Université Jean Moulin - Lyon III
1C avenue des Frères Lumière - CS 78242
69372 LYON CEDEX 08