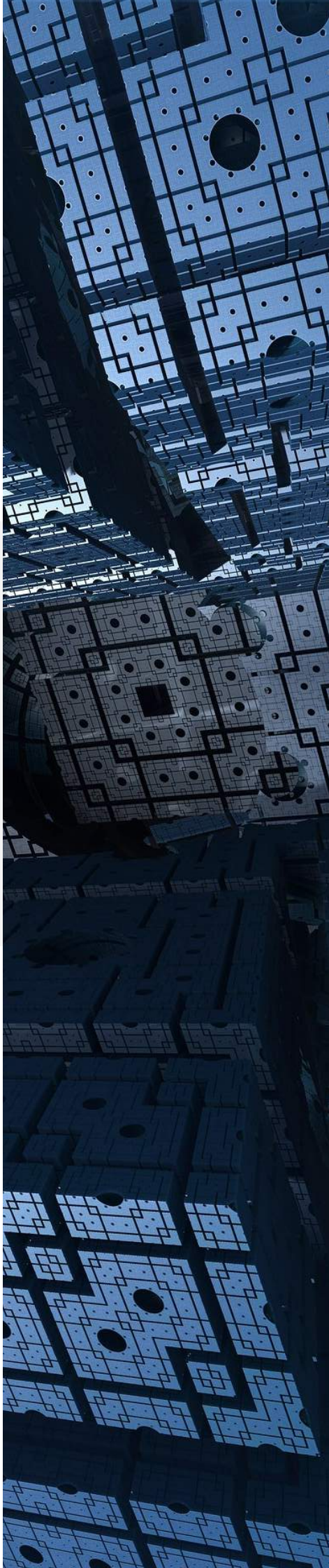
iesd
Institut d'études de stratégie et de défense
Faculté de droit
Université Jean Moulin - Lyon III



NOVEMBER 2020

Digitalization and Reticulation

The digital integration of armies, from tactical incorporation to strategic conjunction

Antony Dabila

RESEARCH PAPER

Analyse technico-capacitaire

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

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: Techno-Capacity 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

PACTE Enseignement supérieur MINISTÈRE DE LA DÉFENSE

UNIVERSITÉ DE LYON
UNIVERSITÉ LYON III JEAN MOULIN

RESEARCH PAPER

Antony Dabila, « Digitalization and Reticulation: The digital integration of armies, from tactical incorporation to strategic conjunction », *Notes de Recherche de l'IESD*, coll. « Techno-Capacity Analysis », n°6, November 2020 (originally in French, May 2020).

Abstract

The implementation of digital tools in the armed forces has led to upheavals at both an organizational and human level, which cannot be understood from a simple technical or technological point of view. For this reason, this paper focuses on conducting a human and sociological analysis centered on the process of "digitalization of armies" rather than analyzing cyber separate from the rest of the armed forces. This change of perspective makes it possible to identify several concepts that complement and enrich the analysis of strategic decision-making processes. From this point of view, the creation of tactical-level units dedicated to computerized warfare is only one necessary step in the "digital integration of armies", requiring the transformation and adaptation of all forces to the new digitized technical command and coordination system. It is; therefore, necessary to distinguish between "tactical digital incorporation" and "strategic digital conjunction" in order to complete an assessment of the armed forces' digital transition processes.

Résumé

La mise en place d'outils numériques dans les armées a entraîné des bouleversements organisationnels et humains qui ne peuvent être appréhendés d'un simple point de vue technique ou technologique. À l'hypothèse d'un milieu « cyber » distinct des autres fonctions des armées, nous proposons de substituer une analyse humaine et sociologique centrée sur le processus de « numérisation des forces ». Ce décentrement débouche sur plusieurs concepts qui permettent de compléter et d'enrichir l'analyse des processus de prise de décision stratégique. De ce point de vue, la création d'unités dédiées à la lutte informatique n'est sans doute que l'une des étapes nécessaires à une « intégration numérique des armées », laquelle nécessitera *in fine* une transformation et une adaptation de l'ensemble des forces au nouveau système technique de commandement et de coordination numérisé. Il semble dès lors nécessaire de distinguer « l'incorporation numérique tactique » de la « conjonction numérique stratégique », afin de remettre en perspective les dynamiques futures du processus de transition numérique des armées.

About the author

Antony Dabila is post-doctoral researcher at the Institute for Defense and Strategic Studies. His work is focusing on the transformations of the human environment formed by the combatants and how strategic thinking adapts to its evolution. He teaches strategy and defense policies at the University Lyon-III-Jean Moulin, Sciences Po Lyon and at the Institut Mines Télécom of Paris (IMT).

Table of content

Digitalization & Reticulation: The digital integration of armies, from tactical incorporation to strategic conjunction

Since the end of the Cold War, one of the most dramatic shifts in military operations has been, without question, the massive use of digital means of communication, observation and analysis by all the armed forces of the main military powers, whether they are global or regional in scope. For many analysts, this phenomenon led to the creation of a new "cyber" domain of warfare. This all-encompassing label poses several problems when it comes to understanding and anticipating the operational consequences of this transformation. In this paper, we hypothesize that it would, in many ways, be preferable to define this phenomenon in the context of a complementary tension between the digitalization of armies on the one hand and a dynamic of digital integration of forces on the other.

The objective of the following reflections is to underline the different conclusions to which the analyst of the military is led, depending on whether he considers the process of extensive introduction of information technology into combat as the creation of an additional "environment" or as a global digitalization of the military tool. In order to understand these differences, we will proceed with a comparison of the doctrines that presided over the implementation of digital means in the French armies and the American forces, the latter tending in fact to define the trends, both technical and conceptual, in terms of defense innovation.

The term "cyber", taken both as a prefix and as a noun, has imposed itself in the strategic discourse to designate the computer technology added to traditional means of defense. However, the word brings together very different fields of expertise, which deal with threats that were previously the responsibility of specialized state agencies. Let us take as an example the latest version, dated July 2019, of the French doctrinal document entitled *Stratégie Nationale du Renseignement* (National Intelligence Strategy), published by the French equivalent of the Director of National Intelligence and the "*Coordination Nationale du Renseignement et de la Lutte contre le Terrorisme*" (National Coordination of Intelligence and Fight against Terrorism). This service, which reports directly to the Presidency of the Republic, characterizes in this document the "cyber" threats as follows: "*the threat, whether it is from a State, private companies or clan organizations, has evolved considerably. It is of several types: data theft, sabotage to the detriment of companies and administrations, penetration for espionage purposes, blackmail with a view to obtaining a ransom, etc. It should be pointed out that some of these predation operations are now part of a new form of organized cybercrime*"[1]. The document adds that "[...] via the Internet and social networks, cyberspace is a vector for the dissemination of hate messages and the manipulation of information which deserves to be monitored, particularly in the field of fight against cybercrime, identification of messages or campaigns amplifying them, attribution of their origin and facilitation of their administrative and judicial hindrance"[2].

As we can see, this document makes extensive use of the prefix "cyber-", which it attaches to a cloud of disparate phenomena to give them substance. These disparate means of action, carried out by heterogeneous actors who do not necessarily have political aims, are grouped under the same category, requiring coordinated action and common services. However, if they did not use the internet, a worldwide computer network, as a common vector, these same actions would of course been carried out by information services divisions of both the police and the armed forces.

[1] « Stratégie Nationale du Renseignement », Paris, Coordination Nationale du Renseignement et de la Lutte contre le Terrorisme, July 2019, p.6.

[2] *Ibid.*

However, there is nothing evident in grouping these threats together in the same category and treating them uniformly by one or more dedicated state services. This leads to questioning the relevance of this categorization in addressing the phenomenon of digitalization of armed forces. We can now ask the question that will be addressed in this paper: **Is the phenomenon of partial digitalization of military confrontations limited to the creation of dedicated and functionally specialized units, or does it require, on the contrary, the implementation of digitized elements within each unit, in order to face, in a proportionate manner, the extremely diverse challenge of "cyber-threats"?** In other words, what is the most relevant mode of digital reticulation for the armed forces? The answer to this question depends on the strategy for the digital transformation of the armed forces, which could be to merge the various agencies into a new format designed to harness the potential of remote computer communications.

"Cyber" as a prefix was first used in science fiction in 1984 by the writer William Gibson[3] and spread rapidly after the World Wide Web computer network was fully opened to the public on January 1st, 1990. It tends to refer to the network created by the interconnection of data stored and produced by computers spread across the planet. This new informatic set up is sometimes described as a "space" in which it is possible to move around to "seize" and exploit data, regardless of where it is created or stored. Gradually, the term gained ground in strategic doctrines, especially after the influential article by John Arquilla and David Ronfeld, "Cyberwar is Coming!" published by the RAND Corporation in 1993[4].

What the emergence of this new vocabulary indicates to us is that this "*milieu*", the newest domain in military operations, should necessarily have corresponded to a new kind of warfare and strategy. Such a logic would in a way be the transposition of Admiral Alfred T.'s thinking. According to Mahan, a particular "space" of armed confrontation necessitates a specific strategy of action and deterrence, with its own rules. This broadening of strategy linked to the emergence of a new environment was rightly and convincingly applied to airspace during the First World War.

Since the Second World War, the same logic has gradually imposed itself in the space domain, with the first space race of the 1950s-1960s and, more recently, with the recent announcement of the creation of a US Space Force[5] and a Space Forces Command for France. Outer space now constitutes the fourth specific medium of warfare, although the appropriateness of a dedicated army (or "component") was strongly disputed[6]. It should be noted; however, that the submarine domain, although endowed with very different physical characteristics, is seen in a rather consensual manner as an extension of the maritime domain[7].

In a similar regard, it is also necessary to question whether it is appropriate to speak of a "digital space" entirely composed of electromagnetic waves and computer data as a domain in and of itself. This leads us to another question: does this "medium" have its own strategy? The conceptual work behind this question is not insignificant. The way of answering it will define a certain vision of the digital "area" and will; therefore, influence, in a very concrete way, the decision making in this field, since the scheme chosen for the digital defense architecture is the prerequisite for the digital transformation of forces.

---

[3] Gibson, William, *The Neuromancer*, New York, Ace Books, 1984.

[4] Arquilla, John & David Ronfeldt, *Cyberwar is Coming!*, Santa Monica, RAND Corporation, RP-223, 1993.

[5] Cf "Us Space Force Facts Sheet", December 19th 2019, Washington, Department of Defense, https://www.spaceforce.mil/About-Us/Fact-Sheet.

[6] Cf. McCain, John S., "National Defense Authorization Act (NDAA) for Fiscal Year 2019", Public Law n° 115-232, signed by D. Trump in august 2018.

[7] Coutau-Bégarie, Hervé, *Traité de Stratégie*, Paris, Economica, 2011 (7th edition), pp.725-6.

Indeed, beyond the question of a "fourth" branch for French armies (or a "fifth" if space forces become a reality in line with the recent American decision), the crucial point is to know how to integrate digital units into the fighting forces and, depending on the orientation chosen, to decide at which level of military organizational structure they should be placed and directed.

Corollary to the problem of comprehension of digitalization, this paper also seeks to address which level of military command is best suited as decision authority for cyber operations. The stake there is to streamline as much as possible the loop of orders and commands linking the tactical, operational, and strategic levels of military action. To answer these questions, we will examine the measures currently being applied in the French and American armies in terms of the digitalization of fighting forces[8]. This will allow us to observe whether this digital transformation of the military information architecture is really thought out on the pattern of an independent environment or as a digitalization of existing tools and the implementation of a new "technical set"[9] of communication strategies, transversal (or cross-sectional) to all other environments.

Remote computerized communications: a new source of transpolitical insecurity

The range of *agents* of the new "digital insecurity" has been steadily widening over the last twenty years: States, through their security and intelligence forces, terrorist and insurgent groups, criminal organizations, as well as malicious individuals seeking the near-sporting challenge of penetrating and degrading computer systems[10]. To summarize it succinctly, one could say the advent of computers, and then the Internet, has strengthened private actors in the transpolitical arena[11], while at the same time further diminishing the part played on it by the states.

It is all these aggressive behaviors by means of computer networks and operations aimed at defending themselves against them, that have been grouped together under the concept of "cyberwar". However, the term is contested by eminent specialists in this field. Eugene Kaspersky, founder of the cybersecurity company of the same name, challenges the very idea that digital conflict would symmetrically prolong the conflict of reality: "*The attacks we know today give no clue as to who committed them and whether they will hit you again. This is not cyberwar, but rather cyberterrorism*"[12]. The Russian specialist continues to refute the very term and concept by considering the status of the "weapons" with which this war would be waged. "*Cyberweapons can have boomerang effects. You can't catch a missile, take it apart, reassemble it and send it back; a cyber-attack can. You can copy it, modify it and send it back. It may not be easy, but it can be done. And it's much easier than building a missile, of course*"[13]. Once used, the very means of aggression can affect the computer security of the perpetrator. We are here in the field of security rather than defense unless we can identify which actors are involved. If not, the political specificity of war would then be lost.

---

[8] Rapport parlementaire Becht-Gassilloud n° 996 about the « Les enjeux de la numérisation des armées », Paris, Assemblée Nationale, may 2018.

[9] Selon l'acception de Gilbert Simondon, *Du Mode d'existence des objets techniques*, Paris, Aubier-Montaigne, 1958.

[10] "Field Manual 3-12 (R) – Cyberspace Operations", Joint Publications, *United States Department of Defense*, février 2013, p.19-20.

[11] If internal political space is defined by the existence of procedures of tendential pacification, space exterior to the political unit can be défined as a space of potential conflicts. It is this space, where political units (or "polities") are virtualy at war, that we name "transpolity". The derived adjective is « transpolitical ». Cf Jean Baechler, *Nature et Histoire*, Paris, PUF, 2000, pp.80-93

[12] "Latest Viruses Could Mean 'End Of World As We Know It,' Says Man Who Discovered Flame", *Times of Israel*, 6 juin 2012.

[13] Kaspersky, Eugène, « Cyberguerre : "il n'y a aucune preuve" selon Eugène Kaspersky » in *Usbek et Rica,* 29th june 2019, Consulted on the 10th of july 2019, https://usbeketrica.com/article/cyberguerre-il-n-y-a-aucune-preuve?fbclid=IwAR1PZybPmU6qyr520VafxmbC3SSXL0qxPOElOhEP-uh9UeUGooIKtIfqohk

An important characteristic of cyberattacks; therefore, lies in the fact that they can only be attributed in a fastidious and uncertain manner, long after the action has taken place[14]. Some groups can thus hide their real objectives behind false and unverifiable claims. For example, the actions of "hacker" groups may be hijacked or supported covertly in order to carry out intellectual property theft or to destabilize a competitor. On another level, Russia has been able to take advantage of "spontaneous" attacks by hacker groups in its international actions against Estonia in 2007, Georgia in 2008 and Ukraine in 2014. All of them contributed to achieving the political objective of these operations: to punish the Estonian government's lack of respect for the Soviet soldiers of the Second World War and to disorganize the armed response of the governments of Tbilisi and Kiev.

