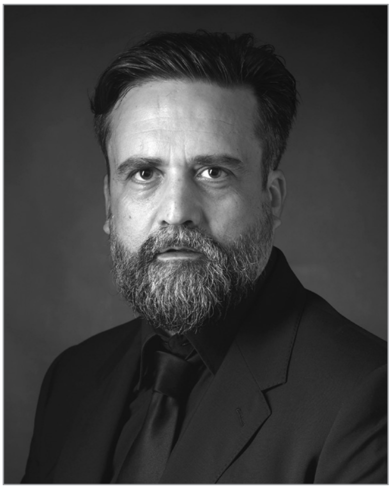
Artificial Intelligence in Digital Warfare: Introducing the Concept of the Cyberteammate

Rudy Guyonneau
Arnaud Le Dez

THE SAME OLD HUMANS IN A BRAND-NEW, DIGITALIZED WORLD

Technology changes our world at such a rapid pace that our natural, human intelligence has a hard time coping with its brutally disruptive evolution. The transformations of digital technologies have made deep and lasting impacts on our societies. Information, which is at the heart of the last century's technological developments, has become such an essential resource that it is now a component of power. Information exchanges have sped up and intensified, which has resulted in a loss of culture as societies have become more uniform. Cyberspace, which appeared in the blink of a geologic eye, has become a favored way to communicate because of its ease, accessibility, and global range.

Despite advances in technology, humans remain the same at their core. Cyberspace has become a confrontational place where ideas and wills oppose themselves. Alternate "truths" have found a way to express themselves unrestingly there, thus producing discord. Unlike the dream of the generation that created it, cyberspace is not a world of peace and of universal harmony. Because this new, digital world can also carry the expression of an adversarial will, it thereby becomes mandatory to manifest oneself there, in order to fight it. From now on, one must be in capacity to take action in cyberspace, to act upon information if not on the means to process it. And sometimes, to impose one's will, one must move towards war. While an actual war has yet to occur, the military is already engaged in digital warfare. At first, cyberfighters acted independently, but are now integrated into the combat forms of the land, sea, air, and space domains. It is the cyberfighter's duty to support and augment physical battles in those domains. Cyberfighters, in contrast to their military brethren, can sustain a form of permanent conflict against non-state political entities without ever having to declare war. Digital warfare is indeed a long-haul fight, with the objective of weakening adversaries in cyberspace to win an advantage in military, economic, political or societal spaces.



Rudy Guyonneau is a Senior Consultant in Artificial Intelligence for Cybersecurity at Sopra Steria SA. His doctorate thesis with Spikenet Technology at the Brain and Cognition Lab in Toulouse led him to study visual information processing in the primate's brain, to apply its keys in the fields of Machine Vision and Neuromorphic Engineering. After postdoctoral research at Georgetown University on Brain-Computer Interfaces, he eventually led the R&D effort at Spikenet Technology, applying spiking neural networks and related technologies to the industry, among them, Videoprotection. He joined Sopra Steria in 2016 to accompany the development of AI within Cybersecurity and to assist Airbus Commercial Aircraft in its Innovation strategy. He holds a PhD in Computational Neurosciences from Toulouse III University and acts as the Lead Cyber Data Scientist on behalf of Airbus CA.

As humans are not physically present in cyberspace[1], digital warfare is inherently technical. This does not mean it is an obscure affair of engineers withdrawn into some virtual tower. Plenty of military-specific concepts maintain their meaning in cyberspace. Military people engaged in cyberspace nurture the understanding of combat at every level, from tactical to strategic. Digital warfare is also a matter of defense and of attack, and ought to be fully integrated within global maneuvering, for the benefit of all fighters. The security team's duty is to outfit the corresponding cyber-ground so that it supports fighters engaged on land, in air, at sea or in space. The cyber-defense team hunts the attacker with the intent of disarming or weakening it. Such a defense can sometimes lead to cyberfighters acting beyond the digital frontline, in gathering intelligence or enforcing power. Right at the heart of digital warfare, in the very fabric of the space itself, cyber-fighters can find information and data. The growing automation and interconnectivity of military equipment multiplies the importance of information control—it is a key to power.

