The Essential Digital Transformation of the Battlefield and Its Effects

Gérard de Boisboissel (École spéciale militaire de Saint-Cyr)[1]

Introduction

While the digital transformation of our armies is a process that has been underway for years, we have only recently become aware of our vulnerabilities in the face of symmetrical or long-lasting conflicts.

It raises several questions that we will try to address in this article: the importance of data, the essential prioritization of the protection of our digital systems, the place of the military decision maker in the technological systems of tomorrow (which should evolve in such a way that s/he retain full control over them), and finally the risk of vulnerability that this race to digitization could introduce to our forces in a future conflict.

And so, could the digitization of the battlefield, essential for military efficiency . . . become a colossus with feet of clay?

Digitalization of the Battlefield

The Importance of Data as a Factor in Victory

From the scouts of antiquity to the dispatch riders of World War I, armored reconnaissance units, planes, and finally satellites, any operation aiming at gathering intelligence, and analyzing, exploiting and transmitting it contributes to military victory because it allows for anticipating the enemy's tactical and strategic maneuvers ahead the tactical and strategic maneuver. Because knowledge is power, and therefore victory.

[1] This text is a translation of an article originally written in French.

However, since the invention of the Intel microprocessor in 1971, armies have entered another phase, that of the digitization of all military equipment, the spread of modeling and digitalizing any process of any military phase or activity, with the consequence of a significant increase in the volume of data. This raises the question of data processing, but also of interpretation and control over the data, opening a large and new conflictual space, namely, cyberspace.

This race for digitization is inescapable because it has a double foundation:

- the desire to master all the parameters involved in battlefield modeling in order to not be surprised by the unexpected: from the weather to the number of cartridges per charger for each infantryman, to the possible position of the enemy on a digital map;

- but more importantly, the speeding up of the tempo of operations: the side that first processes information and deduces the most appropriate reaction takes the initiative, and therefore raises the probability of victory.

The value of the data as a factor in victory is therefore quite clear. Cyberspace thus becomes a new combat dimension, a space ringfenced by new defensive and offensive doctrines that states develop to ensure their sovereignty and control, even as they consider that recourse to the use of force may be motivated by acts of war that take place in cyberspace itself.

The Digital Transformation of Military Equipment

This digital transition has long been underway for the French armed forces. All new military equipment now incorporates a digital component that allows it to be connected to the outside world and to exchange with other equipment, to be configured and supervised remotely.

This is true for the equipment worn by combatants (FELIN system of the French Army), for new-generation military vehicles equipped with a vetronic network (such as the new armored or transport vehicles of the French program Scorpion, which is upgrading its tactical combat weaponized platforms), but also includes the newest tools of the battlefield, namely military robotic systems. The latter are now remotely operated but will gradually acquire some form of

autonomy in order to help the combatant maintain his permanence on the field and his military efficiency. For the purposes of protection and efficiency, soldiers may soon be able to delegate to robotic systems tasks or missions, allowing them to be performed without intervention (without relinquishing control).

Data Security and Control: Essential Prerequisites for Military Mastery

Nevertheless, this race for innovation can be very dangerous if data, which are at the heart of this transformation, are not secured. For when we speak of digital processing, we must speak also of potential vulnerability of the systems to cyberattacks and anticipate the digital battle of tomorrow. We must cyber protect our systems and integrate cybersecurity from the start of their design: cybersecurity by design. It must be a natural component of any systems and solutions that evolve in cyberspace. Our systems must therefore be resilient by design, that is to say able to withstand, operate under attack, and propose bypass measures even if running in degraded mode[2].

Otherwise, a soldier will not be able to trust a machine that may become inoperative by a cyberattack, or even diverted from its original use by an enemy takeover. Similarly, if a soldier embarks on a mission with technological equipment, any action setting it out of control would render him weakened and potentially inoperative.

Rethinking Our Approach to Military Planning

New challenges are emerging for the military forces, related to the security of information systems. While these challenges are now accounted for in the responses put in place by a number of states that have recognized this issue, it is still true that, like any major new technological

[2] Gérard de Boisboissel, "Sur la cyberrésilience des systèmes d'armes," *DSI*, no. 52, Special Edition, "Cyberguerre: L'heure de l'action," 2017.

evolution, the doctrine of use must follow and adapt to new opportunities and new threats in cyberspace.

And in fact, the superabundance of data changes precisely the way to prepare for warfare and to carry it out.