As a consequence of this impossibility - or great difficulty - of attributing the attacks, the nature of the confrontation is not comparable to conventional warfare, with well-established lines of contact and period, or even to guerrilla warfare seeking to undermine the political order and show its weaknesses. It is a diffuse and permanent conflict, in which no state of peace will succeed a state of war. The politically motivated actions are only episodes of greater intensity, amidst constant attempts to circumvent the defenses laid out around the data and the infrastructures making up the network. According to Eugene Kaspersky, quoted above, this is ultimately a kind of "digital hygiene programs" rather than a security policy targeted at specific groups: "Traditional security is not able to solve this problem. I think we need to move from cybersecurity to what I call cyber-immunity. We need to design a new IT architecture so that it is much more complicated, if not impossible, to hack"[15].

This vision, which does not limit digital defense to its security dimension, calls for the architecture for data flow and security to be built on the basis of other fields of expertise, such as medicine: "Today," Kaspersky concludes, "we are adding layers of protection to an already existing architecture. Wouldn't it be simpler to implement secure solutions at the design stage? [...] Around us, we know that there are a lot of microbes that gravitate around us, and they don't reach us because we are more or less immune. Every once in a while, we get a cold. Right now, the systems that are connected are not immune, because they're not designed for it. For them to be, they have to be redesigned. It's going to be a long job. We've already come up with a solution of cyber-immunity for the Internet of Things"[16].

However, the agents of the new "digital insecurity" are indeed a threat and are already full-fledged players in the "physical" or "kinetic" battles between armed forces. This diffuse and very diverse threat was not (or hardly) within the competence of the armed forces before their "digitalization", but rather that of civilian intelligence agencies. It was only as these threats entered the battlefield, interacting with physical devices or stealing information useful for the conduct of combat, that their true scope was gradually grasped. However, while the challenges facing armies are becoming more tangible, the place of digital combat in the conduct of warfare is not fully specified, even on a five- or ten-year horizon.

This unpredictability of evolution is due to two specific characteristics of digital confrontation: the constant effective use of techniques that allow the penetration and damage of opposing networks, as well as the intrinsic rapidity of the evolution of these techniques. Contrary to field of atomic weapons or air power, where the unit of time is a decade rather than a year, the acquisition cycle of new technologies tends to be measured in months, as General Nakasone, commander of the US Cyber Command since 2018, points out: "*Unlike the nuclear realm, where our strategic advantage or power comes from possessing a capability or weapons system, in cyberspace it's the use of cyber capabilities that is strategically consequential.*

[14] Kempf, Olivier, *Alliances et mésalliances dans le cyberespace*, Paris, Economica, 2014.

[15] Kaspersky, Eugène, « Cyberguerre : "il n'y a aucune preuve" selon Eugène Kaspersky », *op. cit.*

[16] *Ibid.*

The threat of using something in cyberspace is not as powerful as actually using it because that's what our adversaries are doing to us. They are actively in our network communications, attempting to steal data and impact our weapons systems. Therefore, advantage is gained by those who maintain a continual state of action. [...] When we buy a capability or tool for cyberspace, we rarely get a prolonged use we can measure in years. Our capabilities rarely last 6 months, let alone 6 years"[17].

Since the invasion of Crimea and the formation of the Islamic State, the last six years have made it possible to clarify the place the use of new generation computer technologies tends to occupy in the military domain. Previously difficult to predict, the concrete use of new technologies within the battle space has become much clearer since the Arab Spring Wars and the Donbass War. These conflicts were led by underfunded insurrectional groups forced to use new strategies and tactics to fight against their enemies in the absence of a well-established doctrinal corpus and the lack of a state army supported by heavy equipment[18]. In particular, the war in Syria and Iraq provided the opportunity to observe the operational consequences of a generalization of the use of digital means in multiple domains (command, communication, reconnaissance, information, propaganda, recruitment, claims, etc.).

The determination of modern insurgent groups to take advantage of benefits from new cheap communication technologies in order to do maximum damages with minimum budgets is on par with the strategic line of the *Global Islamic Resistance Call* published in 2004 by Al Qaeda strategist Abu Musab al-Suri[19]. As a result, this desire has turned the confrontations of the Syrian civil war into a "laboratory", where observations can be made on the role of new digital technologies in this new type of warfare[20]. Thus, the way in which digital technologies are being implanted in all dimensions of the conflict showcases the underlying logic of digitalization of combat instruments to obtain political effects on the international scene.

In the field of civil security, the so-called "Wannacry" episode, which blocked part of the London hospitals in May 2017, has raised awareness of the scale of a coordinated attack and its potential consequences on the daily life and economy of European countries, including the most militarily powerful. The recent Iranian attacks on the Israeli water supply network and the Hebrew reprisals on the port of Bandar Abbas further illustrate the potential scale of digital sabotage[21]. What would have happened if these blockades had occurred during an episode of tension, such as the COVID-19 crisis, or during a confrontation? In any case, the blockage of the Shahid Rajaee terminal shows that supply chains could be greatly impacted by a digital assault.

Ultimately, it seems that we are witnessing an accelerated digitalization of the weapons used to wage war, sometimes combined with an automation of certain violent devices. This natural evo-

[17] Interview of general Nakasone in *Joint Forces Quarterly,* n° 92, 1st trimester 2019, pp.4-9. "*Unlike the nuclear realm, where our strategic advantage or power comes from possessing a capability or weapons system, in cyberspace it's the use of cyber capabilities that is strategically consequential. The threat of using something in cyberspace is not as powerful as actually using it because that's what our adversaries are doing to us. They are actively in our network communications, attempting to steal data and impact our weapons systems. So advantage is gained by those who maintain a continual state of action. [...] When we buy a capability or tool for cyberspace we rarely get a prolonged use we can measure in years. Our capabilities rarely last 6 months, let alone 6 years*".

[18] "Strategic Cyberspace Operations Guide", US Army War College, Carlisle, Pennsylvania, juin 2016, p.9.

[19] Brynjar, Lia, *Architect of global Jihad*, London & New York, Hurst &Columbia University Press, 2008.

[20] Andress, Jason & Winterfeld, Steve, *Cyber Warfare. Techniques, Tactics and Tools for Security Practitioners*, Amsterdam, Syngress, 2011, p.5.

[21] "Israel Behind Cyberattack That Caused 'Total Disarray' At Iran Port" in *The Times of Israel*, May 19th 2020, https://www.timesofisrael.com/israel-said-behind-cyberattack-that-caused-total-disarray-at-iran-port-report/?fbclid=IwAR0QCZ2XzYBOCzNw8yWUqdHfsf71U7_cl9rHS3HsmjMI4uvmgUhBAwC19E4

lution in arms technologies is nevertheless surprising by the suddenness of its spread. Driven by the fast democratization of these technologies and the obvious benefits that "techno-guerrillas" derive from them, but also by the race for technological mastery between great powers (especially for “high strategic capabilities”), the digitalization movement concerns all fields and all components. All this suggests that we do not ultimately see the creation of a separate digital war space, but rather the establishment of instruments for the production and communication of information forming a new digitalized communication space.

Following a term proposed by Jean Baechler, it seems useful to consider this space as a new type of "agory" (from the Greek “*agora*”). This term describes a space where communication and the exchange of information are allowed and conditioned by their social and technical determinants[22]. This "agory" takes place within the new "global digital agory" created by remote computer communication, the most well-known manifestation of which is the Internet. We thus propose to speak of the social space created by the irruption of tools of this kind in the war confrontation as a new "**military digital agory**", whose very existence, and the possibilities it contains, necessarily modifies the nature of the military confrontation. In fact, according to Clausewitz's second "reciprocal action", war is defined by the impossibility of controlling the means by which combat is carried out, for the adversary dictates his law to me as I dictate mine to him[23]. Therefore, the "military numerical agory" is bound to be used by one of the opponents if it allows any advantage and rebalances the confrontation in its favor. As a potential source of sudden tactical and strategic revolutions, digital technical means of warfare (and not only on the battlefield) must therefore be thought out and their evolution anticipated in order to avoid military surprise[24].

The new military digital agoria: integration, incorporation and convergence

The hypothesis supported here on the nature of "cyberwar" thus finds its contours: the overuse of words composed from the prefix cyber- (cyberwar, cyberspace, cybersecurity, cyberthreat, etc.) has led to an unfortunate expansion of the concept[25]. This inflation is damaging because it prevents armies from focusing on their primary mission, which is, under the self-rule of political power, to use force or the threat of force to protect the territory and the people of France from the ravages of armed violence. However, as Thomas Rid states in his book *Cyberwar Will Not Take Place*, the idea of cyberspace as the "fifth domain of war" is a metaphorical term, mainly used by the US Air Force since 2005[26]. Therefore, referring to all hostile or malevolent digital activities as "cyber war" prevents us from seeing a major fact: the use of the Internet for espionage and sabotage has narrowed rather than expanded the realm of war. Indeed, according to Rid, digital attacks "[...] achieve a goal that would previously have required the use of a certain amount of political violence”[27]. There was; therefore, less extension than substitution. The choice of an insufficiently precise concept has led to a confused understanding of the reality of cyber warfare. This has proved harmful in the implementation of public policies aimed at providing the State with bureaucratic bodies in charge of the digitalization of its defense.

Because of this inadequacy of the terms derived from "cyber-", perhaps it would be preferable to re-

[22] Baechler, Jean, *Nature et Histoire*, Paris, PUF, 2000, pp.148-160.

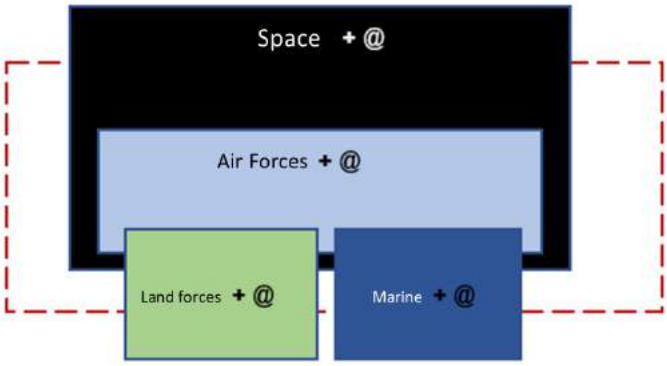
[23] Cf Clausewitz, *De la Guerre*, Paris, Editions de Minuit, 1955, Livre I, Chapitre 1, p.52-54.

[24] That was also the case for the previous Steele and Stein revolutions. In their article on the weight of the evolution of communications on the structure of the international scene, Steel, Cherie & Stein, Arthur, "Communications Revolutions and International Relations", in Juliann Emmons Allison (dir.), *Technology Development and Democracy: International conflict and Cooperation in the Information Age*, Albany State University of New York Press, 2002, pp.32-35.

[25] For an illustration of the intensive use of prefixe « cyber », see *infra* and the chapter « The organizational and human challenge of digitalization », p.19 of this study

[26] Rid, Thomas, *Cyberwar will not take place*, Londres, Hurst, 2017 (2nd ed.), p.165.

[27] *Ibid.*, p.167.



fer to the phenomenon of digital transformation of combat capacities of the simple concept of "digitalization of armies". This process has several facets, which need to be distinguished.

- On the one hand, the setting up of units dedicated solely to computer combat and the protection of infrastructures, servers, and data. Although cyber warfare is often reduced to these creations, they represent only the first, necessary step in the digital transition of armies.
- On the other hand, and as a second step, we need to consider a phenomenon which, in our view, is even more crucial in terms of the use of political violence. This is the setting up of a communication and transmission network for the data necessary for combat within the fighting units themselves. This phenomenon could be called ***digital integration***[28].

A classical division of military thinking divides between the tactical and strategic levels, i.e. between the actual use of force and the provision of the resources necessary for the use of that force[29]. This dichotomy is still relevant for thinking about the numerical integration of armies, although it brings with it an inevitable confusion about the precise dividing line between the two levels. As Clausewitz demonstrated, any tactical action can indeed have a strategic dimension, and vice versa[30].

In accordance with this division, it may be necessary to distinguish more than is currently the case between the digitalization of the tactical and strategic levels. The first one insists on the transformation of the combat itself and on the participation of digital tools in the actions of force, while the second emphasizes the global character of the mutation, which concerns all the power tools of armed forces, but also their intelligence, command and coordination capacities.

In order to translate these two phenomena into distinct concepts, which it is imperative not to confuse, we propose to name them **digitalization of tactical (combat) devices** and **digitalization of strategic (command) tools**.

Because of the impossibility to separate the two levels perfectly, we make this distinction in the knowledge that most concrete actions will frequently cross the barriers between these two processes, navigating in a kind of "digital glacis" at the operational level, which will allow the tactical and strategic levels to communicate. This tactical-strategic dichotomy is more of a tool to better situate and thus interpret concrete situations, rather than a rigid separation of two disjointed entities, whether in planning or in execution. The result is that a set of numerical operations belongs to both levels[31].

But this should not mask what these concepts allow us to highlight: the increased ability of armies to converge their forces on selected points of the opposing apparatus and to concentrate the avail-

[28] See our contribution on this term in our article « Les évolutions du paradigme cyber : de la 4e armée à l'intégration cybertactique », in *Revue Défense* Nationale, n° 806, janvier 2018.

[29] See Dabila, Antony, « L'Engagement militaire : essai de sociologie comparée », PhD thesis defended at the University of Paris-Sorbonne, 5th November 2013, specially the chapter « Disposer et Mettre à Disposition », p.89. https://www.theses.fr/2013PA040132.pdf

[30] Clausewitz, *De la Guerre*, Paris, Editions de Minuit, 1955, livre V, chapitre 2, intitulé « Armée, Théâtre de Guerre et Campagne », p. 307.

[31] On the notion of « digital glacis », see Boyer, Bertrand, *Cybertactique, conduire la guerre numérique*, Paris, Nuvis, 2014.

able strike power there thanks to the unprecedented possibilities offered by remote computer communications. These allow the various elements constituting an armed force to be more and more integrated and thus to produce multiplied effects, with fewer means, while striking the most exposed points of the enemy's apparatus at a given moment[32].

We will finally opt for the term **numerical integration of armies**, while separating, as the diagram above suggests:

- **tactical digital embedding** (Army x + @) and
- the **strategic numerical conjunction** (represented by the "numerical ring" in red).

While the digitalization of armies, which is based on successful joint digital integration, is bringing clear benefits, it is also revealing new weaknesses that could completely paralyze them. These benefits are particularly important in the area of command. However, if this critical function is attacked digitally, it risks paralyzing the entire integrated joint system. The opportunities of digital technology thus carry their antithesis in them, because while increasing the performance of command systems and the potential virtuosity of operational "conductors", they also open back doors that allow us to get to the very heart of the military systems that have staked everything on this same digital integration.

Through this dual concept, we seek to better describe the transformation process from new digital communication and analysis devices to combat functions[33], leading to the establishment of a *communication and coordination system*[34] that relies primarily on remote computer communications. The aim of this system is to shorten the time required to produce and propagate information while its characteristic feature is to digitize the entire transmission of orders within armies and to automate as much as possible the processing and circulation of data on the adversary and on oneself.

