Digital sovereignty: The role of the armed forces

Arnaud Coustillière,
Vice-admiral, managing director of information et communication systems, Ministry of the Armed Forces

Abstract:
The Ministry of the Armed Forces plays a major role in national sovereignty in the digital realm. The French Constitution legitimates the armed forces as the ultimate defense of the state's sovereignty; and cyberspace is no exception. Rapid changes in technology and society are forcing us to clarify the armed forces' conception of their assignment in cyberspace. Before describing the Ministry's role, national sovereignty is discussed in terms of defense. The Ministry of the Armed Forces is seeking, in digital matters, to acquire knowledge for anticipating events and the capacity to undertake actions to fulfill its duties.

> "*Armies have to plan and conduct operations in the digital realm, down to the tactical level, fully integrated in the chain of command for planning and conducting kinetic military operations.*" (*Revue stratégique*, §299, October 2017)

Sovereignty

Cyberspace is an artificial environment in three layers: hardware (servers, networks, terminals), software (software, robots, operation systems) and a cognitive layer (information, social relations). An object in cyberspace has coordinates in these three dimensions. The dependance of devices on these three dimensions does not hamper the fluidity of exchanges. Quite to the contrary, factors such as space and time, which determine other spaces, are erased, even made unoperational. Individuals or firms can be attacked even inside a nation's borders. Cyberspace is nearly homogeneous. From this homogeneity ensue the properties of ubiquity, anonymity and remanence. For instance, the information placed on an electronic network might be simultaneously located in several places. The cost of tracking its movements is high; and it is unrealistic to want to delete all traces of it.[1]

It is not evident how the concept of sovereignty applies to cyberspace. One approach would be to make comparisons with other, familiar environments over which we exercise control. Sovereignty understood as being land- or earth-based is a SOVEREIGNTY OF OWNERSHIP; and control over the environment entails a standing occupation of the soil. When the seas were "conquered", a new concept of sovereignty was worked out. Part of the sea fell under the concept of territorial continuity, but the high sea belongs to no one, and ships belong to the flag flown. To signal its position, a nation-state places ships on the high sea and intermittently conducts surveillance: this is a SOVEREIGNTY OF PRESENCE, *i.e.*, exercised by being present. Air space, an extension of the land over which flights pass, refers to the sovereignty of ownership or of presence depending on the place. The case of airports is noteworthy: it is a "passage", where control must remain flexible. In an airport, sovereignty is a mix of ownership and of presence completed with considerations

[1] This article, including any quotations from French sources, has been translated from French by Noal Mellott (Omaha Beach, France). The translation into English has, with the editor's approval, completed a few bibliographical references.

about access. Finally, sovereignty in outer space has its own rationale: a SOVEREIGNTY OF ACCESS. A state is sovereign there when it can freely access this space.

As for cyberspace, it belongs to no one, but everyone has access to it. Since it is materially established in a place, some states have chosen to "territorialize" the Internet so as to exercise more control over their own cyberspace. Russia, Iran and China have made this choice, but neither France nor other Western nations. By conceiving of cyberspace as a place both of freedom and of law, the French state has set the objective of sovereignty in cyberspace for its armed forces as the capacity for conducting digital interventions there for the sake of the national interest but without exercising standing control. This form of sovereignty can be said to be a SOVEREIGNTY OF ACTION.

The Ministry of Armed Forces: Its ambitions in cyberspace

Exercising sovereignty means having a strategy that fully fits in with the state's digital policy. The role of the armed forces in cyberdefense was presented in an official report in 2008 and then confirmed, with new objectives, by another report in 2013.[2] In 2015, Prime Minister Manuel Valls set the objectives of a national strategy for digital security;[3] and Jean-Yves Le Drian, minister of Defense, created a Cyber Command (COMCYBER) in December 2016 while emphasizing that "*cyber weapons are full-fledged weapons, part of the means at the disposal of the military high command*".[4] Cyber reality now has a place in France's defense policy. The digital dimension is present everywhere in the "*strategic review of defense and national security*" submitted in October 2017 to the president.[5]