Accelerating the Data Processing Cycle

First, the deployment by military units of new equipment integrating interconnecting components of digital information processing will allow the offsetting of potentially mobile sensors and effectors permanently on area, and their deployment within geographical spheres of immediate interest. Such a deployment, in addition to widening a unit's possible area of action, will allow for the reduction of its response time, whether in terms of its decision-making once the information is acquired, or by the use of its remote effectors.

For example, robots occupying the space will be available to launch a response allowing the unit to take or keep the initiative by reducing the cycle of Detection-Decision-Neutralization, otherwise known as OODA (Observe - Orient - Decide - Act), with lower data processing time than humans. These systems will thus be able to detect fired shots and position their effectors directly in the dangerous direction and the target that they can automatically follow if it is in motion, while transmitting this information to the supervisor.

Modern armies have understood this issue and have directed their engineers to work on this gigantic challenge of embracing the complexity of different possible combinations of events on a battlefield, to win the battles of anticipation and responsiveness.

Managing the Data Overload

While interconnected tools and systems ensure easier flow of information, they have also proven to be formidable data producers, requiring complex treatment methods. This requires,

according to LCL Bertrand Boyer, the rethinking our relationship to information, its processing, and its exploitation in the service of decision-making.

Indeed, most of our models are today from an era not really digitized, where data was scarce and where the effort was focused on collection via the deployment of sensors, with ultimately fully human supervision of data analysis.

However, while there is an overabundance of data, the main goal of dissipating the "fog of war" may actually thicken it if data are not captured and analyzed. It is therefore a question of constructing the right models of analysis and presentation, in order to obtain an appreciation of tactical information.[3]

Avoiding the Paralysis Effect

The effects of digitization may be the opposite of those expected, most notably the growing need for information that can induce a form of paralysis in decision-making. Continuously fed, the chain of command may tend to postpone its choices, for fear that a new element will alter its initial appreciation of the situation. Paradoxically, while digitization should reduce the OODA loop as indicated above, it can, conversely, lead to its blocking,[4] especially as the ability to trace any information exchange will allow replaying the sequence later and judging a posteriori the best strategy that should have been adapted.

Seizing New Opportunities

If this is a vulnerability for our military forces, it is also an opportunity for more effectively combatting enemies of a conventional or irregular nature. Unsecured or unsecured transfers of data between sensors, the free access to certain tools or services accessible by external channels, open

[3] LCL Bertrand Boyer, "Comprendre pour agir à l'heure du big data: Une approche stratégique de la donnée," *DSI*, no. 52, Special Edition, "Cyberguerre: L'heure de l'action," 2017.
[4] Ibid.

for our military forces the possibility of constructing new modes of action to usurp, recover, degrade, destroy, or modify data used by opponents.

Adapting to New Military Modes of Operation

The digital transformation of the battlefield poses a crucial question, that of system empowerment. This is a logical evolution of the constant increase of the computing power of embedded components, as well as of the recent development of algorithms that adapt to unknown environments or that self-learn as in the case of Artificial Intelligence(AI).

After wanting to strike further and stronger, military action now involves delegating repetitive or dangerous tasks to machines, so that they react by themselves as quickly as possible.

Toward a Dehumanized Action

This gradual introduction of robotized systems on the battlefield will induce a paradigm shift: contact combat will inevitably become robotic in the future, relying on sophisticated machines analyzing threats in near real time, making decisions accordingly, and triggering action much more quickly than a human being could (emission of an alarm, automatic pointing of an effector towards the dangerous direction, its activation, repositioning, retreat toward a strategic position in the rear, etc.).

It is therefore inevitable that weapons systems with some form of autonomy will emerge in the coming decades, going even so far as lethal use.

Nevertheless, if the temptation of a dehumanization of the warfare seems to be on the horizon, leaving the battlefield to machines is an idea which, while it presents an interest for the protection of the combatants during the battle, remains both illusory and limited. In fact, it will always be necessary for men to be at the heart of military action to understand and guide it, providing the situation with an intelligent direction that machines cannot have. It is within this

action that human perception and human intuition will prevent the total robotization of combat and thus its dehumanization.

Also, totally removing humans from zones of military confrontation becomes nonsensical when it comes to the occupation of the terrain. In fact, it will always be necessary to have soldiers (male and female) physically occupy an area, to feel it, and to ensure contact with the civilian population.

Keeping Humans at the Heart of Digital Systems

The Responsibility of the Leader

Whatever the technology, the military commander is not exonerated from the responsibility for its use. He commits himself, and commits his country, whatever the equipment he uses.

