



Digitisation of data processing

military-Earth thinking notebook

le Lieutenant-Colonel Victor LE BIHAN

Published on 13/01/2020

Sciences & technologies

Cyberspace has expanded extremely rapidly and has become intrinsic to our society. It is a place of expression and individual freedoms, of exchange and wealth creation.

Although it is based on computer architectures ("hardware"), cyberspace is an essentially immaterial medium that exists and makes sense only through information. Information can be understood in two ways: as digital data (processed, stored, consulted, manipulated) and as traditional, i.e. semantic, information that is full of meaning for human intelligence.

The majority of sectors of activity today rely on information and communication technologies (ICT). Information is emerging as one of the keys to industrial, economic, cultural and operational superiority. Big data, open data, datacenter, datascientist, personal data, all these terms are mostly used by Anglo-Saxon companies and testify to the central place taken by digital data in our post-modern societies riveted on the screens of our smartphones, phonebooks, tablets, computers ?

Cyberspace accentuates the preponderance of information in conflict. War is "info-centric". One of the effects induced by the revolution in military affairs (RAM) has been to push back the fog of war through better exploitation of information.

Cyberspace is a space for sharing, allowing the instantaneous transmission of all information to the multitudes. It abolishes the notion of the front line and, in so doing, on the one hand the decision-maker finds himself at the heart of the action with the risk of obliterating his judgement at a level of detail that is not his own; on the other hand each citizen becomes a combatant of the digital world: depositary, vector and target of information. Consequently, the issues at stake concern both the capture and exploitation of information.

The use of cyberspace increases tenfold the possibilities of capturing information and complements traditional intelligence gathering techniques. The Internet offers a profusion of digital data that requires increasingly sophisticated and powerful research and analysis tools: big data, which is aimed at analyzing large volumes of data. This is the strength of GAFA¹ which values our personal data through targeted advertising. "When it's free, you're the product". The paradox is the naive attitude of the user: so careful to protect his private life from public authorities and who willingly contributes to the dissemination of his personal or even professional information.

The offensive computer battle offers the opportunity to enter the adversary's digital battle space and to access its digital data, particularly for intelligence purposes.

The corollary is the growing importance of cybersecurity (cyber protection and defensive computer warfare) to protect friendly digital space. It is a question of defending access to our information systems and ultimately protecting our digital data. Digitization offers new techniques for concealing information (steganography, generalization of encryption). It is an endless iterative struggle whose aim must not be absolute protection but to ensure that information is properly protected until its relative value expires.

For the protection of digital data, the user remains the first line of defence. He has a central role both as a sensor of weak signals that may indicate a discreet and complex attack in progress but also as a source of vulnerabilities through ignorance or by seeking to break security rules.

The second issue is the exploitation of information. The prerequisite is "information management": making sure that the right information reaches the right person in time and thus allowing it to be properly taken into account. Here again, digital technologies support the treating officers by allowing them to analyze a greater amount of information. Predictive analysis, such as the chess player tries to predict the opponent's next move from the numerical data collected. Thus, the patrols of Operation SENTINELLE in Paris can be optimized by analyzing the sectors and periods during which incidents occur.

Finally, **it is necessary to challenge the adversary in cyberspace**. Digital technology has become the preferred medium for propaganda or destabilization actions because of the rapid dissemination of information offered in particular by social networks and the possibility of publishing and disseminating information without any geographical notion. Thus, the Internet makes it possible to act on the perceptions of a large number of actors in order to disseminate an ideology, recruit new supporters, dissuade opponents, give instructions or raising funds.

The digital component of information operations (digital information operations or digital psyops) makes it possible to act on the perceptions of the adversary, to disrupt or neutralize the opposing device. These operations, which target the semantic and social layer of cyberspace via technical and cognitive actions, can have effects at the tactical, operational and strategic levels.

In conclusion, cyberspace multiplies the means and fields of the struggle for information control, a factor of operational superiority. It generates new vulnerabilities but which can be transformed into opportunities if we know how to seize them.

¹ GAFA or GAFAM: Google, Apple, Facebook, Amazon, Microsoft.

Title : le Lieutenant-Colonel Victor LE BIHAN
Author (s) : le Lieutenant-Colonel Victor LE BIHAN
Release date 12/09/2018