More broadly, by taking account of operations, of the personnel's everyday activities and of relations with citizens, Florence Parly, minister of the Armed Forces, approved the document *Ambition numérique* in November 2017. Convinced that the digital revolution will be a strong vector of this transformation, she wants "*to place it at the service of the Ministry. The Internet of things, artificial intelligence and big data are works under way which we can use to bolster the success of our weapons and the efficiency and excellence in the leadership of all the Ministry's missions.*"[6] The digital revolution is a powerful driving force changing all big organizations and accelerating their performance. Having resolutely made the decision, the Ministry and armed forces are seizing this opportunity to remain on the cutting edge of the best technology and practices. The purpose of this shift is to adopt, as soon as possible and in the best conditions, emerging techniques for fostering breakthroughs in practices, organizations, work methods and forms of action.

Since this approach centers around electronic data, it is necessary to improve data processing, to better secure data at the national level and to share data for the benefit of the the armed forces' actions during military operations and in the everyday operation of the Ministry itself.

As a pillar for confidence-building, the issue of digital identification is important for reasons of state. Deploying digital identifications and making them secure and viable are indispensable for generalizing a dematerialized approach in trade and in the citizen's relations with a modern public administration.

---

[2] Respectively: http://archives.livreblancdefenseetsecurite.gouv.fr/2008/IMG/pdf/livre_blanc_tome1_partie1.pdf & http://www.livreblancdefenseetsecurite.gouv.fr/pdf/le_livre_blanc_de_la_defense_2013.pdf.

[3] https://www.ssi.gouv.fr/actualite/la-strategie-nationale-pour-la-securite-du-numerique-une-reponse-aux-nouveaux-enjeux-des-usages-numeriques/

[4] http://discours.vie-publique.fr/notices/163003632.html

[5] Revue Stratégique de Défense et de Sécurité Nationale: https://www.defense.gouv.fr/dgris/presentation/evenements/revue-strategique-de-defense-et-de-securite-nationale-2017.

[6] https://www.defense.gouv.fr/actualites/articles/innovation-numerique-le-ministere-poursuit-sa-transformation

As part of its “digital ambitions”, the Ministry of Armed Forces has given a meaning to digital sovereignty through its determination to amplify the capacity for rapid developments, thus favoring the use of open-source software, a powerful factor of independence and agility in making new services available.

Apart from the technology as such, the intent is to attract the new talents of innovators and to make jobs in information and communications technology (ICT) at the Ministry more agile and attractive. In 2018, the DGNUM (Direction Générale du Numérique et des Systèmes d’Information et de Communication, previously DGSIC) was assigned to orchestrate this process of in-depth modernization, to speed it up in conformity with the 2022 interministerial action plan.[7] Three strategic objectives shape this approach: *a)* guarantee operational superiority and the control of information on the theaters of operations; *b)* make the mediums used more efficient and facilitate the personnel’s everyday activities; and *c)* improve relations with citizens and enhance the Ministry’s attractiveness.

At stake: Anticipation and intelligence

Anticipation, an action with many channels, relies on information garnered through intelligence, both for its finality and in strategic monitoring activities. In the long run, the aim is to anticipate trends and tendencies so as to enable France to decide and act autonomously and sovereignly. The strategic monitoring conducted by the Ministry of the Armed Forces has this role.

In the short run and for the purpose of potential actions, the need for intelligence is decisive. Theoretically, a line separates intelligence of “cyber origins” from intelligence of “cyber interest”. The first is intelligence coming from open sources (mainly but not always the Internet), computer searches and the examination of digital mediums (such as hard drives, USB sticks, telephones, tablets or the electronics in weapon systems), whereas the latter purposes to provide the military chain of command for cyberdefense with the information that has to be known and understood in order to operate in security in cyberspace. It seeks to evaluate cybethreats against forces on operations and to seize opportunities in the enemy camp.

The capacity for exchanging information both among services in the Ministry and with our allies and for orienting searches is essential. This process involves the classical cycle in intelligence: orientation, search-and-find, exploitation, diffusion.