This allows us to distinguish three levels of responsibility for any military system:

- The responsibility for its design:
    - A design responsibility belonging to the engineer on technical issues;
    - A design responsibility for human engineering that includes the training of men in the use of military equipment.
- The responsibility of the leader who uses it for his benefit:
    - Consideration by the engineer of the constraints of the military terrain;
    - Training for and preparation of the mission including the military systems.
- The responsibility of its operator:
    - Ensure the proper use of the weapon expressed in terms of proportionality;
    - Ensure from the start the proper functioning of the system.

The use of digital systems, basically, does not exonerate the operator or the leader of their responsibility. The latter are the guarantors of the use of the former. This constraint will have the

virtuous effect of introducing a duty of care for the decision-maker in the use of his machines and will prevent him from using them in a dangerous way or in a way that would run counter to the laws of war.

The Commander Gives Meaning to Military Action . . .

It remains fundamental that the last two categories of actors above, the military leader and the operator who use digitized military systems (robots, information systems, or weapon systems), must retain the mastery of use and control allowing them to lead and run the military action.

The commander, meanwhile, gives meaning to the overarching maneuver, which machines will never be able to do for lack of intuition and awareness in action.

While autonomy is useful for robotic systems deployed in the field, they must remain executive actors in the same way as any human tactical element. They have to be subject to orders counterorders. This is because while the chief commands the units he has under orders he also trusts them in carrying out the mission he entrusts to them, which is fundamental to the principle of subsidiarity.

For this reason, it is of no interest to him to have a robotic system that governs itself with its own rules and objectives, or which can show disobedience or free itself from the frame it was given. Similarly, such a system must respect orders and military instructions, because it is the leader who issues them and who gives meaning to the military action, all while being responsible for its outcome. The consequence is that at any time the leader must be able to regain control of a robotic system and potentially make it exit the “semi-autonomy mode” into which he himself had allowed it to enter.

This is important because it means that he has to have full mastery of communication and access to the systems and equipment at his disposal, as well as of everything that feeds these

systems, namely the data captured and processed from the battlefield, intelligence data, orders received, and external data that contribute to the development of the maneuver (such as the weather forecast for example).

This control requires cybersecurity systems that must ensure the reliability of data processed. If this is missing, the supposedly efficient systems will not be credible, the soldier will not trust their use, and either reject them or will work in an environment in which he cannot trust them to function effectively.

. . . Without Being the Weakest Link

The constancy and responsiveness of automated machines being superior to that of humans, some may consider combatants to be the fragile element in the military systems deployed in future theaters of operations. A declassified document of DARPA indicates that the human element (the soldier) has been considered the "weak link" of defensive systems as early as 2002.

Having already emphasized his primary role in the conduct of operations, it is then necessary to ensure that he is helped to maximize his abilities to supervise the systems he has at his disposal on the battlefield, and to organize tasks and control the tempo of operations and the decision cycle. Today, moreover, new, unprecedented opportunities exist to strengthen human capacities, both physically and psychologically, through new technologies, particularly NBICs (nanotechnologies, biotechnologies, informatics, and cognitive sciences), which could strengthen a soldier's capabilities or help him in his decision-making.

These technologies are either equipment worn by the soldier, like embedded customized systems, or external systems with which he interfaces through human-machine interfaces. Here again, the vulnerability of these systems is one of the new factors of future conflicts, as such

equipment includes hardware and software components that could be endangered by cyberattacks or electromagnetic impulses.

There is no doubt that the enemy will seek to address the weak point of these customized systems, probably via either the data that irrigate them and on which the soldier will rely in the heart of battle, or via the human/ machine interfaces that he will use. The enemy will therefore seek to render them inoperative, either by destroying them by physical attacks using electromagnetic war means, or by neutralizing or altering them through cyberattacks.

Cognitive Overload: A New Challenge for Military Decision-Makers

The digital transformation is driven by technological innovation but its consequences go beyond information processing and networking tools: it brings with it a flattening of organizations and alters hierarchical organizations by transforming the decision-making circuits. Man thus finds himself in the center of, first of all, an individual sphere in which he must master equipment that can increase operational capabilities, and secondly in a wider sphere where he pilots the new tools at his disposal for military action.

This double dimension is new because it puts him in the middle of a dual technological and decisional system, bringing with it the risk of a cognitive overload.

One possible solution to this problem is the recent development of artificial intelligence, a promising technology that will help in adapting to the unknown by combining the double advantage of:

- Allowing some autonomy of adaptation to robotic systems;
- Allowing decision support for the military commander.