In doing so, the tactical and strategic levels are gradually being brought closer together, to the point where the perception of their demarcation line is being questioned. Of course, the interference of the strategic level in the tactical level is much stronger than the other way round. It is the so-called "strategic micro-management" threat that is a reality in today's Command & Control centers[35]. This situation must be taken into account when designing the next digital communication and coordination systems, in order to decentralize the execution of operations as much as possible, while maintaining the capacity to centralize information for the command.

This way of understanding the digitalization of the military tool is opposed to the desire to give the "cyber threat"[36] a global character. If we consider that the task of armies is to ensure the security of citizens and the State in the whole spectrum of computer exchanges at the global level, the inevitable consequence will be to expand the field of action of the armed forces and make them miss the main goal imposed on them by the global technological change: to digitize their own military tools for precise operational effects centered on adversaries who seek to fight them. Digitizing the armed forces does not go without careful consideration of the division of labour between the army, the police, and the intelligence community, as well as, of course, the sharing of information between these

[32] See for example the new doctrine entitled « Mosaic Warfare », published by the DARPA and written David Deptula. See « Restoring Americas's Military Competitivness: Mosaic Warfare », by David Deptula and Heather Penney, with Lawrence Stutzriem & Mark Gunzinger, Arlington (Virginia), The Mitchell Institute for Aerospace Studies, september 2019.

[33] Porche, Isaac R. III & Colin, Clarke P., *Tactical Cyber: Building a Strategy for Cyber Support to Corps and Below*, Santa Monica, RAND Corporation, Aroyo Center, 2017.

[34] We prefer this term to "command and control," which is less explicit, especially transcribed as it is in French.

[35] See Deptula, « Mosaic Warfare », *op. cit.* 2019, p.22.

[36] This term mis very is often used in the Defense French White Paper of 2013.

Command and Control Center of the Swiss Air Force, a good example of digital strategic conjunction.
Image: Keystone

three entities. This implies, even if this approach goes against the discourse imposed since 2008 on the defense-security continuum, to distinguish between the tasks of defense and those of security without separating them.

The extensive vision of the cyber threat or cyber-conflictuality is surely a pertinent argument strategy to convince the hierarchies in place to devote substantial credits to new technologies, which may have seemed at first as simple "gadgets" in the face of traditional or "kinetic" weapons. This way of presenting, in a worrying light, the potential hostility of digitalization to legislators and public opinion has certainly been useful within competing bureaucracies to gain a bigger share of budget[37].

Despite these perfectly classical justifications from the point of view of political analysis, it seems urgent today to reformulate the nature of the digital challenges facing the French armed forces. The dangers arising from the Internet and communication between computer networks are well understood and no longer need to be "oversold" to the public and lawmakers[38], particularly since the establishment of COMCYBER, to which we shall return later. Let us simply note that COMCYBER has been positioned within the General Staff of the Armed Forces, and not as a "4th Army".

The term "cyber" belongs to another age of the computer epic. Like other even older suitcase words (who still uses "technotronics", which was very much in vogue in the 1970s?), it might be rele-

[37] In France, the roles are distributed to DGSE (Foreign Intelligence), l'ANSSI (Computer Services Security Agency) and ComCyber (Military Cyber Intelligence).

[38] Iasiello, Emilio, "Are Cyber Weapons Effective Military Tools?" in *Military & Strategic Affairs*, vol.7, n° 1, mars 2015.

vant to present it at least as a catch-all and encompassing prefix. No one today would say Google or Apple are "cyber-companies" or that they work in the "cyber" industry. They are digital and computer technology companies, inventing and selling solutions to acquire, process, and share computer data[39]. This is precisely the task that armies must carry out in their missions, namely, to defend French interests by force when groups threaten them with violent political demands. The rest is the responsibility of the police, in the case of criminality, and of non-military intelligence services in the case of threats of potential violence (for example, interception of terrorist groups) and activities endangering the national interest. A methodology has yet to be developed to calculate the costs and benefits of implementing digital technology packages within existing weapon systems.

Multiplicity of digitalization models: digital integration & *path dependence*

Digital integration of armies can be more accurately defined as the bringing together of all levels and milieus of warfare, to enable the components of armies to fight in a more coordinated manner than was previously imaginable with analogue systems. It is not a question, in the perspective of this note, of diagnosing the birth of a new space, but rather of appreciating the consequences of the formation of a transversal set of technical tools, allowing for a better "tying" of the environments where confrontations take place and a better coordination of maneuvers. It is precisely this new form of integration that is currently referred to as "multi-domain operations" in official American and French doctrine documents[40], even if this term still covers a wide variety of meanings for the moment. All the emerging properties of this unedited intricacy of the different strategic milieus (or "domains") have not yet been explored and will no doubt be the source of future "strategic surprises"[41].

To be effective, such systems of communication and coordination must be thought for concrete military needs. They are not only very sophisticated technical systems, used by the best technicians in a remote production line. They must be suitable tools used in action. One of the main challenges of their successful implementation; therefore, lies in their coherence with the army model on which this "technical set[42]" is grafted. There is no singular model to follow, but a multiplicity of solutions, the best of which will be the one that responds to the following three requirements:

- to fight more effectively;
- secure a new system;
- reduce the cost and duration of the transformation[43].

[39] Another term very much in vogue in France during the 1980s was "telematics", a term born of the contraction of telecommunications and computing under the pen of Simon Nora and Alain Minc, in a notable report written in 1978 about "the computerization of society". Associated with the Minitel era, the word disappeared completely with the advent of the Internet and the disappearance of the French terminal in 2001. See Mathelot, Pierre, *La Télématique*, Paris, PUF, coll "Que sais-je", 1982. The disappearance of the term can be interpreted as a consequence of the lack of anticipation of an open and totally decentralized network, to which it is possible to connect through several types of terminals. This is the opposite of the technical vision of the Minitel, a closed, centralized network that could only be accessed with a single device, which has changed very little in its twenty years of existence. From this point of view, the term "cyber" corresponded better to the Internet era than "telematics".

[40] See the document which first used this concept : *FM 3.0, Operations*, Washington, Headquarters Department of the Army, October 2017.

[41] Bott, Jonathan W., "What's After Joint? Multi-Domain Operations as the Next Evolution in Warfare", United States Air Force School of Advanced Military Studies, Fort Leavenworth, 2017. See also the field manual of French Army, *L'emploi des forces terrestres dans les opérations interarmées* (DFT 3.2 Tome 1 [FT-03]), 1er juillet 2015. The concept of « cross-domain coordination » (p.35), allowed by digital tools, is used to describe that phenomenon.

[42] All the concepts in quotation marks are taken from the seminal work of Gilbert Simondon, *Du Mode d'existence des objets techniques*, Paris, Aubier-Montaigne, 1958 (english translation *On the Mode of Existence of Technical Objects*, Minneapolis, Univocal Publishing, 2016).

[43] "Strategic Cyberspace Operations Guide", *United States Army War College*, Carlisle, Pennsylvania, June 2016.

Ultimately, the transition to a digital technical model must allow armies to improve their combat functions by ensuring as few digital vulnerabilities as possible appear and by optimizing the resulting "transaction cost"[44].

The challenge of digitizing the military apparatus aims at adapting new technologies to existing military systems in the best possible way. One way would be to start from the concrete experience of the users of the finished product (the user experience, i.e. the military itself) so that the technology put in place to accomplish a specific task really maximizes the new operational possibilities while minimizing the "transaction cost" (i.e. in this case, the amount of energy required to implement and learn the new techniques). To consider this phenomenon, it is no doubt necessary to bear in mind the digitalization and networking of forces is subject, contrary to what one might intuitively believe, to a very powerful path dependency effect. The cost of the new technologies must be evaluated based on the "transition cost" from the previous state of the system, and in particular the cognitive cost for the end users, i.e. the military[45].

To be even more precise, we could say that the imposition of a new digital "technical set" for communication and the incorporation of "elements" and "technical individuals" within pre-existing sets is necessarily incremental[46]. It must; therefore, consider their characteristics and limitations in order to define a transformation strategy that maximizes improvements, but without exploding costs. This is what armies call *retrofitting*, i.e. adding new technologies to old equipment. The amount of effort required to move the system from one state to another conditions the degree of digital agility and technical versatility of armies. Taking better account of these parameters in the preparation phase for a unit digitalization could save time and improve efficiency. The reduction of transaction costs through the reduction of the design cycle could be achieved by adopting a more agile, "spiral" development model[47], integrating the user experience from the outset.

A very characteristic example, the modernization of the American B-52 and the Russian Tupolev-95s resulted in a modernization of the navigation system thanks to new tools ("individuals" in Simondon's language). Designed in the 1950s, these two models of long-range nuclear bombers were "digitized" and connected to the technical systems of their respective armies by means of a new digital transmission system, quite different from the analogical transmission system of the Strategic Air Command. Another relevant example here would be the Abrams M1 tanks, which have been constantly upgraded since their entry into service in 1981. The latest update, named M1A2, concerns the implementation of control and communication systems The U.S. Army is looking to equip this highly robustly engineered and designed tank with the means to participate fully in the digital battle ahead, without scrapping the hundreds of tanks the U.S. Army has at its disposal[48].

---

[44] According to the concept coined by Ronald Coase in *The Nature of the Firm* (1937). The economic theory considers the costs of « policing and enforcement » as transition costs. Cf Dahlman, Carl J., "The Problem of Externality" in *Journal of Law AMD Economics,* n° 22, vol.1, 1979, pp.141–162.

[45] Kurti, Erdelina & Haftor, Darek, "The Role of Path Dependence in the business model adaptation: from traditional to digital models", Proceedings of the 2014 Mediterranean Conference on Information Systems, Paper 28. It should also be noted that these costs should not be overestimated, by choosing technologies that are too simple, adapted to today's soldiers, but which will be insufficient for the future recruitments (the rotation speed of the workforce being faster in armies than in a company or an civilian administration).

[46] Gilbert Simondon, *On the Mode of Existence of Technical Objects*, *op. cit.*

[47] Cf Boehm, Barry, "A Spiral Model of Software Development and Enhancement", in *ACM SIGSOFT Software Engineering Notes*, ACM, n° 11, vol.4, pp.14-24, août 1986. Le modèle de développement en spirale, fondé sur l'expérimentation précoce et le prototypage, est d'ailleurs né dans la gestion de projets complexes dans le domaine informatique et de la mise au point de logiciels.

[48] Gouré, Daniel, "The M1A2 Abrams Is The Tank Of The Future", *The National Interest*, 3 novembre 2018 (https://nationalinterest.org/blog/buzz/m1a2-abrams-tank-future-35067?fbclid=IwAR3s0r7COu77roRCQcMsanovowdslEskkp0BnwfSVDvvBnQ7EymF2IUah8s)

Similarly, the SCORPION program to modernize the French Army's armored vehicles includes a retrofit of the Leclerc tanks, in a version called XLR. The armored vehicles, which entered service in 1997, will be fitted with brand new encrypted communication capabilities: the Scorpion Combat Information System (SICS) and "Vetronics"[49], which will enable it to communicate with the other vehicles in the new range (Griffon, Serval, Jaguar) in a secure manner. This approach corresponds to the complementary concepts that the French Army refers to as "info-valuation" and "collaborative combat"[50].

Conceptually distinct, these two objectives are aimed at producing knowledge in the form of data for one and improving maneuvering for the other. However, they ultimately depend on the quality of the capture and transmission of digitized information and therefore on the efficiency of the data architecture. Has the art of operation become a simple function of the quality of digital tools? On the contrary, it is the quality of digital tools that is measured by the possibilities of maneuvering and command they allow. The ability to command with a certain degree of freedom must; therefore, be thought out and integrated right from the design of the military digital technical object.

According to this new need for a high volume of information, one of the main current limitations is the insufficient bandwidth for data exchange in the sensor/C2/effector circuit. The transmission capacity is indeed often saturated on systems designed before the year 2000. The SCORPION Combat Information System (SICS) gives, in this perspective, a broad widening of French armed forces' bandwidth in order to enable sizeable enough data. This allows a tighter tactical integration while making the Command & Control of tanks easier, including shared target acquisition. Freed from a technical constraint, the maneuver becomes more agile, faster, and more unpredictable.

The French Army expects this overhaul to provide a real increase in power by updating its numerical communication and coordination system. It will also make them more independent from allies (most importantly from American capacities). As an example, all units equipped with SCORPION's communication system, called "Synthèse Tactique" (SYNTAC, or Tactical Synthesis), will be able to share a carto-graphic vision of the environment and the adversary through augmented reality[51]. Playing the card of innovation and information sharing to the full, some versions could even house reconnaissance drones to increase visibility on the battlefield in order to send data collected with the more fragile units that have to stay away of the frontline[52].

Hence, the same number of armored vehicles will produce more power thanks to the concentration of fire resulting from SYNTAC, while maintaining a physical dispersion limiting vulnerability. This is a textbook case of digital incorporation and conjunction based on the retrofitting of old equipment and the incremental addition of new elements within a technical system redesigned for information sharing.

Problems and dilemma of the battlespace digitalization

This advanced digital integration is the result of a process of reflection that has been underway for several years, particularly since the French 2008 White Paper of Defense. The French military has also been challenged by the very rapid progress of digitalization in a tight budgetary context, characterized by a constant decline in budgets since the end of the Cold War until the shock of the attacks of 2015. Issues following the introduction of a digi-

[49] Short form of Vehicules Electronics

[50] See Paul, Philippe, « Notions sur le combat collaboratif et observations récentes des expérimentations », in *Pensée Militaire Terre*, Paris Centre de Doctrine et d'Enseignement du commandement, June 2019, p.1.

[51] *Ibid.*, p.52.

[52] Lagneau, Laurent, « Nexter prépare une version du char Leclerc capable de mettre en œuvre des drones aériens », in *Zone Militaire* 21 février 2019. http://www.opex360.com/2019/02/21/nexter-prepare-une-version-du-char-leclerc-capable-de-mettre-en-oeuvre-des-drones-aeriens/.

tal communication and coordination system[53] were already raised in the 2008 and 2013 editions of the White Paper and was again addressed in the Strategic Review published in October 2017[54].

Formulating a digital strategy for French armed forces as early as 2008, the White Paper invoked the concept of "Lutte informatique offensive (LIO, or Offensive Informatic Combat)", which should have enabled France to respond to digital attacks. Above all, it proposed, thanks to an adequate combination with kinetic forces, to multiply the effects of conventional force and to lower the costs of its production. "*The effectiveness of defense and security forces at all levels depends and will increasingly depend on the proper functioning of their information systems. The planning and execution of operations combined with cybernetic actions are becoming the norm. Even before physical targets are destroyed, any defense system can be [...] disrupted and partially blinded by silent, targeted strikes*"[55].

Note the early abandonment of the prefix cyber- to describe these operations, which are not "virtual" at all, since they are a direct part of the military effort and are intended to minimize the danger faced by soldiers. The technical problems of such an implementation of digital combat capabilities were already mentioned, but without addressing the question of the actual command of these missions. Even if entanglement was necessary, the idea of a direct contribution to forces "in the last tactical kilometer" was not yet addressed.