At the same time that the conditions for digital warfare emerged, automated information processing capacities experienced a qualitative leap. Artificial intelligence (AI) can thus be found at the heart of cyberwarfare because of its perceived potential and inherently numerical nature. Its impact over our hyperconnected world makes us interrogate ourselves to determine what constitutes humanity. From initially being the focus of academics, AI has quickly become the center of industrial interest and public expectation. The question of AI now tends to manifest under the guise of a mythicized omniscience and therefore, of a mythicized omnipotence. This can lead to paralysis of people fearful of having to fight against some super-enemy endowed with such an intelligence that it would leave us bereft of solutions. If this anxiety can be

[1] In France, the « *espace numérique* » is thought of as composed of three layers: physical, logical and informational. Humans and, through information, their perceptions become a target via the third layer. Humans are thus present in this part of cyberspace but remain less representative a function in a world that is inherently electronical. Combat remains in *fine* the matter of a dialectic in-between human wills.

Arnaud Le Dez is a French officer assigned to the Center for Doctrine and Command Teaching (CDEC) of the Army as a cyber defense expert. He started his military career in electronic warfare and information system administration and security, then switched from operation duties to headquarters positions, and was involved in several external missions in Lebanon and Afghanistan. In 2010, he joined what would later be known as COMCYBER and held various positions in cyber defense operations. Arnaud Le Dez holds a specialized Master's Degree in "Operations and Crisis Management in Cyberdefense" from Ecoles de Saint-Cyr Coetquidan. He is also an associate researcher at the "Mutation of Conflicts" division of Ecoles de Saint-Cyr Coetquidan Research Center. He authored "Tactique Cyber, le Combat Numerique," published in January 2019 at *Economica*.

understood, then the high stakes around the AI question become clear and must be addressed with reason.

Digital warfare and artificial intelligence share the same space—electronic equipment—and the same representativeness—digital. But what relationship do they have? How could this translate onto the field? What could it mean in the long-term? Here, we try and reframe the debate on rational and concrete grounds, which eventually led us to the vision of a cyberteammate. We do this because, in order for digital warfare to utilize AI and grow as a capability, and hopefully, as a force, we must have a grounded stance.

Digital Warfare: A Fight Like Others

Like other forms of combat, digital warfare is defined by its environment. Cyberspace grows by the interconnection of information systems of all kinds—business systems, as well as industrial and military ones—that form global networks. It is a medium for storing and making the quasi-instantaneous exchange of information that humans rely on daily. The information stored ranges from the most intimate testimonial to political action to economic, diplomatic, strategic, and tactical exchanges. It can be a tremendous echo chamber for communities of people and offer a way for the most vulnerable populations among us communicate and advocate. Cyberspace is not the exclusive tool of the mighty; it can enable the emergence of evil or benevolent organizations and ideas by connecting otherwise isolated individuals.

As an integral part of joint and tactical maneuvers, the operations and missions that utilize digital warfare are planned according to their expected effects within cyberspace or beyond. In and of itself, cyberwarfare is combat, which requires a planned and targeted process to conduct operations. It also requires intelligence at the tactical, operational, and strategic levels to measure its efficacy as well as its own rules of engagement. In cyberspace, the fog of war is induced by its very nature as a dense, complex, and heterogeneous web of data where stealth and swiftness reign. The limits commonly associated with digital warfare (non-permanence, measure limitations, machine-scale speed, and anonymity)[1] stem from this fog of war. Yet it is possible for one to grab onto and rely on recurrent signals amidst the fog of cyber warfare. In its purest form, it is an insurrection/counter-insurrection type of fight where the weak attacks and the strong defends. Indeed, defense always has more strength, as it has control over its own system, in a physical and a digital sense, which enables it to oust the attacker, including through the radical maneuver of replacing all of the hardware and the software by different equivalents.[2]