Artificial Intelligence (AI): Supporting the Digital Transition and Security of Our Systems

In September 2017, Russian president Vladimir Putin famously claimed that "whoever becomes leader in AI field will be the master of the world," a thesis that resonates with the July 10, 2017 statement of the Russian company Kalashinkov, which foresees the development of autonomous armed modules based on neural networks for the detection, identification, and automatic processing of targets, and the willingness of the Russian army to have automated systems to accelerate the decision making cycle of military leaders.

The Russian authorities therefore designate AI as the key to success on modern battlefields, providing a better understanding of the environment, a faster capacity than humans (and therefore the enemy) to write and transmit orders or tactical options. For her part, French Minister of the Armed Forces Florence Parly demonstrated her awareness of the immense opportunity that AI can bring when she defined the new French strategy in this area on April 5, 2019, at Saclay, stating that "the development of The AI is now a place of strategic competition, a race for technological power, economic but also military, and that France cannot take the risk of missing this technological shift."

The Possibilities Offered by AI

The importance of this technology for machines lies in the possibility of delegating to them specific behaviors related to:

- Solving problems that are neither simple nor deterministic;
- Automatically detecting, characterizing, and processing information in complex environments or widened spaces;
- Performing data fusion, that is to say aggregating data from heterogeneous sources;
- Making correlations between domains that are not easily connected to each other (within Big Data, for example);

- Being extremely responsive where analysis time is too short for a human to do it on his/her own.[5]

AI may also help by allowing the:

- Treatment of massive data in times unattainable by humans;
- Reducing the range of possibilities if parameters are too numerous;
- Simulating human cognitive functions such as perception, knowledge representation, reasoning, communication and expression skills, and the implementation of decision-making processes.[6]

As a result, new command support tools will gradually be integrated into the battlefield. It is in this field of action that AI can bring real benefits, improving tools that are currently hampered by low interface quality or software age. The possibilities are multiple:

- Provide decision-making options to the military leader depending on the context, usually known as decision support;
- Automating certain repetitive tasks within the Military Staff, which currently sometimes lead to a significant time lag between the situation presented to the commander and the actual situation;
- Automation of messaging after analysis, synthesis, and dissemination of the processed information;
- Automatic image processing or mapping;
- Etc.

AI and Data Security

[5] Gérard de Boisboissel, Contribution, *DSI* no. 65, Special Edition, "Intelligence artificielle, vers une révolution militaire?," April 2019, 18.
[6] Jean-Gabriel Ganascia, Contribution, *DSI* no. 65, Special Edition, "Intelligence artificielle, vers une révolution militaire?," April 2019, 9.

According to Thierry Berthier,[7] associate researcher at CREC Saint-Cyr, artificial intelligence (AI) accelerates, rationalizes, optimizes, and automates more and more complex functional sequences that can now be run in "very high frequency" mode.

However, algorithmic progress is accompanied by a widening of the spectrum of cyber threats. AI is a possible answer to improving the reactivity of countermeasures to be applied to cybermenaces, in order to protect systems against more and more complex cyberattacks in real time, recognizing in particular abnormal behaviors or unwanted weak signals.

On the offensive side, AI will also transform the classic methods of cyberattacks, making them more autonomous. Contemporary examples include the False Data Injection Attacks targeting the components used for automatic learning embedded in systems, as well as the "Adversarial Examples" attacks that exploit specific vulnerabilities affecting artificial neural networks.

The Question Posed by AI

The major issue of Artificial Intelligence is that of the delegation of human decision-making capacity to machines that demonstrate a certain form of semi-intelligence, in particular because they incorporate self-learning capabilities. Basically, any self-learning system must be educated. Also, just as the owners of animals are responsible for their training and the possible damage they could commit, military leaders will be responsible for the proper learning and the proper use of machines in the field. To do this, they will have to supervise the self-learning process and then update it regularly and ensure control over it as time goes on.

[7] Thierry Berthier, Contribution, *DSI* no. 65, Special Edition, "Intelligence artificielle, vers une révolution militaire?," April 2019, 34.

The implementation of this constraint is complex, unless soldiers deployed in the field are prohibited from activating by themselves self-learning processes whose certification would be too complex to carry out in the field with uncontrolled data and, above all, a result difficult to certify without the requisite technical expertise. One may also mention here the risk of loss of confidence by the soldier in his machine if the success of its apprenticeship is not guaranteed.

In fact, a safe approach would be to train the AI from databases that have been duly validated but which are stored in a confidential area and secured outside the theater of operations. This location outside the theater ensures that the responsibility for training will be on the technical experts of the AI and of the host machine, all validated by the military.

Software Safeguards

In order to ensure control over of the systems of the future integrating some form of semi-autonomy or AI, and in order to overcome any error that could be dramatic for a country, the use of force must be framed by safeguards that are simultaneously legal, ethical, and technological.