The White Paper of 2013, on the other hand, placed great emphasis on the creation of a "cyber threat" and more clearly evoked the idea of integrating digital capabilities into the armed forces. The White Paper, which clearly defined the field of criminality and the mission of protecting the State, noted the interdependence of certain private interests and those of the political community, and consequently gave an extensive version of the task of the armed forces: "*Attempts to penetrate digital networks for espionage purposes, whether they target State or corporate information systems, fall within the scope of national security. An attack aimed at destroying or remotely taking control of computerized systems that control the operation of vital infrastructures, automated management systems for potentially dangerous industrial tools, or even weapons systems or strategic military capabilities could thus have serious consequences. Cyberspace is therefore now a field of confrontation of its own*"[56].

Although one part of hostile and malevolent threats is separated from the law enforcement side, the "cyber threat" continues to be an extremely broad area. The real tactical and operational change brought about by the new information dissemination capabilities was not analyzed per se, but through the connection between intelligence and headquarters. Anchored in the "theory of the five environments" (land, air, sea, outer space and cyberspace), French strategic thinking thus came up against the definition of objectives relating to the introduction of the new digital tools within the battle space constituted by the four environments that "cyber" actually effects. It confines the mission to the will to "[...] acquire and maintain operational superiority over our adversaries"[57] and specifies that "coercive engagements"[58] must be "conducted in a

[53] Equivalent for the armed forces of SCADA systems (Supervisory Control And Data Acquisition) used in industry, allowing to monitor a complex set of inert technical objects. The difference for the armed forces is that they must control animated and autonomous beings, facing enemies who are themselves autonomous and inventive. The two activities cannot therefore be thought with the same conceptual framework.

[54] *Revue Stratégique*, Paris, Secrétariat Général à la Défense et à la Sécurité Nationale, October 2017, see in particular Part 1, title 4, « Des ruptures technologiques et numériques », pp.33-37.

[55] *Livre Blanc de la Défense et de la Sécurité Nationale*, 2008, p.207. It was the case during israélian offensive on the nuclear facilities of Syrian regime of Deir-ez-Zor in 2007. Radar systems were remotly disabled, allowing Israelian Air Force to destroy its target without any possibilities to be struck.

[56] Livre Blanc de la Défense et de la sécurité Nationale de 2013, p.45.

[57] *Ibid.*, p.84.

[58] *Ibid.*

coordinated manner in the five domains"[59]. Such a vision presupposes, in an approach that can be described as Mahanian, the constitution of forces specific to the new domain, on the pattern of the Navy and the Air Force, well separated in budget and hierarchy from the Army.

However, the creation of a "4th Cyber Army" is arguably not the appropriate way forward[60]. Indeed, it is by no means possible to compare the air or maritime domain to "cyberspace". The first two are geographical environments that require a technical system that can be developed there, while the computer environment is a completely new "technical unit" that can be adapted to all other environments and deployed anywhere while the other environments remain clearly separated from each other.

However, the question of command was raised in the 2013 White Paper. At that precise moment in the French strategic debate, it revealed a real intellectual tension between those in favor of a fully-fledged, but separated environment and those in favor of better integration and synchronization of the armed forces thanks to digital tools and the very rapid use of intelligence data: "*The development of military cyber defense capabilities will be the subject of a marked effort, in close relation with the intelligence field*", the document states for the time. "France will develop its position based on a cyber defense organization that is closely integrated into the forces with defensive and offensive capabilities to prepare or accompany military operations. The operational organization of the armed forces will, thus, integrate an operational cyber defense chain of command that is consistent with the operational organization and structure of our armed forces and adapted to the specific characteristics of this area of confrontation"[61]. To conclude, the document states that this digital "*operational chain*" must be "*centralized from the operations planning and control center of the Armed Forces Staff, in order to guarantee a global vision of the entry and rapid mobilization of the necessary resources*"[62].

These doctrinal conceptions are the yardstick against which the changes that have taken place in the organization of the armed forces over the past decade or so must be assessed. They all point in the direction of a digital interlocking of the various units and an increasingly rapid collection and transmission of information between units, rather than in the direction of a "4th cyber army" organically added to the Army, Navy, and Air Force, as we shall now see.

The organizational and human challenge of digitalization

France has gradually equipped itself with the institutional means to ensure its digital security, which is threatened by the multiplication of hostile actions carried out by various transpolitical actors reinforced by the new digital "agory". The identification of new threats first resulted in the creation of new structures to oversee the security effort in the IT field, such as the ANSSI in 2009, or the Cyber Defense Citizen Reserve in 2012. To these were added, since 2016, the "Commandement des Systèmes d'Information et de Communication" (abbreviated to COMSIC), placed under the leadership of a single officer, with 4,750 military personnel and 150 civilians[63], the 807th CTRS brigade (specializing in communications), and the cyber-defense operational reserve. Finally, the COMCYBER ("Cyber Command"), which oversees all digital processes within the three armies, was established in January 2017 within the Army Staff, thus, ruling out the creation of a specific army.

[59] *Ibid.*

[60] Gartzke, Erik, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth" in International, Security, vol. 38, N° 2, Fall 2013, pp.41–73. Singer, Peter & Shachtman, Noah, "The Wrong War: The Insistence on Applying Cold War Metaphors to Cybersecurity Is Misplaced and Counterproductive", Brookings.com, August 15th 2011.

[61] Livre Blanc de la Défense et de la sécurité Nationale de 2013, p.94. Nous soulignons.

[62] *Ibid.*

[63] « L'armée de Terre Au Contact », July 2016, Ministère de la Défense.

COMCYBER's mission makes it perfectly clear the organization of the digital forces is unlikely to result in the creation of a separate entity. On the contrary, the task of COMCYBER is to coordinate, under the direct authority of the Chief of Staff of the Armed Forces, all the digital actions of the armies. Its location at the very heart of the central command and control centers of the armed forces (on the model of the American CYBERCOM, created in 2010 and integrated into the Joint Command) clearly shows this solution was preferred to the creation of a fourth branch in charge of the "cyber domain". This command was place at a nodal point of the decision-making process, rather than to create a complete structure that would have made the coordination process even more cumbersome. From this perspective, IT services and resources are at the disposition of all army units and weapons while providing them with the most accurate information possible to define their targets, ward off or avoid a possible hit from the adversary, and guide "kinetic" operations in a faster and more reactive manner, i.e. requiring the use of physical force.

The use of digital means is, therefore, not confined to a separate and independent space, but applies its full weight in the conduct of warfare. The Revue Stratégique, published in October 2017, insists particularly on this point. Adopting the spirit of cyber-tactical integration, the French Army went even further away from the cyber-space/cyber-strategy/cyber-army vision: "Armies, the document states, must [...] plan and conduct operations in digital space up to the tactical level, in a way that is fully integrated into the planning process and execution of kinetic operations. In addition to cyber-space-specific operations, operations in digital space broaden the range of traditional effects available to political authorities and exploit the increasing digitalization of our state and non-state adversaries. This ability requires a strengthened and sufficiently agile human resource as well as the continuous development of specific technical solutions"[64].

This document was completed six months later by the *Revue Stratégique de Cyberdéfense* (Cyberdefense Strategic Review)[65], which defined the roles of each bureaucratic entity in the process of monitoring and reacting to threats and malicious actions, in order to provide France with a coherent global policy in terms of digital security. Focusing on the protection of the nation's vital services, this review, for the first time centered on the digital domain, emphasizes the tripartition of roles between non-military intelligence (the DGSI), the Ministry of the Armed Forces (the ComCyber, located within the Armed Forces Staff), and the executive branch of government (the ANSSI depends on the SGDSN, a body directly subordinate to the Prime Minister)[66].

From the point of view of political science and the "sharing of power" between competing bureaucracies, the fragmentation of authority between several bodies dependent on different authorities seems to be confirmed. Written by the General Secretary of Defense and National Security (of SGDSN, who reports to the Prime Minister), the review underlines "the normative role of the ANSSI", one of its components, whose role is clarified and affirmed one year after the creation of ComCyber[67].

As a direct result of the recommendations made in these two "strategic reviews", a twofold document was published by the Ministry of Defense in January 2019, specifying the military use of digital assets. In its parts entitled respectively "Public Elements of Military Doctrine for Offensive Computer Warfare" and "Public Elements of Military

[64] *Revue Stratégique*, Paris, Secrétariat Général à la Défense et à la Sécurité Nationale, 2017, §299, p.83.

[65] *Revue Stratégique de Cyberdéfense*, Paris, Secrétariat Général à la Défense et à la Sécurité Nationale, 2018.

[65] *Revue Stratégique de Cyberdéfense*, Paris, Secrétariat Général à la Défense et à la Sécurité Nationale, 2018.

[66] *Ibid.* pp.46-47.

[67] *Ibid.*, p.108 : « *Forte de sa mission et de ses compétences, l'ANSSI s'est naturellement imposée comme référent pour la définition des normes de sécurité pertinentes pour assurer la protection des données et des systèmes d'information les plus sensibles, à commencer par la protection du secret de la défense nationale* ».

Doctrine for Defensive Computer Warfare"[68], this twofold document provides France with clarified rules of engagement (ROE) giving French officers precise directives on what they are allowed to do. A clarification of prerogatives and areas of responsibility was operated, to avoid harmful hesitations and debates when action must be rapid and decisive, especially in times of acute crisis. Above all, the way in which the general organization of the numerical maneuver is envisaged as well as its level of integration with the military action taken in an extensive sense, is described.

The offensive doctrine first underlines the existence of "possible fields of action" for the attackers, whose "four major objectives are espionage, illicit trafficking, destabilization, and sabotage"[69]. We note there is no question of military action, but of a numerical continuation of illicit actions.

The defensive document states "cyberspace is a confrontational environment for States or non-governmental organizations in which the risk of attack is considered to be permanent, including in peacetime"[70].

Distinguished in the *Revue de Cyberdéfense*[71], Offensive Combat (LIO) and Defensive Combat (LID) are given precise definitions:

- "*Offensive computer-based combat for military purposes (LIO) covers all actions undertaken in cyberspace, conducted autonomously or in combination with conventional military means. It aims to produce effects against an adversary system in order to alter the availability or confidentiality of data*"[72].
- "*The defensive struggle, on the other hand, is broader and goes far beyond the military domain. "The LID covers all actions, technical and non-technical, carried out to face a risk, a threat or a real cyber-attack, in order to preserve our freedom of action. The LID mainly covers three of these missions: anticipating, detecting and reacting, and completes the missions: preventing, protecting and attributing. It thus contributes to the resilience of armies and, more generally, to the development of response strategies at the ministerial and interministerial levels*"[73]. Its conception and execution are by nature interministerial and, consequently, are beyond the competence of the General Staff or the Ministry of Defense.

From an operational point of view, the LIO is the only relevant one in the conception and implementation of an action in a theatre of war. Consequently, it "[...] *is conceived at the strategic level (in the overall joint operational maneuver) and at the tactical level (in the maneuver of army components in theatres of operation)*"[74].

The constitution of a numerical maneuver, or participation in a global maneuver, requires both a degree of autonomy that allows the development of operations with many distinctive features, and the mastery of a sufficient level of coordination to ensure strategic conjunction. "*The use of the LIO,* the document insists*, is therefore part of a temporality of its own. While its effects can be dazzling, its integration into the overall operational maneuver is a process that is characterized by long and very specific planning. These effects can be material - neutralization of a weapon system - or immaterial - collection of temporary, reversible or definitive information. It proposes discrete and effective modes*

[68] *Éléments publics de doctrine militaire de lutte informatique offensive* & *Éléments publics de doctrine militaire de lutte informatique défensive*, Paris, Ministère des Armées, January 2019, https://www.defense.gouv.fr/salle-de-presse/communiques/communique_la-france-se-dote-d-une-doctrine-militaire-offensive-dans-le-cyberespace-et-renforce-sa-politique-de-lutte-informatique-defensive

[69] *Éléments publics de doctrine militaire de lutte informatique offensive*, *op. cit.*, p.4.

[70] *Éléments publics de doctrine militaire de lutte informatique défensive*, *op. cit.*, p.9

[71] *Revue Stratégique de Cyberdéfense*, *op. cit*, p.52

[72] *Éléments publics de doctrine militaire de lutte informatique offensive*, *op. cit.*, p.5.

[73] *Éléments publics de doctrine militaire de lutte informatique défensive*, *op. cit.*, p.5.

[74] *Éléments publics de doctrine militaire de lutte informatique offensive*, *op. cit.*, p.7.

of action against digitized systems, capable of substituting for other modes of action, preparing them or complementing them"[75].

Regarding digital tactical incorporation, offensive doctrine identifies "three types of operational objectives in the conduct of military operations":

1) Evaluation of adversary military capabilities: gathering or extracting information;
2) Reduction or even neutralization of adversary capabilities: temporary disruption or creation of major damage to adversary military capabilities;
3) Modification of the adversary's perceptions or analytical capacity: discreet alteration of data or systems, exploitation of information stolen from an adversary's military information system.

It is here the capabilities of information, sabotage, propaganda or disinformation are built up. These operations are conducted in complete independence by the military and are placed "under the authority of the chief of staff of the armed forces"[76]. Thus, "COMCYBER[77] is the authority for the use of the military cyber offensive capability, an integral part of the operational chain of the armies, in perfect coherence with their organization and operational structure"[78]. The objective of this is to ensure the perfect strategic conjunction of forces and not to streamline the chains of command.

This necessary numerical autonomy of the Armed Forces General Staff implies a total control of its own computer capabilities. Can we not see here a contradiction with the general competence of the ANSSI on the computer security of the ministries and agencies of the State? It is probably to clear up any misunderstanding that the 2018 Cyber Defense Strategic Review designed four "operational chains", defined as areas of competence. Thus, a "military action" chain is entrusted to the Ministry of the Armed Forces and is distinct from the "information", "judicial investigation" and "protection" chains[79]. Here again, the sharing of roles, already effective in practice, is ratified by the publication of a doctrinal document consolidating a situation which already exists de facto.

Nevertheless, certain actions, situated on the frontier between these four domains, occasionally require the collaboration of all the actors. How, in fact, can the fight against illegal financial flows that provide water for the Islamist insurgent groups in the Sahel, against which France is fighting, be delegated to a single actor? How do we respond to an attack by the Islamic State on a French news channel or newspaper, threatened to lose all their data and no longer having control over the content they broadcast (as was the case in 2015 for TV 5 Monde and for the Twitter account of the newspaper Le Monde[80])? Thus, in order to ensure the coherence and cooperation of all these operational channels, an Inter-ministerial Coordination Centre for Cyber Crises was set up in April 2018. It is "*led by the General Secretariat for Defense and National Security (SGDSN) under the authority of the Prime Minister*"[81]. It deals with four distinct areas: "protection, military action, intelligence and judicial investigation"[82].