How The Traditional Principles Translate In Cyberspace

The principles of digital warfare still need to be codified. Their origins can be found by studying what has actually succeeded on the field, although there are too few examples so far to make any generalizations. Still, techniques and strategies evolve at a frantic pace, the former through the exigence imposed by early experiences in the field and the rate of technological development, the latter as our understanding of the stakes grows. The tactics of digital warfare are still developing, but can rely, at least partially, on the logics established by other warfare domains. Despite its youth, digital warfare can be thought of in relation to trends, and discovering the parallels to guide us. According to the ancient foundations laid out by General Ferdinand Foch in the early twentieth century, the French Land Army relies upon three principles that stem from the legacy of land conflicts: freedom of action, economy of means, and concentration of efforts.[3] The first two have a direct expression in cybertactics, while the third one is harder to distinguish.

- Freedom of action corresponds to the capacity given to achieve the mission. This is where strength can be found. A physical capacity in its original form, its cyber counterpart points directly to capabilities. Hence, according to the picture drawn above, strength lies predominantly on defense.

- Economy of means corresponds with reaching the best effects-to-effort ratio within the means available. Since wars are long, longer than battles, and since digital combat remains a human affair, as techniques and operations are led by humans, the economy of means remains one of the principles of victory. Time appears as a center of gravity, around which to apply the economy of means in order to win the fight.

- Concentration of efforts corresponds with the convergence in time and space of the actions and effects of the involved operational functions. Now, the digital space is constantly changing as it is less material than the natural space where the principle was forged. And time... what is time in cyberspace anyway? One can consider a subpart of the problem, however: combat speed, for example, it is definitely not determined by the speed of the cyber ammunition.[2] As far as we know, speed comes from decision-making, planning, and implementation, just as in classical forms of combat. One can infer that a, if not the, concentration factor is the person or people overseeing a project. This person is situated at the core of the action, and is essential in controling the tempo, maintaining the initiative, and keeping focused on precise actions. Taken at large though, concentration of efforts remains less distinguishable, because of the digital nature of the cyberspace.

The digital warfare principles question remains open because of the nature of the field, while being the focus of ongoing reflection. Even though its principles are yet to be firmly established, it nonetheless requires a means of organization, that can be refined as our understanding broadens. What we know for sure, and for now, is that decision-making speed must be prioritized. Decision-making means information-processing. The mind-bendingly rapid development of information technology we are witnessing in this early twenty-first century—best exemplified by AI—can be expected to weigh heavily onto a form of combat that is in its early stages.

From Machine-Intelligence to the Intelligence of Machines

Artificial Intelligence is a technology. It is, by definition, the science of information processing. If the Dartmourth conference baptized AI, its birth can be traced to the seminal "Computing Machinery & Intelligence" paper by Alan Turing in 1950.[4] AI captures some computationable aspects of cognition in mathematical form. These aspects of cognition pertain to the acquisition, representation, and production of knowledge. In one instance, it translates in the automation of logical rules, better known as the "symbolic approach." It is found across the entire spectrum of programming and it manifests itself in the von Neumann information processing architecture that we still call a "computer," and which now takes the shape of smartphone, a fridge, a vehicle, or a weapon system. Note here that a computer is seen as the materialization of a Turing Machine—a machine capable of simulating any kind of algorithm.[5]

The intelligence found in a symbolic AI is programmed and automated by humans. Machine intelligence relies on the subjective experience the programmer had with said problem. Machine intelligence is constrained by the logical formalism of the language and device by the programmer, which means that its behaviour model is strictly bound by human experience. As a result, the machine is able to replicate human expertise onto a defined world, but lacks any capacity to predict outside of it.