Consequently, the consideration of security issues in the development, maintenance, and use of software becomes an imperative arising from the omnipresence of the risks of digital cyberattacks.

Safe by Design

In practice, "safe by design" is a first response presenting major advantages for any military system and permitting continuous follow-up of the development of any negative traits or defects that an innovation may have in regard to international and ethical norms.

Let us recall that, in order to be legal, all new weapons systems must respect a certain number of constraints and rules, namely :

- International regulation

- Rules of engagement formulated by the head of the military
- An ethical imperative that the military chief develops depending on the situation on the ground.

These constraints and rules are extremely complex to transcribe in computer language. Nevertheless, software safeguards "by design" can ensure compliance with this normative framework, despite a number of constraints, which are as follows:

- Any robotic weapons system must be under the control of its operator and the military commander who uses it;
- It is imperative to ensure the framing of a self-learned machine and ensure compliance with rules during code execution;
- Translate into engineering language the rules and constraints so that the subjectivity of the law is not an obstacle to the development of software that wants to respect the rules;
- The autonomy for a weapons system must be limited both in a delimited space and in time.

Our systems must be able to evolve, because legal frameworks are constantly changing and because ethics adapt to the complexity of the situation, just as the rules of engagement do. Thus the behavior of these machines must be able to adapt dynamically within this context.

Evaluation of "Safe by Design"

Product testing allows us to check if a product meets performance, quality, or safety criteria.

What about digital systems embedding "by design" security software safeguards, and AI which we know can self-learn from unknown situations? Agnès Delaborde[8] indicates that the answer is negative if it is a black box situation (high TRL, marketed solutions): in that situation,

[8] Research engineer in AI evaluation and robotics, LNE

whatever the design mode of the system, only the inputs / outputs are taken into account. On the other hand, the answer is positive if it is a white box situation, because we can understand and study the entire algorithmic flow of decision-making; this situation seems preferable for both testing and certifying systems.

Conclusions

The performance of our weapon systems of tomorrow will allow us to maintain the ascendancy over the adversary, and thus the initiative, the guarantee of victory. This performance involves the integration of new digital technologies, such as AI, allowing progressive autonomy of systems, whether they are information processing systems or robotic systems deployed on the battlefield.

Nevertheless, this inevitable technological evolution must be accompanied by a cautious approach toward these systems and their use, for several reasons:

A) First of all, humans, even if they can delegate tasks to more responsive and precise systems than themselves, and with information processing capabilities superior to their own, will have to remain at the heart of decision-making loops because it is they who gives meaning to military action and ensure a humanization of the battle space, being the guarantors and carriers of the ethical virtues that their country asks of them.

B) Furthermore, these systems will have to be reliable, because a military commander will not use them if he does not trust the security of their use and cannot control them. To this end, software safeguards ensuring compliance with security constraints should be integrated “by design,” from the conception of these systems, and updated regularly according to technological developments and specific rules of engagement in the military theatre.

C) They will also need to remain resilient in the face of possible technology failures. Cyber-resilience is the ability of a system to resist a crash or a cyberattack and return to its original state after an incident, or in other words the ability of any entity to recover its initial properties after significant alteration.

The digital transformation of the battlefield is underway, inevitably. States globally have realized that they can only maintain their strategic and tactical superiority by developing new tools at the service of the combatant, such as military robots, data processing tools to manage the multitude of data captured on the battle field or embedded at the heart of our systems, and decision support tools for military leaders. And all of this, in order to be permanently present on the battlefield, must be more responsive in reactivity, more precise in execution.

But this race for technology is viewed dubiously by our unconventional enemies, who see in it an alienation of the fighter in favor of technology, and a possible renunciation of traditional military values in favor a dependence on systems that are certainly powerful but very dependent on the data that feeds them.

For conventional armies, this enslavement to these new systems induces an opportunity for offensive actions already doctrinally integrated in the army headquarters: neutralizing the systems physically or neutralizing them by attacks on the data completely paralyzes the enemy's operating mode. Hence the absolute necessity of ensuring the cybersecurity of our own systems, which is the essential foundation for the use of our weapons systems.

Nevertheless, there are still some wars that are long lasting, and we achieve victory if we outlast the opponent. It is a safe bet that for high intensity conflicts, the first battle will be the battle over data and their control, the guarantee of our technological superiority. But it can be followed very quickly by a battle with none or disrupted access to our data, making our systems inoperative.

Only nations with the strongest will are going to triumph, digitization or not, relying on more classic patterns of resilience, learned and practiced in training, by their soldiers.