The analysis, tedious but necessary, of the progressive implementation of these various documents shows that France has consolidated a model of cyber defense resting, in the last instance, on the executive, in close collaboration with the Joint Chiefs of Staff and intelligence, and not exclusively on the latter. This is a notable difference with the

[75] *Ibid.*, p.6

[76] *Ibid.*

[77] Which depends on the Chief of the Defense Staff (the equivalent for Joint Chieff of Staff).

[78] *Éléments publics de doctrine militaire de lutte informatique offensive*, *op. cit.*, *p.5*

[79] *Revue Stratégique de Cyberdéfense*, *op. cit*, p.53.

[80] See Boyer, Bertrand, « Comprendre les cyber-opérations » (https://www.amazon.fr/gp/product/B0173TUS0W/ref=dbs_a_def_rwt_hsch_vapi_tkin_p1_i0), and Damien Leloup & Untersinger, Martin, « Comment notre compte Twitter a été piraté », *Le Monde*, January 24th 2015.

[81] *Éléments publics de doctrine militaire de lutte informatique offensive*, *op. cit.*, p.4.

[82] *Ibid.*

American model, where the weight and specificity of an agency like the NSA induces different interactions between the bureaucratic actors of cyber warfare. Particularly in the offensive domain, the military authority affirms in its doctrine its total autonomy: 'LIO actions are conducted, under the responsibility of the Chief of Defense Staff, within the framework defined in domestic law by the Defense Code and under the conditions set by the Prime Minister"[83].

Thus, a global policy of digital integration is gradually emerging, extending the doctrine of Permanent Security Posture (PPS) with regard to the threats arising from the generalization of remote computer communications: "*The tension generated by these cyber-attacks, cyclical or sudden, of varying severity, requires the adoption of constant vigilance, which is embodied in the Permanent Posture of Cyber Defense (PPC) for the Ministry of the Armed Forces. The PPC is made up of all the provisions adopted to ensure the permanent (24/7) defense of the Ministry's computer systems in the peace-crisis-war continuum*"[84].

In order to ensure the defense of its servers and its digital warfare tools, the Ministry has also set up its own organizations dedicated to this task: "*At the Ministry level, under the orders of COMCYBER, the Center for Defensive Cyber Combat (CALID) provides an overall technical "hypervision", which synthesizes and shares information on cyber situations produced by all the Security Operating Centers or by its own means*"[85]. In the latest documents pub-

Exercise Serpentex 2016, Close air support assisted by digital tools
Image : Assemblée nationale, Commission Défense

[83] *Éléments publics de doctrine militaire de lutte informatique offensive*, *op. cit.*, p.10.

[84] *Éléments publics de doctrine militaire de lutte informatique défensive*, *op. cit.*, p.9.

[85] *Ibid.*, p.8.

lished, the Chief of Staff of the Armed Forces reinforces his role and rules out any possible contestation of his authority in the "military chain of command" created by the Cyber-Defense Strategic Review: "*At the top of the LID chain, COMCYBER relies on the Cyber Operations Centre (CO Cyber) to guide the work of CALID and the Security Operating Centers. More precisely, it shares the level of cyber threat and newly discovered vulnerabilities in order to optimize the effectiveness of the department's cyber defense and protection chain*"[86].

This permanent defensive posture cannot be ensured at all times by the Armed Forces, but is routinely ensured by the National Agency for the Security of Computer Services, but it can switch at any moment to a crisis configuration, in order to be able to operate in coordination with the Armed Forces and the intelligence agencies. The risks of ambiguity in the definition of competence in the decisive moments of a crisis or of refusal to share information have thus been reduced. French agencies were thus gradually given the means to establish a form of deconfliction within its digital defense policy since the publication of the 2008 Defense White Paper and the creation of the first dedicated agencies, at the same time as the setting up of specialized services within the armed forces and intelligence services.

This confirms that the defensive mission "*is the responsibility of the National Agency for the Security of Information Systems (ANSSI), in coordination with the intelligence services and the Cyber-Defense Command (COMCYBER) within the perimeter of the Ministry of the Armed Forces*"[87]. The "cyber-defense mission" of "reaction"[88] is established as a framework and receive a precise definition: "*it is a matter of resisting a cyber-attack so that it does not prevent the continuation of our activity. In most cases, the COMCYBER then triggers a LID operation, in liaison with the ANSSI. It may involve the use of means outside the domain of cyber defense, or even the Ministry of the Armed Forces (referral to the courts, diplomatic action, economic retaliation, etc.)*"[89].

Finally, the ultimate responsibility, which is that of drawing the political consequences of a digital attack, remains the prerogative of the Head of State: "*The intelligence services are at the heart of this process of gathering indications of attribution. The decision to attribute responsibility rests with the highest political leaders*"[90].

It should be noted that the attribution of responsibility for an attack to a diplomatically recognized state, either as a direct operator or as a sponsor, has just received an original response in the American document. Any state accused of a computer attack, sponsoring an attack or harboring a group organizing such an offensive that endangers national security, will be liable for a response that is not simply symmetrical and limited to the field of digital warfare, but "kinetic". In this regard, the United States has formally extended the scope of conventional and unconventional deterrence to the digital domain. Any state actively or passively using computer destabilization strategies is thus threatened by a conventional military strike[91]. This represents an extension of the principle of "peace through strength" in relation to which France cannot avoid positioning itself in the years to come.

The last step: Digitalization of the « last tactical kilometer »

Through a commentary on the latest published doctrine documents, we have just examined in detail France's global strategy to create institutions

[86] *Ibid.*

[87] *Éléments publics de doctrine militaire de lutte informatique défensive*, *op. cit.*, p.4.

[88] Instaurée par la *Revue Stratégique de Cyberdéfense*, *op. cit*, p.48.

[89] *Éléments publics de doctrine militaire de lutte informatique défensive*, *op. cit.*, p.4.

[90] *Ibid.*, p.5.

[91] *National Cyber Strategy*, Washington, Presidency of the United States, September 2018, p.21: « *All instruments of national power are available to prevent, respond to, and deter malicious cyber activity against the United States. This includes diplomatic, information, military (both kinetic and cyber), financial, intelligence, public attribution, and law enforcement capabilities* ».

enabling resistance to general attacks, exclusively in the digital domain. But what about the digitalization of traditional units, which must implement offensive or defensive means of computerized warfare?

For this, the digital architecture examined above is a prerequisite, but is not the final word in the digital reform of armies. Many actions are minor or cannot wait in the field for the time needed to put into action a structure located on the national territory, several thousand kilometers away.

Armed forces also need a digital transition model at the lowest scale, i.e. the tactical level. It is; therefore, interesting to focus on models that would enable integration of digital capabilities into existing structures while trying to measure whether this integration is harmonious or not. This requires observing the most recent mutations in this rapidly changing field of military confrontation, where concrete, documented and accessible examples are, in the end, quite rare. To conclude this invitation to debate, we shall refer to the way in which the digital shift of French armed forces is currently taking place at the tactical level.

With each confrontation, the role of "electronic warfare" tools in the "last tactical kilometer"[92] proves to be a little more central. It has already allowed groups such as the Islamic State or the Al-Nosrah Front to carry out sophisticated low tech and low budget operations which are increasingly difficult and costly to fight[93]. However, the know-how enabling these low tech means to be neutralized is beginning to accumulate in the various units of the Western armies and certain lessons can be drawn from this.

The combat units of the three "traditional" branches depend on new information and communication technologies to perform an increasing number of tasks. If we assume that the belligerent groups, and thus the conflicts and tactical areas of operation, will be digitalized ever more rapidly, their importance will be even greater in the future. They will be indispensable for operating in hostile areas of high information density, such as urban centers where future fighting may tend to be concentrated.

This dependence should lead to greater collaboration and cohesion between the entities collecting intelligence and those using it at the tactical level. One of the keys to successful collaboration is the establishment of a legal framework for effective collaboration, allowing for teamwork that minimizes competition and the refusal to collaborate ("deconfliction" in the American vocabulary), which we have just examined. Moreover, as the logic of digitalization, which can also be observed in the economic field[94], requires that digitized collaboration be more "horizontal" and rely less on the "vertical" circulation of orders and useful information, while reserving improved targeted intervention capabilities for the benefit of the command. An examination of digitalization "from below" (digital tactical incorporation) is also necessary, after examining the transformation initiated from above (the digital strategic conjunction).

A first step in tactical incorporation could be the introduction at all levels of officers and NCOs specialized in computer tasks and the integration of soldier-technicians with lower skills (similar to the "radio operators" present in each battle group, whose task has already been mentioned, for the management of simple computerized tasks). There is already many examples of that phenomenon, which is occurring everywhere. For instance, the French army introduced a digital transmission device, named *Auxylium*. It is a small tool, based on a smartphone available in retail stores, but modified

[92] Expression forged by Porche, Isaac R. III & Colin, Clarke P., *Tactical Cyber*, *op. cit.*, p.26.

[93] Bronk, Chris & Anderson, Gregory, "Encounter Battle: Engaging ISIL in Cyberspace" in *Cyber Defense Review*, 2017, n° 2, vol. 1. See also Hashim, Ahmed S., *The Caliphate at war: Operational realities and innovations of the Islamic State*, Oxford, Oxford University Press, 2018.

[94] See a good description of the consequence of digital transformations on the governance of organizations of all types in *World Bank World Development Report 2019: The Changing Nature of Work*, Washington, International Bank for Reconstruction and Development, December 2018.

for military purpose. This device, which can be operated by a single soldier, permits a broader flow of information to reach other tactical units of the French Army (in France, the "combat group", i.e. between 8 and 12 men). This is a good illustration of the diffusion, in small units, of new roles and new specializations. Their large number and dispersion will provide more opportunities for combat teams to access a reliable digital link with C2 nodes. This will not only permit them to receive information from all other capacities, but will enable them to gather and diffuse their own intelligence using the "bottom-up" method, acquired through simple tasks: penetrating a wi-fi network, scrambling or intercepting digital communications of the adversary, signaling conventional information on adversary's moves and equipment, etc.[95].

Maintaining a strict separation between a "cyber army" or units purely dedicated to cyber warfare but located thousands of kilometers away does not make it possible to create the "esprit de corps" necessary for the continuation of combat, which remains above all a human phenomenon. This configuration does not make it possible to establish real solidarity between the two teams and often leads to the cancellation of the mission at the slightest hitch in relation to the initial plan, because communication between the hierarchy and the digital team is not optimal. Since 2017, the US Army has thus set up a complete hierarchy of "Electronic Warfare Officers" and managers of the electromagnetic spectrum, to be incorporated from the top of the hierarchy to the lowest echelons[96].

From an operational point of view, certain lessons can already be drawn from the digitalization of entire units and the implementation of digital "support". The comparison with the United States can be used here. The document *Tactical Cyber: Building a Strategy for Cyber Support to Corps AMD and Below*[97] is a study of the use of cyber-tactical tools in three US external operations, belonging to both civil security and military action. These are:

1) the joint interagency task-force-south, tracking drug trafficking from South America;
2) the Marine Corps cooperation with the NSA in receiving and using Signals Intelligence (SIGINT); and
3) the use of military UAVs in Operation Enduring Freedom.

What they have in common is the use of state-of-the-art tools and a very precise use of digital intelligence for the success of the mission. The most salient points of these three in-depth case studies can be reduced to a few conclusions, which can guide the consolidation of the tactical level thanks to the new digital tools:

1) Building a cooperative relationship between tactical units and intelligence services (especially in cases where several agencies are involved, some of which belong to other states) requires mutual trust, which can only be achieved through sustained collaboration. This co-operation is of course deepened by the phases of operations requiring numerous and rapid transmissions of information. The cohesion born of repeated collaboration is valuable and must be put to good use in future operations. The "sodalic"[98] congruence of the groups in-

[95] For all the tasks that could perform such "electronic warfare officers", see Porche & Clark, *Tactical Cyber, op. cit*, p.52. They call it "Remotly Supported Cyber Operator", that would be an infantery man performing basic operations to link its units to the C2s. This RSCO would work in liaison with reach back experts and more specialized brigade level personnel to manage the liaison and endeavor more complex tasks.

[96] Voir le "Field Manual 3-12 – Cyberspace and Electronic Warfare Operations", Joint Publications, *United States Department of Defense*, April 2017, chapter 3 (Corps to brigade-level electromagnetic cyberspace operations). Previous version, FM 3-12 (R) of 2013, was simply called "Cyberspace Operations". It introduced the notion of « Electronic Warfare », now also used by French Armes Forces (« Guerre Electronique », or "GE"). See the new Army model, « Au Contact », already mentioned.

[97] Porche, Isaac R. III & Colin, P. Clarke, « Tactical Cyber: Building a Strategy for Cyber Support to Corps and Below », Santa Monica, RAND Corporation, Aroyo Center, 2017.

[98] Derived from *sodalis*/*socius*, which designate the companion, the associate, or the member of brotherhood in latin. Sodality is for Baechler the « capacity to form a group,

volved is essential for the success of the mission and must be considered as a natural and inevitable problem, and its overcoming as an objective obstacle, the resolution of which is a condition for the smooth running of operations.

2) Collaboration must be beneficial to all participants. Establishing a mutual understanding of the interests and principles of each organization is a prerequisite for a healthy collaborative relationship. This can be enhanced by exchanging personnel and agreeing on a simplified standard procedure for information sharing. Through this human cooperation, which is concretely established through liaison officers, the needs of the unit on the ground are identified by a delegate from the signal intelligence agency. Refusal to give certain information then becomes more difficult when a human and procedural agreement has been established at the outset of the cooperation. This leads to a common identification with the goals of the mission and builds a community of interests directing efforts in the same direction[99].
3) The success of certain operations should be used to demonstrate the mutual interest in cooperation and to be able to deepen it (on the model of Allat unit[100], for example, making it possible to cross-reference information from the various French intelligence agencies and thus more effectively detect the preparation of terrorist operations). The demonstration of non-hostility must be made in order to establish a dialogue beneficial to all stakeholders. The fundamentals of the analysis of bureaucratic organizations can be found here in the domain of political science[101].
4) The legal framework of the operation must be precisely defined from the outset, in particular so that authorizations to launch digital operations do not require a multitude of steps at the highest level and cause the command to miss tactical opportunities. The tactical initiative, as well as the "agility" referred to in the 2017 French Strategic Review, must not be diminished by a procedural burden that deprives the command of its capacity to act in the right tempo of the operational theatre.

It is on these principles that the digitalization of the French Army units was started, with the implementation of the Scorpion program. Taking as an example the US Army's "Cyber Support to Corps and Below" pilot program, cited by the RAND's Tactical Cyber document published in 2017[102], the Army is seeking to equip its troops with the equivalent of CyberWarfare Officers, as noted by Lieutenant-Colonel Cheize of the Command Doctrine and Training Center: "*a tactical commander in mid-earth is responsible for an area of operations that is becoming increasingly dense in terms of digital systems and data volume, stored and transmitted through various communications media, and this trend may continue to grow with ever more capable means. It must therefore be able to act on this environment in a reactive manner, either to defend its own systems under increasing strain or to seize tactical opportunities by engaging its adversary in or through cyberspace"*[103].