The novelty lies in the implementation of programs that allow machines to learn their own model. Under the term "Machine Learning," one finds a machine's capacity to develop its own responses to its environment, rather than relying on specified responses to a given set of symbolic inputs. Humans specify an architecture for the machine to learn an optimal behavior, as measured through an error fuction. This information processing paradigm appears during the 2012 ImageNet challenge, when Geoff Hinton's team demonstrated the power of what would become "Deep Learning" (DL) by winning the competition. The success of the "Machine Learning" approach is due to three factors which have become its pillars:

sophisticated algorithms (prominently, neural networks), cheap, parallel, computing power, and a sufficient amount of data describing the activity at hand. This is the ACD triangle. Programmed in this way, the machine has the capacity to unearth relations within the data that would have escaped the expert's attention, because of the following:

a. The number of channels a machine can analyze at any given moment is much higher (spatial dimension) than what a human could analyze.

b. The characteristic signal is too weak to be perceived on a single occurrence (temporal dimension).

c. The expert excludes significant channels because they do not correspond to his or her expertise (cognitive dimension).

If its creation, and sometimes its inspiration, is and remains human-driven, we are dealing with a budding machine intelligence. Yet one has to bear in mind that in no way is the resulting machine "autonomous," "free," or "possessing a will of its own."[2] The reason is simple: AI as a technology maintains a tool-to-crafter relationship with humans. In other words, AI machines are strictly the byproduct of human intelligence, which makes the latter responsible for every aspect of the formers' design, development, and deployment. Thus, it is early to assert machines will eventually surpass and annihilate us. As a technology who originates in a cognitive rather than physical capacity, one can, and actually should, conceive AI in a dialogue with natural, human intelligence. Its products are not "beings," even if the idealization is understandable. They are tools, and in the case of warfare, weapons. The so-called annihilation through AI would be ours, not AI's.

More concretely, the historical perspective presented here reaffirms the sometimes overlooked "software" reality of AI[3], even though there is a quantitative leap at the functional level. The "new" AI is bound to be deployed in all computers, to gather data. This reframing brings a remarkable insight as to how to utilize it for digital warfare.

The Cyberteammate at the Heart of the Digital Warfare-Artificial Intelligence Dialectic

Convergence between digital warfare and Artificial Intelligence starts in the very space where the former happens. When one considers AI as the science of information processing, then AI is the origin of cyberspace, since it proceeds from computers and their interconnection. It has allowed humans to multiply and automate their exchanges, thus generating such an impressive amount of data that AI was able to enter a second age, that of learning. In return, one can sense that an impact that AI will have on cyberspace will be to extend the machine's operational field to the natural space itself.[6]

Within the context of digital warfare, the amount, complexity, and heterogeneity of data, and the speed of aquiring and processing it, form the cyber fog of war. This data is generated by machines, upon which humans act to manifest their will throughout cyberspace. Where

[2] Not to mention that scientifically speaking, how do you compute autonomy, freedom or will? Desire?

[3] Precisely « computational », but strictly limited to the software level for the sake of argumentation, in waiting for its passing onto the hardware level.

cyberfighters are concerned, capabilities are computers and ammunition, pieces of code: these are inherited from AI's early paradigm. How will the new AI paradigm impact digital warfare then? Machines now have the capacity to make sense of a set of data that is too much for a human to comprehend, even with early-age equipment. AI speaks the language of machines and will translate it for humans to conduct their fight within a machine space.

The cyberteammate is the application of the AI technology for cyberdefense purposes. It is software for now and it provides a unique, and otherwise lacking, sense of the environment to the cyberfighter. With the conditions that learning algorithms are ready, computing power sufficient, and data available, AI will offer myriad applications for cyberdefense. Through AI, the cyberteammate will build its own understanding of cyberspace and will support the cyberfighter by giving them a clear perspective and understanding of the conflict. In this way, it can heighten the intensity of cybercombat, thereby reaching its potential as a planned, commanding fighting capacity. The cyberfighter is appropriately named, as a part of cyberspace and a budding intelligence that will bloom depending on the accompanying conditions, it will support the fighter to accomplish its mission.