The capacity for action

> “*The considerable issue represented by cyber threats calls for substantially reinforcing both the defensive and offensive means of France. The capacity for detecting and attributing attacks, which depends on acquiring intelligence of human and technical origin, will be a key element*” (*Revue stratégique*, §299, October 2017).

Ultimately, sovereignty is guaranteed by the capacity for conducing actions. This capacity has two requirements: the resilience of the systems of the armed forces and the holding of options, defensive as well as offensive.

By enthusiasm, we might confuse the resilience necessary for sovereignty with the independence or full autonomy of the means to be used. In a globalized economic system, this orientation turns out not to be pertinent, since the armed forces are unable to control from start to stop the autonomy of their production in electronics and ICT. Since this position is shared with partners, the choice has been made to tightly secure only what is vital in an environment that is felt to lack security.

[7] https://www.economie.gouv.fr/lancement-programme-action-publique-2022

The armed forces thus need to exercise control over but a few specific components in order to be able to make secure a system built of bricks that lack reliability. This means, first of all, having sovereign cryptographic tools for ensuring the integrity and confidentiality of data. It then means controlling networks via, in particular, the possession of fully controlled and reliable sensing probes so as to guarantee the availability of data. Finally, national algorithms are needed to process data. Disposing of these means fills the armed forces' fundamental needs.

The lack of systematic certification of hard- and software is offset by encrypting procedures and the readiness for service. Furthermore, the armed forces, though not autonomous with regard to hard- and software, can be considered to be independent owing both to the diversity of suppliers and manufacturers, and to the use of several protected, physically separate networks. It is illusory to believe that all hard- or software can come from France or Europe. Efforts oriented in this direction would prove useless: digital products can never be deemed perfectly reliable, not even if the armed forces developed their own. Furthermore, keeping them up to date and in secure conditions very often bears major costs; and this makes proprietary software from outside the nation very attractive.

The development of the data sciences and machine learning are creating a new need: the need to possess national sets of labeled data to be used for machine learning and for evaluating algorithms.[8] For example, in an environment increasingly dependent on intelligence from open sources and search engines, it is important to be able to assess the reliability and biases of public search engines. This is true even beyond the limits of the armed forces as such. It raises questions about the confidence to be placed in algorithms that are not public. The validation of private algorithms by secret sets of data managed under the control of public authorities could satisfy the need for certification.

Le second aspect of the capacity for action is to maintain a defensive or offensive striking force ready to serve. An omnipresent cyberspace is a strategic stake, both civilian and military. The international community has had difficulty adapting international law to this situation. Besides the big and some middle-sized powers that have a full capacity for cyberactions and that, owing to political or economic competition, can conduct unfriendly actions in intelligence, several nations or organizations can conduct operations that extend beyond spying. We must also reckon with activist groups, in particular those linked to international terrorism and/or various forms of nationalism.

Cyberspace has turned into a full-fledged battlefield. The armed forces must have the capacity for acting in this environment. Likewise, the state, through its institutions, must maintain its operations, the activities of vital importance, security and economic activities, in the face of cyber threats. These threats fall into three groups: those that directly target information, those aimed at information systems and those that pass through cyberspace but are aimed at physical targets (critical equipment and installations, etc.).

In cyberspace, the concept of evidence and ideas about the attribution of actions are much more complex to discern. This modifies the classical balance of power between assailant and defender: the assailant's relative advantage is bolstered by the proliferation of attack techniques (*e.g.*, Wannacry, a sort of self-replication ransomware). It is tricky undertaking an action in cyberspace, and France wants, defensively and offensively, to be a driving force in the construction of an international order.

The Ministry of the Armed Forces has a definite role in the nation's digital sovereignty: guarantee both a high level of performance of all components by benefitting from the digital revolution and, too, deploy its forces for combat in this new space. To guarantee lasting success, the armed forces are undergoing a digital transformation of their processes and equipment. The creation of COMCYBER and the DGNUM in 2018 demonstrates that the Ministry has adapted its organization to respond to challenges in cyberspace, an evolving environment, compressed and immediate, that raises questions for all our models.

[8] "Supervised learning" entails using data that match results (the "labels"), which are verified manually or by robots. The biases of labeling due to the set of training data will be "engraved" in the algorithm's functions.