---

efficient to reach the goal it was given ». Voir Baechler, *Nature et Histoire*, *op. cit.*, p.150.

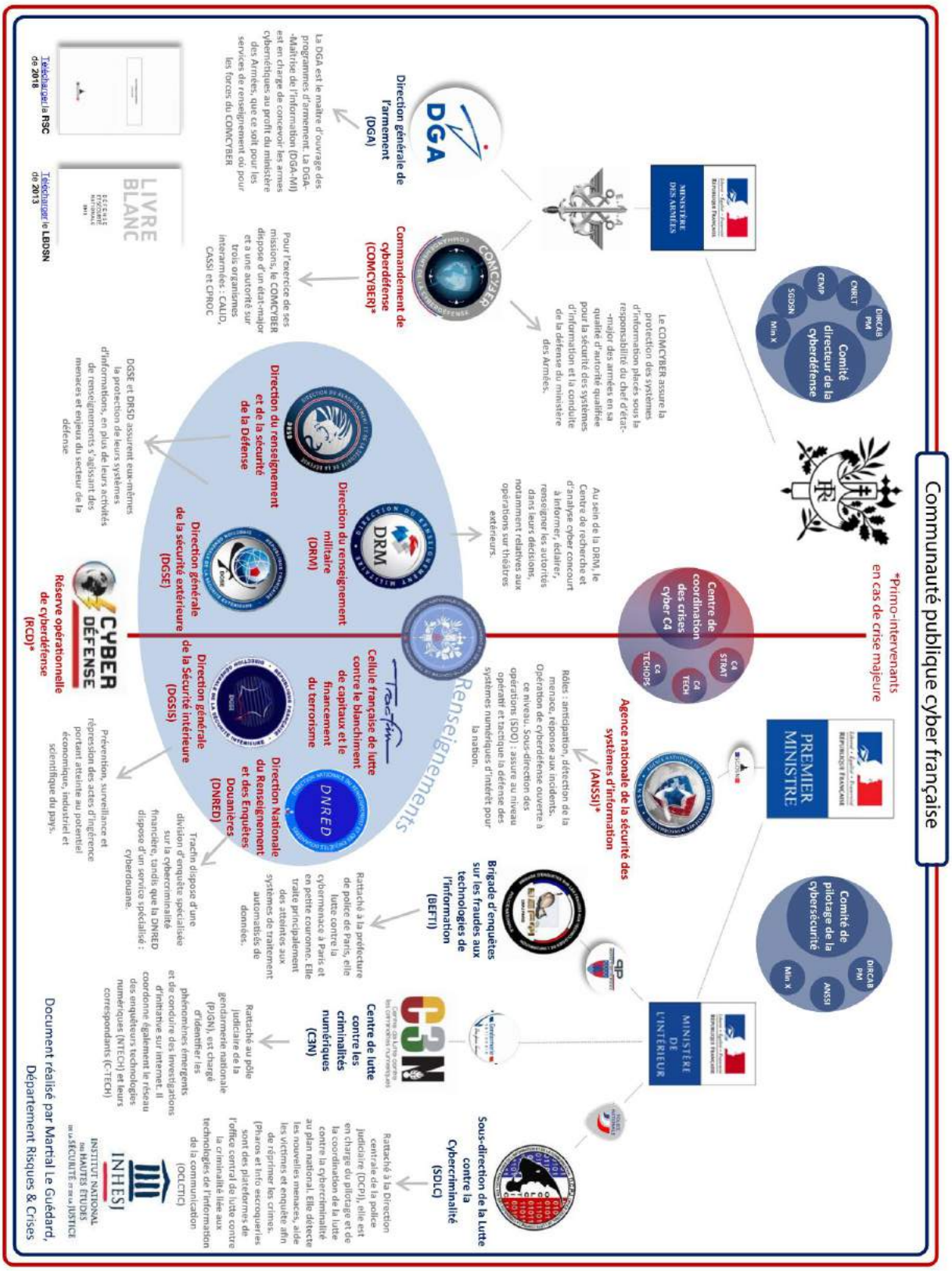
[99] See Goya, Michel, *Res Militaris : de l'emploi des forces armées au XXIe siècle*, Paris, Economica, 2011.

[100] Named after a pre-Islamic goddess, this cell provides a forum for the exchange of information on terrorism and the Iraq-Syrian conflict. Its procedures, based on direct solicitation and an immediate response from the department concerned, were considered particularly effective. This judgment confirms the relevance of the "foot in the door" strategy encouraged by the Tactical Cyber report. Based on personal knowledge and understanding of the operational needs of other agencies, it enabled the circulation of information at a much faster rate than usual and set up a real "deconfliction", limiting the war of services and the retention of information.

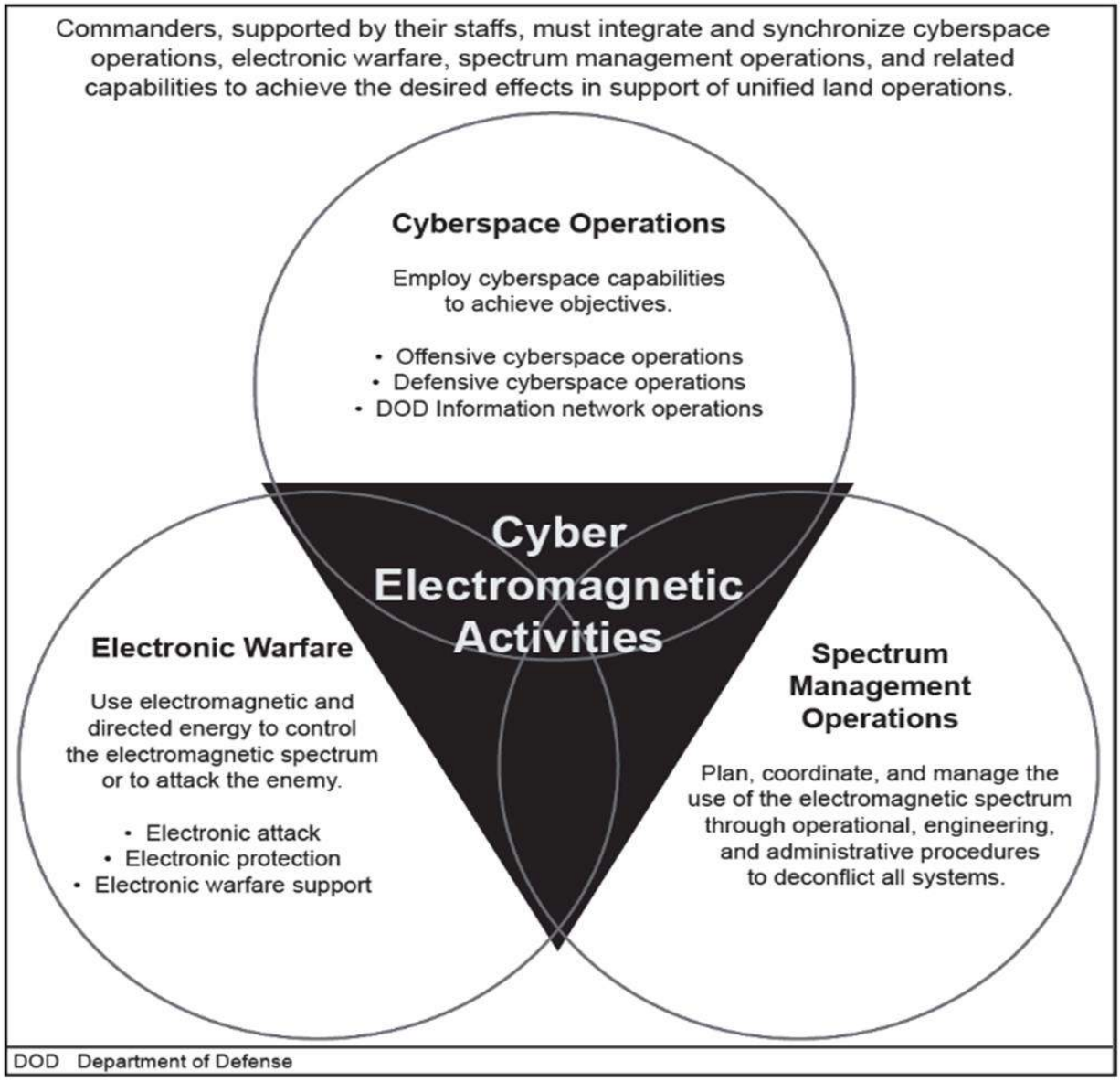
[101] Haas, Richard, *The Bureaucratic entrepreneur*, Washington DC, Brookings Institution Press, 2001.

[102] Porche & Clark, *Tactical Cyber, op. cit*.

[103] Cheize, Julien, « Les enjeux du cyberespace pour l'armée de Terre », in *Pensées mili-terre Centre de doctrine et d'enseignement du commandement*, published on March 21st 2020.



« Communauté cyber française »,
Document réalisé par Martial Le Guédard, 2019.



For this, the solution of technicians with skills that can be multiplied in many tactical groups seems to be the best one. The effects sought clearly indicate an objective centered on the tactical level: "the challenge for the Army," says the officer cited, "is to put its land forces in a position where they will be in a position of capability:

- to provide a situation assessment of their own environment, through a Cyber Reference Situation (SCR, or CP);
- to defend their weapon, command and control (C2), information and command and control (C2) systems;
- to identify and request, in support of their work, effects that will be produced by higher levels, up to the operational or strategic level;
- to produce these effects directly thanks to tactical capabilities that would be deployed within a division, a brigade, or even a joint tactical group (or GTIA)"[104].

[104] *Ibid.*

These issues, if we compare them with the conceptual framework proposed in this note, do indeed belong to the field of digital tactical embedding. Of course, these new capabilities are not without new vulnerabilities, as Serge Caplain of IFRI notes. More problems could arise from difficulties that were not sufficiently anticipated, such as the ability to maintain the link between units. It would then be the tactical level that would suffer from the sum of all the shortcomings accumulated upstream: "*[The] interconnection problems are essentially found at the tactical levels, the very ones that have the least time and resources to deal with technical turpitudes. The most obvious consequences are problems of transcription fidelity, loss of speed in information processing and a possible slowing down of the maneuver*"[105]. There is little doubt that problems of this kind will be one of the main occupations of armies that have carried out their digital integration. The real gain in power gained through the digital transition will depend on their successful resolution.

Far from being a pure technical operation thought out and implemented by an engineer, digital cooperation between different units, which are themselves digitized, must be thought out and analyzed as a complex process, with technical, economic and social (more precisely sodalic and agoric) stakes. This process, which Philippe Lépinard calls "augmented organization"[106], is a challenge for the digital transformation of armies. Like any human and political phenomenon involving the sharing of resources and power, this process already brings individuals and bureaucratic groups with sometimes divergent, if not antagonistic, objectives into conflict. It is therefore a question of considering these strategies of "bureaucratic entrepreneurs", as Richard Haas calls them[107]. As we have already pointed out, these analyses are the result of the application to strategic studies of the classical tools of political science and sociology, as well as technological or economic analysis.

To sum up, according to the elements that emerge from the Tactical Cyber study, it seems possible to retain four principles for the implementation of effective digital cooperation: the digitalization of armies is:

- (1) a social process, based on a proven collaboration of stable groups.
- (2) having built a common vision of the objectives to be achieved and established a climate of reciprocity and absence of hostility.
- (3) having by nature divergent bureaucratic strategies and decision-making processes.
- which (4) must not be made too costly by the legal and regulatory framework of the command[108].

According to the principle brilliantly identified by the geographer Pierre Gourou in his analysis of development policies (another type of adaptation of technical systems to a less advanced technical and human environment), the procedures and techniques of supervision, and even "prejudices", must be considered as "objective obstacles" to the implementation of new techniques[109]. Perceived as "progress" among humanitarians, they may, however, appear as a social and economic regression to the people one seeks to help. Like development policies, the digital transition must take as an "objective obstacle" the cognitive configuration of soldiers, who must perform complex tasks for which stability is a guarantee of safety.

USAF's *Advanced Battle Management System:* A soon completed digital transition?

To face Chinese and Russian threat, the US armed forces need, as underlines Christian Brose in its book *The Kill Chain: Defending America in the Future of High-Tech Warfare*, to put up un "military Internet of things". This endeavor aims at con-

[105] Caplain, Serge, « Les 10 pièges de la numérisation des forces terrestres », article posted on the author's personal LinkedIn page, January 15th 2018.

[106] Lépinard, Philippe, « La numérisation des forces terrestres : de la numérisation de l'espace de bataille à l'organisation augmentée », 18e Congrès de l'Association Informatique et Management, Montréal, 2018. https://hal-upec-upem.archives-ouvertes.fr/hal-01823344/document

[107] Haas, Richard, *The Bureaucratique Entrepreneur*, *op. cit.*

[108] Porche & Clark, *Tactical Cyber*, *op. cit.*

[109] Gourou, Pierre, *Les Terres de Bonne Esperance : le monde tropical*, Paris, Plon, coll. « Terre Humaine », 1982, p.284.

necting everything and sharing data at much higher pace. In doing so, commanders would be able to "move the most useful information rapidly to those who needed is the most", as Andrew Marshall, Director of the Office of Net Assessment at the Department of Defense, stated it in his influential report on the Gulf War[110].

Today, US Joint Chief of Staff has much clearer view of what kind of network it must build to permit a permanent and seamless exchange of data between all its platforms. Brose describe the requirements of such a network as "a large, distributed network of military systems that could be built and modernized faster, cheaper, more flexibly, and in greater numbers than any of our traditional military systems. These autonomous systems could also help to deliver even larger numbers of even smaller, lower-cost, but shorter range autonomous systems to future battlefields"[111].

To achieve this objective, the US Air Force launched one of the most ambitious projects currently being conducted by the US Department of Defense: the Advanced Battle Management System (ABMS). The ABMS is the US Air Force's new Command & Control model, based on a completely redesigned data architecture. It intends to connect not only the platforms of USAF, but to encompass all the platforms and the censors of US military. This new kind of C2 was designed to cope with information flows that are still impossible to process, because they are generated by a very large number of sensors set up by the Pentagon without an equal number of analysts being available. In many ways, this is a new generation of "command and coordination system" that could set a precedent and provide the first model of an army whose elements would be integrated into a digital canvas designed for an entire army. As we will see, this system is not only a technical creation, but also takes into account its "human environment" of the network and clearly aims to adapt to soldiers' cognitive faculties.

The need for a totally redesigned "military Internet of things" is the logical consequence of the doctrinal changes made since 2017. This concept of an "Advanced Combat Management System" is the declination of the doctrine of Multi-Domain Operations (later renamed Joint All Domain Operations by the US Air Force) in terms of digital Command & Control. The objective here is to "[...] *create dilemmas for opposing forces, surpassing their capabilities with too many threats to counter effectively*"[112], by giving all the "operators" the benefit of data collected by much more advanced sensors used by the latest generation aircraft, such as the F-35. Indeed, as Lieutenant General David S. Nahom, Deputy Chief of Staff of the US Air Force Planning Staff, points out, the current data infrastructure is insufficient to take full advantage of the capabilities of these aircraft: "*Those F-35s are bringing in data information at a level no other airplane on earth has ever been able to do. How do we get to a point where we can share this information with that special ops team directly below that airplane? We need to build an infrastructure that allows that*"[113]. The networking of sensors and operators across the entire armed forces is; therefore, necessary. " *Air Force, Navy, Marines, Army… everyone has a sensor out there. The question is how do we loop them all in, so we can share data at shot quality level*"[114].