Cyberspace is mostly an immaterial space: non-natural, logical, comprehended with one's mind. This is why electronic warfare and perception combat are intimately bound to cyber. It highlights the oftentimes non-physical nature of digital warfare, as it rarely moves into the material world, wrecking destruction on physical objects[4]. On the other hand, AI is an attempt at automating some facets of the human mind. As we can see, these two disciplines, which can be conceived as separate when reduced to their technical aspects, are intrinsically bound one to each other. They co-evolve around a cognitive axis. As sharing a common technical and cognitive cyber nature, it makes the most sense to heavily invest in AI's development for digital warfare.

Augmented Intelligence

Intelligence is key to sucessful combat and maybe be even more important to cybercombat than other forms of combat. In cyberwarfare, intel is data, collected in cyberspace. Cyberfighters need to know about their adversary's silhouette, weapons, and action modes (IOCs and TTPs), and must be able to characterize the operational theater in terms of environment, culture, economy, etc. At the tactical level, gaining intel is an aspect of combat itself. Intel provides the cyberfighter with an understanding of what is happening on the cyberbattlefield and in relation with the physical world. It is achieved at the tempo of combat, so that the officer in charge conducts it within the joint maneuver. Good intel is the sign of the strong convergence between AI and digital warfare, and its most obvious application can be found in the evolution of Natural Language Processing.

Swift, flawless, automated translation is expected by the intel world. Based on the advances in analyzing unstructured data, and the growing capacity to output in a given language, AI will help overcome the cultural barrier to conducting research and, more importantly, interaction.

[4] The physical treatment of cyberspace infrastructure might be a necessity of combat, but is not at the heart of its vocation.

A cyberteammate for intel would rapidly collect data across an otherwise unaddressable range of open sources, translate and synthesize it in a short paragraph, provide a status and isolate the tactical and technical information relevant for combat. It would also improve its capability of cultural influence through social media by automating part of the translation process and simulating more credible legends to magnify the impact of inflamatory posts. It can be deployed passively, as when it assess massive amounts of open written text as it is able to detect changes in tone or style, and link together different texts written by the same, anonymous author.

Situated at the heart of combat itself, augmented intel can dissipate the fog of war, resulting in a swifter and more just attribution. AI's capacity to address vast amount of data has a natural application in the data analysis performed to a battlefield's situation. When data relative to the combat zone is analyzed in its entirety, it can produce a complete and precise picture of the situation. The cyberteammate also contributes by establishing a situational map of operations on the battlefield, accounting for the battle's history and progress, perhaps to the point of actually predicting its evolution, at least in the short-term. Attribution is an exercise in nuance rather a binary one[7]; attribution increasingly relies on a given data, analysis of its timecourse, studying its interactions with the surrounding data, and addressing it within the global context while utilizing intel from sources other than cyber.

Simulation and Customization

If the corresponding data exists and can be acquired, a cyberteammate has the capacity to simulate any type of environment, whether friendly, neutral, or adversarial. These simulations improve the training of cyberfighters by designing a more realistic operational theater as well as a more complex opposition; one can relate here to Reinforcement Learning and its achievement in the GoGame, as well as to Generative Adversarial Networks.[8] These platforms recreate scenarios that have been encountered in the field to explore the consequences of choices other than the ones that were made.

Prior to combat, the simulation allows fighters to rehearse with action modes and weapon types tested in realistic wargames. The damage output and the expected effects can be measured, studied, and validated and their results can then be integrated in the global planning. Non-compliant cases can be tested and others discovered. The cyberteammate provides simulation support during operations as well, by predicting outcomes based on data gathered and analyzed. AI will never be omniscient, and it will not replace humans, especially in spheres like combat, where determination, strength, and passion are necessary to succeed. Emotions and such characteristics are simply not computable, at least right now. Cyberfighters can choose to heed the advice of a digital teammate, or dismiss it. The challenge will be for us to understand its limitations, biases, and difficulty assessing an enemy we might not recognize; we will have to learn to "talk" to it.