The implementation of a new data architecture is a way to drastically improve the speed of target acquisition for "all-out" attacks. It could also prove to be a necessity in enabling the system to function properly without being overwhelmed by the exponential weight of the data collected. As stated in the US Air Force's budget request for fiscal year 2021[115], ABMS is seen as a necessary evolution of

[110] Quoted in Christian Brose, *The Kill Chain: Defending America in the Future High-Tech Warfare*, New York, Hachette Books, 2020, p.3.

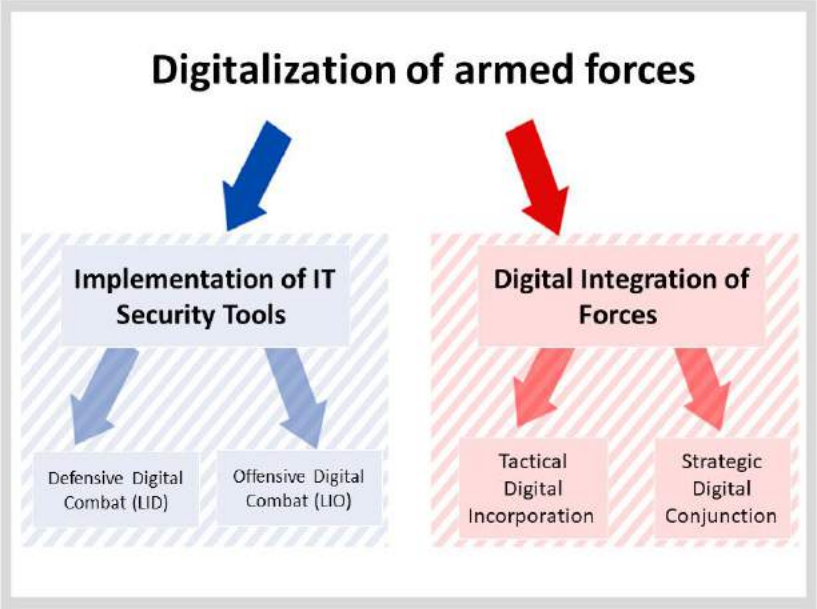
[111] Christian Brose, *The Kill Chain, op. cit.*, p.143.

[112] *Entretien du Lt General David S. Nahom, USAF Deputy Chief of Staff for Plans and Programs, pour le Mitchell Institute for Aerospace Studies, 16 avril 2020,* https://www.youtube.com/watch?v=VPWsdbr3BZc.

[113] *Ibid.*

[114] *Ibid.*

[115] *United States Air Force Posture Statement Fiscal Year 2021*, Washington, *Department of Defense*, February 2020.



offensive capabilities as well as a vital update of the information circuit. As near-pear adversaries return, the information circuit is under the dual threat of its own complexity and the new performance capabilities of potential opponents, particularly thanks to the spread of low-cost digital technologies: "Connecting these platforms, sensors and weapons via ABMS and Joint All-Domain Command and Control will maintain their viability and lethality in combat"[116].

However, the success of this reform could give the US Air Force tactical and strategic superiority to maintain and even strengthen the Total Air Dominance it still enjoys today. With the contribution of digital technologies and the automatic processing of certain tasks by artificial intelligence, the US Air Force Staff hopes to "generate a window of superiority in the air and in cyberspace, with joint forces converging on the most important targets"[117].

The idea of a *Total Cyber Dominance* that will be necessary to establish, along with air dominance[118], emerges in this budget request making explicit the ultimate objectives of America's future combat system. In addition, information management being facilitated, concrete benefits would be offered to operational personnel. For example, pilot activity could be refocused on combat, moving away from constant communication with squadrons and C2: "*A recent trial involved connecting the computers of two Air Force stealth aircraft - an F-22 Raptor and an F-35 Joint Strike Fighter - allowing them to share data automatically, so their pilots could spend less time talking to each other and more time evaluating and acting on the data*"[119]. An increase in threat avoidance and destruction capability is also expected from this digitalization of Command & Control, which is an important step in improving strategic connectivity.

The four US armies would thus be able to transmit data and positions, whether they concern the enemy or themselves, at any time and automatically: "*When the Air Force employs in concert with Army, Navy, Marine Corps, and Space Force capabilities, opponents will have to defend their forces across all domains, all the time. The Air Force will enable JADO by helping connect all forces into a cohesive battle network in ways they are not connected today*"[120].

---

[116] *Ibid.*, p.5

[117] *Ibid.*

[118] On that idea, see Wielhouwer, Peter W., « Toward Information Supériority: The contribution of Operational Net Assessment », in *Air & Space Power Journal*, Vol. XIX, n° 3, pp.85-96. This concept is underlying in the title of the current program of the USAF « *Next Generation Air Dominance* » (NGAD). This program is supposed to conceive and craft the 6th generation of fighters.

[118] Tucker, Patrick, "Toward A War With Fewer Radio Calls." In *Defense One*, January 21yh 2020,

https://www.defenseone.com/technology/2020/01/toward-war-fewer-phone-calls/162562/

[119] Tucker, Patrick, "Toward A War with Fewer Radio Calls." In *Defense One*, January 21st 2020.

https://www.defenseone.com/technology/2020/01/toward-war-fewer-phone-calls/162562/

[120] *United States Air Force Posture Statement Fiscal Year 2021*, *op. cit.*, p.2.

A few interconnections could be considered to accomplish the most difficult task today; shared and automated target acquisition, not between several weapons, but between several armies, or even with allied forces. For instance, the US Air Force said in its 2021 budget request to the US Congress, "*our fifth-generation aircraft cannot easily share data with some older fighters, the sensors on many Navy ships cannot detect the batteries of the Army's air defense artillery, and soldiers and Marines cannot always access the real-time video feeds of our international partners during combat*"[121].

The key feature of the system is the ability to provide a digital architecture that allows for simple data flow, where all partners can "plug in" without too much difficulty, while still allowing control of shared data. But to be successful, the implementation of this new architecture needs to be massive and encompass all available users, while at the same time setting a new standard for future acquisitions. If digitalization is carried out inconsistently, it would result in a cumulative sum of delays and underperformance, which would make it impossible to achieve any real gain in power: "*the Air Force sees the ABMS architecture as the key to avoiding creating a massive acquisition effort from disparate programs like Reaper or the legacy JSTARS fleet*"[122]. The underlying idea here is that this global digital transition may only be possible within a limited time window, before too many automated systems are coupled, and before data obtained from space capacities start to flood the systems.

Indeed, if these new means were to be "plugged in" with their own standards, it would undoubtedly delay the ability to share and receive information continuously. The ABSM system "will include a mix of traditional manned aircraft, drones, space-based technologies and data links"[123]. But "*It is so easy to start talking about satellites and airplanes and forget what ABMS is going to have to uniquely champion, which is the data architecture that will connect them*", said Will Roper, director of the US Air Force Acquisition Department[124]. Once this data architecture is secured and made efficient with all aircraft, "*ad hoc* mesh networking will allow platforms to automatically begin working together and sharing information without human interference"[125]. "Closing the kill chain", as Christian Brose puts it[126], will then be possible at a much faster pace.

Based on the techno-optimist projections of the vast majority of U.S. Force Architects, it is only after the complete digitalization cycle is complete that digital capabilities will be able to support the much more progressive "kinetic" forces thanks to the new configurations enabled by the ABMS. According to General James Holmes, who leads Air Combat Command, only then will the contribution of new digital assets fully participate in strategic decision making: " We think we can present more robust teams [to Cyber Command] with better intelligence support behind them and present some information ops options … [at] a larger scale"[127].

If these promises are fulfilled, ABMS could be extended to the entire U.S. military. The budget requested by the Pentagon for 2021 devotes $302 million to this, compared to the $144 million voted

[121] *Ibid.*

[122] Insinna, Valérie, « Here's the Number One rule for Air Forces New Advanced Battle Management System », in *Defense News,* July 9th 2019, https://www.defensenews.com/digital-show-dailies/paris-air-show/2019/07/09/rule-no1-for-air-forces-new-advanced-battle-management-system-we-dont-start-talking-platforms-until-the-end/

[123] Insinna, Valérie, « Here's the Number One rule for Air Forces New Advanced Battle Management System », in *Defense News,* July 9th 2019, https://www.defensenews.com/digital-show-dailies/paris-air-show/2019/07/09/rule-no1-for-air-forces-new-advanced-battle-management-system-we-dont-start-talking-platforms-until-the-end/

[124] *Ibid.*

[125] *Ibid.*

[126] Christian Brose, *The Kill Chain*, *op. cit*.

[127] Pomerleau, Mark, "How A New Air Force Unit Could Help Beat Russian Air Defense Systems", in *C4ISRNET*. 12 November 12th 2019, https://www.c4isrnet.com/battlefield-tech/it-networks/2019/11/12/how-a-new-air-force-unit-could-help-beat-russian-air-defense-systems/

for 2020[128]. We are therefore confronted to a real enablement of this kind of digital architecture, which could see its budget double next year. Indeed, "*ABMS is part of a broader Pentagon vision called Joint All-Domain Command & Control [or JDAC2]. JADC2 represents an effort to create a networked nervous system for warfare. It aims to link every ship, soldier, and jet, so that ground, air, sea, space, and cyber assets can share the exact same data and can be used almost interchangeably to take out targets, even in environments where communication is being heavily jammed or where adversaries have advanced air defenses*"[129]. The US Armed Forces would then be the first to have fully completed its digital transition, reconciling the two "sides" of optimized digital integration proposed in this note: on the one hand, *tactical incorporation*, and on the other hand, the *strategic conjunction*.

Conclusion: toward a cyber battlespace or new tools for Digital Command and Communication?

The digitalization of armies poses, as we have tried to show in a very synthetic way, a series of human, organizational. and "sodalic" challenges that would be harmful to neglect. The problems it poses for the staffs appear to be as much linked to the emergence of new technical tools as to their manipulation by combat groups with proven habits that are costly to modify. The tools of interpretation derived from anthropology allow us to evaluate, under certain aspects, the necessarily limited rationality of the actors, and to bridge the gap between the technical optimum imagined *in abstracto* and the emerging uses concretely observed.

The designers of future armies will hardly be able to do without these tools of interpretation if they truly wish to establish a diagnosis and implement concrete rectifications to accomplish the task they have to accomplish: to implement communication and computer data production tools within "kinetic" armies at the lowest economic, human (or "cognitive") cost in order to obtain the maximum amount of power in the face of the state and sub-state adversaries with whom the troops will be confronted tomorrow.

For this to happen, a completely new operational know-how must, in fact, be constituted and instilled in the training of officers of all armies. Its quality depends on the relevance of the response to two issues: the integration of the digital component into strategic and tactical decision-making, and the rapid circulation of innovations that can provide a specific advantage.

To do this, there is no need to find a separate army, nor to make the cyber a geographically distinct space. Not considering the digital tool as the "4th domain" of warfare does not in any way bring it into disrepute or undermine its role. On the contrary, it is a matter of insisting on the total transversality of the digital technical system and placing it at the center of all operations (Fig. 1). It also means considering that its place is central in decision-making and that good organizational integration is the guarantee of better tactical agility and a greater capacity for improvisation and adaptation to unforeseen situations. Rather than the organic establishment of armies dedicated to "cyber", it is probably more constructive to opt for fully digitally integrated armed forces.

This debate is crucial for the armed forces of the Atlantic Alliance in particular, which could see their pre-eminence called into question if the wrong choices are made in terms of digitalization policy. The decisions taken today commit them for years, and maybe decades. Wrong choices could durably reduce their capacity for action, which has already begun with the multiplication of crises, external interventions, and the spread of digital tools themselves, which have facilitated the potential for operational nuisance of groups previously devoid of any real influence on international relations.

[128] *United States Air Force Posture Statement Fiscal Year 2021*, *op. cit.*, p.2.

[129] Patrick Tucker, "War on Autopilot? It Will Be Harder Than the Pentagon Thinks." in *Defense One*, February 12th 2020.

The consequences, necessarily unpredictable, of the technical and social transformation linked to the digitalization of operations must be examined step by step in order to understand the nature of the human changes that are being provoked. According to P. Gourou, "each local situation being a complex of techniques that react one on top of the other"[130], the analysis of the digital transition of armies cannot overlook a multidisciplinary anthropological investigation that will make it possible to evaluate the human consequences of the technical change on the microsociology of the social group on which it is imposed. More even so if this group is not a regiment of "cyber-combatants" mounted from scratch and evolving in a vacuum within the army, but groups of traditional warriors who are being taught new digital techniques.

"True military innovation is less about technology than about operational and organizational transformation", says Christian Brose[131]. Thus, the possibility of an analytical tool could emerge, not only technical, but also human, which would undoubtedly make it possible to orient in a more precise manner the political and strategic choices that must be made today and which will have, in the coming decade, the most decisive repercussions on the balance of power between the different powers on the international scene.

[130] Gourou, Pierre, *Les Terres de Bonne Esperance : le monde tropical*, *op. cit.*, p.370.

[131] Christian Brose, *The Kill Chain*, *op. cit.*, *p.*84.

Bibliography

Books

ANDRESS, Jason & WINTERFELD, Steve, *Cyber Warfare. Techniques, Tactics and Tools for Security Practitioners*, Amsterdam, Syngress, 2011

BARNABY, Frank, *The Automated Battlefield: New technologies in modern warfare,* Oxford, Oxford University Press, 1986.

BARNABY, Frank, *What on Earth is Star Wars?: Guide to the Strategic Defence Initiative*, Fourth Estate Ltd, 1987.

BAECHLER, Jean, *Nature et Histoire*, Paris, PUF, 2000.

BONNEMAISON, Aymeric & DOSSE, Stéphane, *Attention : Cyber ! Vers le combat cyber-électronique*, Paris, Economica, 2014.

BOYER, Bertrand, *Cyberstratégie, l'art numérique de la guerre*, Paris, Nuvis, 2012.

BOYER, Bertrand, *Cybertactique, conduire la guerre numérique*, Paris, Nuvis, 2014.

BRODE, Christian, *The Kill Chain: Defending America in the Future of High-Tech Warfare*, New York, Hachette Books, 2020

BUCHANAN, Ben, *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations*, Oxford, Oxford University Press, 2017.

CARR, Jeffrey, *Inside Cyberwarfare*, Sebastopol (California), O'Reilly, 2009.

CLAUSEWITZ, Carl von, *De la Guerre*, Paris, Editions de Minuit, 1955.

COUTAU-BEGARIE, Hervé, *Traité de Stratégie*, Paris, Economica, 2011 (7e édition).