The Tactical Cyberteammates

Digital warfare can be broken up into three tactical modes. The security mode sets up the combat zone and makes it defendable. It checks for good cyberhealth that enables operations and increases the accuracy of attack detection systems. AI can give this mode a camouflage capacity. Once it learns the global behavior of the system it secures, the cyberteammate computes and produces the counter-data necessary for smoothing out the data produced by the securization activities. If the enemy is already within the system, the objective here is to keep the installation invisible, so that the environment seems to be performing as expected, while it enables a strong defense and prepares for a counter-attack. The element of surprise is also a winning factor in digital warfare.

A defensive mode starts with detecting an attack. AI contributes both legacy-wise and novelty-wise. The "honeypot" evolves to enact human-driven and somewhat credible target systems, luring the attacker into taking possession of it. The gain is two-fold: an extension of the domain to defend while shortening the actual attack analysis. AI also brings the possibility of a defense cyberteammate that mimics the defensive stance of a cyberfighter. Such a deployment would act as a first defense layer allowing the human teammates to focus on assessing the global situation and defending more critical systems, both of which are in line with the freedom of action and the economy of efforts principles.

In the offensive mode, the cyberteammate deploys another form of camouflage. Having learned the language and the operating mode of the target, it applies them to the commands to make them invisible. AI can suggest which commands to give, but the ultimate decision is up to the humans fighters. Additionally, the maneuver itself can be fortified by an attack by cyberteammates, which would simulate aggressive behavior and divert the target's attention. If cyberfighters choose to run this type of diversionary tactic, they must give special attention to this type of system as it could potentially hinder the maneuver with undesired affects. The offensive cyberteammate embodies the question raised raised by AI's advanced weaponry and by extension, of their autonomy.

Limits and Perspectives for a Cyber-Oriented AI Development

AI is a technology. It is peculiar in that it reflects us back to ourselves and leads us to believe it might be, if not alive, then animated. It does not have to be this way. Anthromorphizing AI inflates it into some sort of omniscience, a sure sign the "Peak of Inflated Expectations" of the Technology Hype Cycle has been reached. But these outsized expectations always meet a "Trough of Disillusionment" when the early experience fails to meet the expectations of exaggerated marketing campaigns. Now that most technologically advanced nations are strategically planning at the highest levels—without myths but with a strong set of values and knowledge—we can expect that we are starting our way up the "Slope of Enlightment." Presently, the focus is to design AI on a sound basis, for a concrete and rational adoption on the ground.

AI's strength relies on three pillars: algorithms, computing power and data, all of which are enabled by humans. AI's strengths are its weaknesses, which we will address, in part, and suggest some potential remediations.

- **Algorithms:** "Deep Learning" is the most representative type of Algorithm. These are highly-nonlinear so are hardly explainable, if at all. Devoted programs have been launched to tackle this problem (e.g. DARPA's Explainable AI). The rule is for the operational deployment of AI to be effective, controlled and simple. While perfectly reasonable and legitimate, it is a bit of a paradox, as AI is here to develop its own understanding of the vast amount of a data we can no longer handle. We may not need to be able to explain its reasoning in order to be confident in its outputs; we might rather learn to understand and get used to it through training and education. Mostly, we need to keep it in its proper place, that is, not in control.
- The demand for **Computing** power is voracious and requires cloud-like capacities. This solution induces additional delays at the tactical level of combat, especially when moving rapidly. Aiming at local, modest applications could actually help AI-enhanced cybertroops remain within the required tempo. Besides, the simplicity of these applications would advance AI adoption by field personnel, whose operational skills tend to be stronger than their tech-savviness.
- The capacity of AI to account for excess **Data** opens the door to data-manipulation by its very environment[9]. Maintaining the integrity of the data should always have the highest priority, as the consequences of it being tampered with will be equal to the power it could give. A robust algorithm will partially protect the integrity of the data, but quality sensors should also be involved.