DABILA, Antony, *L'Engagement militaire : essai de sociologie comparée*, thèse soutenue à l'Université Paris-Sorbonne le 5 novembre 2013 https://www.theses.fr/2013PA040132.pdf

DEPTULA, David & PENNEY Heather, *Restoring America's Military Competitivness : Mosaic Warfare*, Arlington (Virginie), The Mitchell Institute for Aerospace Studies, septembre 2019.

GIBSON, William, *The Neuromancer,* New York, Ace Books, 1984.

GOUROU, Pierre, *Les Terres de Bonne Espérance : le monde tropical*, Paris, Plon, coll. "Terre Humaine", 1982.

GOYA, Michel, *Res Militaris : de l'emploi des forces armées au XXIe siècle*, Paris, Economica, 2011.

HAAS, Richard, *The Bureaucratic Entrepreneur*, Washington, Brookings Institution Press, 1999

HASHIM, Ahmed S., *The Caliphate at war : Operational realities and innovations of the Islamic State*, Oxford, Oxford University Press, 2018.

HENROTIN, Joseph, *Techno-guérilla et guerre hybride*, Paris, Nuvis, 2014.

HUYGHE, François-Bernard, KEMPF, Olivier & MAZZUCHI, Nicolas, *Gagner les cyberconflits*, Paris, Economica, 2015.

KAPLAN, Fred, *Dark Territory: The Secret History of Cyber War*, New York, Simon & Schuster, 2016.

KEMPF, Olivier, *Introduction à la cyberstratégie,* Paris, Economica, 2012.

KEMPF, Olivier, *Alliances et mésalliances dans le cyberespace,* Paris, Economica, 2014.

KEMPF, Olivier, DOSSE, Stéphane & MALIS, Christian, *Le Cyberespace, nouveau domaine de la pensée stratégique,* Paris, Economica, 2014.

LIA, Brynjar, *Architect of global Jihad*, London & New York, Hurst &Columbia University Press, 2008

RID, Thomas, *Cyberwar will not take place*, Londres, Hurst, 2017 (2e ed.).

RID, Thomas, *Rise of the Machines: A Cybernetic History*, Londres, Norton & Cie, 2017 (2e ed.).

SIMONDON, Gilbert, *Du Mode d'existence des objets techniques*, Paris, Aubier-Montaigne, 1958.

SINGER, Peter W. & FRIEDMAN, Allan, *Cybersecurity & Cyberwar : What everyone needs to know*, Oxford, Oxford University Press, 2014

VENTRE, Daniel, *La Guerre de l'Information*, Paris, Hermès Lavoisier, 2007.

VENTRE, Daniel, *Cyberguerre et guerre de l'information : stratégies, règles et enjeux*, Paris, Hermès Lavoisier, 2010.

VENTRE, Daniel, *Cyberespace et acteurs du cyberconflit*, Paris, Hermès Lavoisier, 2011.

VENTRE, Daniel, *Cyberattaque et Cyberdéfense*, Paris, Hermès Lavoisier, 2011.

VENTRE, Daniel, *Chinese Cybersecurity and Defense*, Londres, Wiley-ISTE, 2014.

VENTRE, Daniel, *Information Warfare*, Londres, Wiley ISTE, 2016.

WIENER, Norbert, *Cybernetics, or control and communication in the animal and the machine*, Cambridge, Massachusetts, MIT Press, 1948 (trad. fr. *La Cybernétique, information et regulation dans le vivant et la machine,* Seuil, 2014).

WIENER, Norbert, *Cybernétique et Société*, Paris, Seuil, 2014 (1er ed. américaine 1950)

Articles

ALLEN, Greg & CHAN, Daniel, « Artificial Intelligence and National Security », Belfer Center for Science and International Affairs, Cambridge, Massachusetts, juillet 2017.

ARQUILLA, John & RONFELD David, *Cyberwar is coming!*, Santa Monica, RAND Corporation, 1993.

ARQUILLA, John, « Cyberwar Is Already Upon Us » in *Foreign Policy*, 27 février 2012.

BALZACQ, Thierry & DUNN CAVELTY Myriam, « A theory of actor-network for cyber-security » in *European Journal of International Security*, Vol.1, n° 2, Juillet 2016, pp.176-198.

BAUD, Michel, « La cyberguerre n'aura pas lieu, mais il faut s'y préparer », in *Politique étrangère* 2012, n° 2 (Eté), pp.305-316.

BERTHIER, Thierry & KEMPF, Olivier, « Vers une géopolitique de la donnée », in *Annales des Mines — Réalités industrielles*, 2016, n° 3, pp.13-18.

BOEHM, Barry, « A Spiral Model of Software Development and Enhancement », in *ACM SIGSOFT Software Engineering Notes*, ACM, n° 11, vol.4, pp.14-24, août 1986.

BOTT, Jonathan, « What's After Joint? Multi-Domain Operations as the Next Evolution in Warfare », United States Air Force School of Advanced Military Studies, Fort Leavenworth, 2017.

BRONK, Chris & ANDERSON, Gregory, « Encounter Battle: Engaging ISIL in Cyberspace » in *Cyber Defense Review*, 2017, n° 2, vol. 1.

CEBROWSKI, Arthur, « Transforming Transformation: Will it Change the Character of War? » in *Transformation Trends*, Département de la Défense, Office of Force Transformation, États-Unis, 2004.

CHEIZE, Julien, "Les Enjeux du cyberespace pour l'Armée de Terre", *Cahiers de la pensée Mili-Terre*, Centre de Doctrine et d'Enseignement du Commandement, 21 mars 2020.

DEPTULA, David & PENNY, Ether & GUNTZINGER, Mark, « Restoring Americas's Military Competitivness: Mosaic Warfare », Arlington (Virginie), The Mitchell Institute for Aerospace Studies, septembre 2019.

DUCHEINE, Paul, « Cyber warfare is taking place! » in *Internationale Spectator*, 2016, n° 6.

GARTZKE, Erik, « The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth » in *International Security*, vol. 38, N° 2, automne 2013, pp.41–73.

GARTZKE, Erik & LINDSAY, John, « Coercion through Cyberspace: The Stability-Instability Paradox Revisited » in Kelly M. Greenhill and Peter J. P. Krause (ed), *The Power to Hurt: Coercion in Theory and in Practice*, Oxford, Oxford University Presse, 2018.

GOURE, Daniel, « The M1-A2 Abrams is the tank of the future », *The National Interest*, 3 novembre 2018.

IASIELLO, Emilio, « Are Cyber Weapons Effective Military Tools? » in *Military & Strategic Affairs,* vol.7, n° 1, march 2015.

INSINNA, Valerie, « Here's the number one rule for Air Forces new advanced management System », *Defense News*, 9 juillet 2019.

KASPERSKY, Eugène, « Cyberguerre : « Il n'y a aucune preuve » selon Eugène Kaspersky », *Usbek et Rica,* 29 juin 2019, Consulté le 10 juillet 2019.

KURTI, Erdelina & HAFTOR Darek, « The Role of Path Dependence in the business model adaptation: from traditional to digital models », Proceedings of the 2014 Mediterranean Conference on Information Systems, Paper 28.

LAGNEAU, Laurent, « Nexter prépare une version du char Leclerc capable de mettre en œuvre des drones aériens », *Zone Militaire*, 21 février 2019

LAWSON, Sean, « Putting the "war" in cyberwar: Metaphor, analogy, and cybersecurity discourse in the United States » in *First Monday*, Vol.17, n° 7, juillet 2012.

LEPINARD, Philippe, « La numérisation des forces terrestres : de la numérisation de l'espace de bataille à l'organisation augmentée », 18e Congrès de l'Association Informatique et Management, Montréal, 2018.

LOCATELLI, Andrea, « The Offensive/Defensive balance in Cyberspace » in *Analysis,* n° 203, octobre 2013.

LYNN, William J. III, « Defending a New Domain: The Pentagon's Cyberstrategy » in *Foreign Affairs*, September/October 2010.

MURAWIEC, Laurent, « La Cyberguerre », in *Agir, Revue Générale de Stratégie*, décembre 1999, n° 2.

NAKASONE, Paul M., « Interview with general Nakasone », *Joint Forces Quarterly,* n° 92, 1er trimester 2019, pp.4-9

NAHOM, David, « Interview with gen. David Nahom", Mitchell Institute for Aerospace Studies, 16 avril 2020.

PAUL, Philippe, « Notions sur le combat collaboratif et observation récente des expérimentations », Cahiers de la pensée mili-terre, Paris, Centre de Doctrine et d'Enseignement du Commandement, juin 2019.

POMERLEAU, Mark, « How A New Air Force Unit Could Help Beat Russian Air Defense Systems », in *C4ISRNET*. 12 novembre 2019.

PORCHE, Isaac R. III & COLIN, P. Clarke, « Tactical Cyber: Building a Strategy for Cyber Support to Corps and Below », Santa Monica, RAND Corporation, Aroyo Center, 2017.

POST, Jonathan, « Cybernetic War », in *Omni*, mai 1979.

SINGEL, Ryan, « White House Cyber Czar : There is no Cyberwar » in *Wired,* 3 avril 2010.

SINGER, Peter & SHACHTMAN, Noah, « The Wrong War: The Insistence on Applying Cold War Metaphors to Cybersecurity Is Misplaced and Counterproductive », *Brookings*, 15 août 2011.

SUTTON, Walter S., « Cyber Operations and the Warfighting Functions », *United States Army War College*, Carlisle, Pennsylvania, 2013.

STEEL, Cherie & STEIN Arthur A., "Communications Revolutions and International Relations", in Juliann Emmons Allison (dir.), *Technology Development and Democracy: International conflict and Cooperation in the Information Age*, Albany State University of New York Press, 2002, pp.25-53.

TUCKER, Patrick, « Toward a War with fewer radio calls », *Defense One*, 21 janvier 2020.

TUCKER, Patrick, « War on auto-pilot? It will be harder than the Pentagon thinks », *Defense One,* 12 février 2020.

VENTRE, Daniel, « Cyberguerre » in *Dictionnaire de la Paix et de la Guerre*, Paris, PUF, 2017.

WIELHOUVER, Peter W. « Toward Information Supériority: The contribution of Operational Net Assessment », in *Air & Space Power Journal*, Vol. XIX, n° 3, pp.85-96.

Official Documents

United-States

« Guide for Cyber Operations », *United States Department of Defense,* 2006.

« Joint Terminology for Cyberspace Operations », *United States Department of Defense,* 2010.

« Cyberspace Operations Concept Capability Plan 2016-2028 », TRADOC Pamphlet 525-7-8, *United States Department of Defense*, 22 février 2010.

« ADP 6-0 : Mission command », Joint Publications, *United States Department of Defense*, mai 2012.

« ADRP 6-0 : Mission command », Joint Publications, *United States Department of Defense*, mai 2012.

« Cyberspace Operations », Joint Publications, *United States Department of Defense*, 5 février 2013.

« Field Manual 3-12 (R) – Cyberspace Operations », Joint Publications, *United States Department of Defense*, 5 février 2013.

« Field Manual 6-0 — Commander and Staff Organization and Operations », Joint Publications, *United States Department of Defense*, mai 2014.

« Field Manual 3-12 – Cyberspace and Electronic Warfare Operations », Joint Publications, *United States Department of Defense*, 5 février 2013.

« ATP 6-02.70 – Techniques for Spectrum Management Operations », Joint Publications, *United States Department of Defense*, décembre 2015.

« ADRP 3-0 : Operations », Joint Publications, *United States Department of Defense*, novembre 2016.

« Strategic Cyberspace Operations Guide », *United States Army War College*, Carlisle, Pennsylvania, juin 2016.

« Securing Cyber Assets: Adressing Urgent Cyber Threats to Critical Infrastructure », *National Infrastructure Advisory Council*, Washington, août 2017.

« National Cyber Strategy », Washington, Présidence des États-Unis d'Amérique, septembre 2018.

« National Defense Authorization Act (NDAA) for Fiscal Year 2019 », Public Law n° 115-232

« Us Space Force Facts Sheet », 19 décembre 2019, Washington, Departement of Defense.

« United States Air Force Posture Statement Fiscal Year 2021 », Washington, Department of Defense, février 2020.

France

« Livre Blanc de la Défense et de la Sécurité Nationale », *Ministère de la Défense*, Paris, 2008.

« PP30, plan prospectif à 30 ans », *Ministère de la Défense*, Paris, 2009.

« Rapport sur la cyberdéfense », Jean-Marie Bockel, Sénat de la République Française, juillet 2012.

« Rapport sur le risque numérique : en prendre conscience pour mieux le maîtriser », Bruno Sido & Jean-Yves Le Déaut, Assemblée Nationale et Sénat de la République Française, 3 juillet 2013.

« Livre Blanc de la Défense et de la Sécurité Nationale », *Ministère de la Défense*, Paris, 2013.

« Guide d'Hygiène Informatique », *Agence Nationale de Sécurité des systèmes informatiques*, Paris, 2014.

« Strategie Nationale de Securite Numerique », *Secrétariat Général de la Défense et de la Sécurité Nationale*, Paris, 2015.

« L'emploi des forces terrestres dans les opérations interarmées » (DFT 3.2 Tome 1 [FT-03]), Paris, Ministère de la Défense, 1er juillet 2015

« Rapport sur la présence et l'emploi des forces armées sur le territoire national », Olivier Audibert-Trouin & Christophe Léonard, Assemblée Nationale et Sénat de la République Française, 22 juin 2016

« L'armée de Terre Au Contact », *Terre Information Magazine*, Ministère de la Défense, Paris, juillet-aout 2016.

« Guide d'Hygiène Informatique », *Agence Nationale de Sécurité des systèmes informatiques*, Paris, 2017.

« Chocs Futurs : Étude prospective à l'horizon 2030 : impacts des transformations et ruptures technologiques sur notre environnement stratégique et de sécurité », *Secrétariat Général de la Défense et de la Sécurité Nationale*, Paris, avril 2017.

« Projet de loi de finance 2018 "Défense" », Assemblée Nationale de la République Française, septembre 2017.

« Revue Stratégique », *Secrétaire Général de la Défense et de la Sécurité Nationale*, Paris, 1 octobre 2017

« Revue Stratégique de Cyberdéfense », Paris, *Secrétaire Général de la Défense et de la Sécurité Nationale*, 12 février 2018

« Rapport sur les enjeux de la numérisation des armées », Olivier Becht & Thomas Gassilloud, Assemblée Nationale et Sénat de la République Française, 30 mai 2018.

« Politique ministérielle de lutte informatique défensive », Paris, *Ministère des Armées,* janvier 2019.

« Politique ministérielle de lutte informatique offensive », Paris, *Ministère des Armées,* janvier 2019.

« Stratégie Nationale du Renseignement », Coordination Nationale du Renseignement et de la Lutte contre le Terrorisme, Paris, Ministère de l'Intérieur, juillet 2019

United Kingdom

« Cyber Primer » 2nd ed., *Development, Concepts and Doctrine Centre, United Kingdom Ministry of Defense* Shrivenham, Wiltshire, juillet 2016.

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