AI is also a science. It advances our understanding of a given topic–the processing of information–and bounds our knowledge through the use of reason. This means our concerns, and sometimes our fears ought to be addressed rationally. AI's development should be embraced because of its potential to be a solution to a cyberspace that appeared too swiftly for the human brain to adapt to and to make its own. Because it is cognitive, and the brain is where cognition naturally happens, AI may be considered an extension of the brain, as foreshadowed by the Neuralink initiative, or DARPA's Intelligent Neural Interfaces program. But let us not forget the pioneering work of Miguel Nicolelis and his team in 2003.[10] It is remarkable that the media makes such a huge use of the brain imagery when discussing AI, and that AI development seem to devote little attention to neurosciences, a discipline which contributed to AI's inception,[4,11] and is at the core of AI's recent progress (DL replicates aspects of the human visual system),[12] and continues to deliver insights.[13] The military, especially, would benefit from using biology, and the neuromorphic engineering sprouting from it, as this has economy of means, both energetic and computational (e.g. IBM's SYNAPSE program).

What's Next for Digital Warfare

Digital warfare is a form of combat, just like more traditional forms of combat. It is highly technical and successful digital warfare requires a tactical sense and strategy, placing it squarely in the military realm. It draws its tactical principles from land, air, sea, and space legacies. AI plays a role at every level of digital warfare, from hunting the enemy through sensors and gathering intel, through assisting in decision-making and simulations, to supporting the maneuver and use of cyberweapons, and more. In its core capacity of addressing the fog of war, AI offers a possible solution—even if only partially—to the non-permanence, the measure limitations, the machine speed and the anonymity that characterizes cyberspace. Efforts to develop AI within the context of digital warfare are strategically important. These efforts will maintain our combat capability in this newly emerged battlespace, while becoming a component of power in all the others.

As mentioned above, the ACD pillars offer many research pillars for increasing cognition degree—synonymous to an increasing degree of automation—to the point of possibly culminating into a real form of autonomy. Military-specific investment in these research pillars is necessary, for the sake of sovereignty and for practical purposes as well, as cyberfighters will make use of AI in rugged conditions. Data-centric development indicates that a dedicated line of operations will be allocated to maneuvering the sensors in charge of collecting data. On a global level, this applies to cyber-oriented intel. This development is a necessary step to get digital warfare to reach its goal of a full and seamless integration within other military operational domains.

Let us not forget the central actor: the humans who forge AI, in order to fight with it. The quality of cyberteammates will depend on the quality of the scientists who conceive them, the quality of the engineers who build them, and most of all, the quality of the military personnel who command their design, their deployment, and their use. The military must take ownership over the development of cyberteammates, in order to guarantee that the technology follows the values the military is sworn to defend, while remaining accountable for its use and effects, in line with the law of war. Without safeguards such as rules of engagement, the introduction of AIs on the battlefield could, and would, instigate a rise of undesired extremes on either side, or, at the very least, a rise in abberant behaviors. But again, as humans are in charge of the design, the development, and the deployment of AIs, they also must be accountable for their machines' behavior. The machines' display of intelligence means that we can never forget that they are weapons, whose creation and continued existence is our responsibility. If we cannot guarantee the behavior of a weapon, we should not be allowed to use it. The dominion of will, and its rights and responsibilities, is and must remain supremely human.

To Choose is to Become

The excitement in building a new capability lies in the freedom of imagination and, its success lies in developing a profound knowledge base in a variety of fundamental sciences such as military, computer, mathematics, cognitive, social, etc. It is a time for dialogue, of sharing ideas and confronting intuitions, collaborating with experts in other domains to work through intellectual deadends. Although the journey is exhilirating, there are pitfalls. The trick is to let go of our anguish, our fears, our resentment, and of our *own* biases; and to stay anchored in reason.

It is far too soon to predict what the future holds, as this is only the beginning of the intelligence of machines. Left to others, AI will materialize as the scary figures they propose. The choices we now make as brains and machines hit their strides around the world will shape the AIs we will adopt on tomorrow's battlefield. One culture's choice of an AI will not be the same as another's, whose approach to cyberspace will differ similarly. Let us remember, in a bid against any distractive anthropocentrism, that cognition is the hallmark of living things, not uniquely of humans. Tomorrow's AI will have the whole range of biological forms to take inspiration from. Why have expensive terminators when you can have easily replaceable swarm of automated killer bees? More seriously though, future digital warfare will have a wide array of approaches and technical choices available, will share a common data-environment, and still be deeply rooted in previously defined objectives and frameworks. Let us reassure Clausewitz and his heirs: because AI is conceived by humans, warfare will remain a combat of human will.

AI and cyberdefense are complex and emerging disciplines. They require quick responses, to account for the pace at which they are being developed, yet these responses must be thoughtful and well-reasoned. The early reflections presented here raise far-reaching questions, and we hope that they will help with the concrete and conceptual development of AI and cyberdefense. Mainly, we show that digital warfare and artificial intelligence converge in cyberspace—the former by expressing our will, the latter by supporting it. Their importance lies in the advancement of knowledge that will happen with their development and the power they have on the battlefield. We should support ambitious research and supervised development to support their growth into maturity and to frame AI in accordance with the military's goals. The force of digital warfare resides in the capacity to analyze and act on collected data, rather than in merely possessing it. AI, the science of information processing, has a key role here.

As a final note, we would like to take a step back and consider the state of the public debate. AI tends to manifest itself under the guise of a mythicized omniscience, and thus omnipotence. AI is not a god; it is a forge and data is its fire, hardware its anvil, and algorithmics its hammer. The weapons in the future will be a myriad, and the cyberteammate who can fight alongside the cyberfighter will be the most remarkable of them all. AI is the key to cyberspace's intelligibility. Without it, digital warfare will endure; with it, it will thrive.

NOTES

1. Kallberg and T.S. Cook, (2017), The Unfitness of Traditional Military Thinking in Cyber. IEEE Access 5, 8126-8130. DOI: 10.1109/ACCESS.2017.2693260
2. A. Le Dez, (2019), "Tactique Cyber, le combat numérique". Paris: Economica.
3. Armée de Terre, (2008), Tactique Générale. Paris: Economica, 28-32.
4. A.M. Turing, (1950), Computing machinery and intelligence. Mind LIX (236), 433-460.
5. A.M. Turing, (1936), On Computable Numbers, with an Application to the Entscheidungsproblem. Proceedings of the London Mathematical Society, 42: 230–265.
6. R. Guyonneau, (2019), Extension of the machine's realm: a brief insight into Artificial Intelligence and Cyberspace. The Cyber Defense Review. https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/1880459/extension-of-the-machines-realm-a-brief-insight-into-artificial-intelligence-an/
7. T. Rid, and B. Buchanan, (2015), Attributing Cyber Attacks. The Journal of Strategic Studies 38 (1-2), 4-37.
8. Silver, S., Hubert, T., Schrittwieser, J., Antonoglou, I., Lai, M., Guez, A., Lanctot, M., Sifre, L., Kumaran, D., Graepel, T., Lillicrap, T., Simonyan, K., Hassabis, D. A general reinforcement learning algorithm that masters chess, shogi, and Go through self-play. Science 362(6419), 1140-1144 (2018).
9. A. Chakraborty, M. Alam, V. Dey, A. Chattopadhyay and D. Mukhopadhyay, (2018), "Adversarial Attacks and Defences: A Survey". ACM Comput. Serv.
10. J.M. Carmena, M.A. Lebedev, R.E. Crist, J.E. O'Doherty, D.M. Santucci, D.F. Dimitrov, P.G. Patil, C.S. Henriquez and M.A.L. Nicolelis, (2003), Learning to control a brain-machine interface for reaching and grasping by primates. PLoS Biology 1(2), e42.
11. J. Von Neumann, (1958), The computer and the brain. Yale University Press.
12. Y. LeCun, Y. Bengio and G. Hinton, (2015), Deep Learning. Nature 521, 436-444.
13. S. Ullman, (2019), Using neuroscience to develop artificial intelligence. Science 363 (6428), 692-693.