Cyber, cyber... Did you say cyber?

BRENNUS 4.0

Par le colonel Jean-Michel Fouquet, directeur de l'enseignement militaire supérieur scientifique et technique du CDEC

Published on 15/03/2020

Sciences & technologies

"What is well conceived is clearly stated, and the words to say it come easily." Nicolas Boileau (1636 - 1711)

Cybernetics, cyber defence, cyber attack, cyber protection, cybersecurity: all terms using the prefix "cyber-". This prefix, which "serves to form many words relating to the use of the Internet network"[1], is however too often used alone, without any additions being associated with it to constitute a derived word with a specific meaning. This abusive use generates many questions, even misunderstandings, and harms the appropriation of terms that are nevertheless clear and intelligible.

It is therefore necessary to make the necessary effort to be precise in the terms used so that "the words come easily to us" and the action is conceived with a clear vision of the spirit of the mission.

Before cyber defence, there was cybernetics, which the Larousse dictionary defines as follows: A "goal-oriented science of action, based on the study of control and communication processes in living beings, in machines and in sociological and economic systems". »

Thus the adjective cybernetics refers to that which is related to cybernetics.

Plato, in his dialogues, already used the term "kubernêtikê", derived from the verb "kubernân", to govern, which he illustrated with numerous examples, from piloting a ship to governing men. He had grasped the structure of all goal-oriented processes of action, based on the comparison of the evolution of the governed system with its desired evolution.

From 1834 onwards, the French mathematician, physicist, chemist and philosopher André-

Marie Ampère[2] used the name cybernetics to refer to "the science of human government".

During the Second World War, American radar specialists applied their knowledge of electronic reaction chains to the design of systems capable of tracking a target and destroying it at the command of a firing computer. Exchanges between physicists, electronics engineers and mechanics, joined by biologists, sociologists and economists, continued under the aegis of the mathematician Norbert Wiener[3] (1894-1964), who defined cybernetics as a science that exclusively studies communications and their regulation in natural and artificial systems.

In the 1980s, the term cyberspace - cyberspace or cybernetic space - appeared in the pen of the American science-fiction author William Gibson[4]. 4] The term cyberspace, which has been taken up by many authors of the genre, goes beyond the realm of anticipation to encompass the world of science and information.

Thus, for the French philosopher, sociologist and researcher in information and communication sciences Pierre Lévy, "cyberspace refers to the universe of digital networks as a place of encounters and adventures, an issue of world conflicts, a new economic and cultural frontier. Cyberspace refers less to the new information media than to the original modes of creation, navigation in knowledge and social relations that they enable . 5] For all those working in this field, the short definition of cyberspace commonly accepted is the communicating digital space.

With these definitions in mind, what about cyber defence?

According to the French National Agency for the Security of Information Systems (ANSSI), cyber defence refers to "all technical and non-technical measures enabling a State to defend in cyberspace information systems deemed essential" .

It thus includes all the physical and virtual means put in place by a country in the context of cyber warfare in cyberspace.

Like defence, which has two pillars,[6] cyber defence is based on military and non-military actions in cyberspace.

At the level of armies, while the subject had been practiced as early as 2008-2009, the concept of cyber defence promulgated in July 2011 (CIA-6.3_CYBERDEF) provided the following definition of cyber defence: " all activities conducted by the Ministry of Defence in order to intervene militarily or non-militarily in cyberspace to guarantee the effectiveness of the action of the armed forces, the accomplishment of the missions entrusted to them and the proper functioning of the Ministry ". Cyberspace is seen as a new environment of confrontation in which various types of malicious actions can be carried out by a wide range of potential perpetrators with different motivations. Based on measures to protect information systems, cyber defence combines active and in-depth defence of information systems, cyber crisis management capability and a capacity to fight in cyberspace.

The 12 September 2013 Use of Force Concept, CIA-01(A)_CEF(2013), refers to cyberspace as one of the two fields of immaterial confrontation, the second being the field of perceptions. Cyberspace thus represents a fifth medium, along with air-land, maritime, air

and outer space, hence the term 5D commonly used to refer to it.

Based on the concept of force employment, operations in cyberspace are the subject of updated joint doctrine promulgated on 5 September 2018, DIA-3.20(A)_OPS-CYBER(2018), Operations in Cyberspace.

It considers cyberspace as "the substrate without which virtually no activity is possible in other environments. It also has intersections with other fields of confrontation (electromagnetic and information environments). It is both an area of vulnerability in which the threat is constantly being perfected, but also an area of opportunity which enables the armed forces to acquire intelligence and to obtain effects on a range of actors" .

Within this framework, military action in cyberspace is organised around two main pillars: cybersecurity and military cyber defence.

Cybersecurity is a sought-after state, which allows the Ministry of the Armed Forces to continue to operate, even under cyber aggression. It is based on the combination of cyber protection, which is synonymous with information systems security (ISS), the resilience of our systems and organisations in the event of attack, and defensive cyber warfare (LID) [7].

7] Military cyber defence, on the other hand, is the set of actions carried out in or through cyberspace to preserve a force's freedom of action in cyberspace and/or achieve effects in order to achieve the objectives of the force commander. Military cyber defence is not the military component of cyber defence. It is specific to the Ministry of the Armed Forces. Indeed, its scope includes engagement and intelligence actions.

On the strength of all these definitions, it is now necessary to show clarity in the use of terms and to banish cyber barbarism, which, while referring to the cybernetic domain, leads to numerous mental translations and misunderstandings. In the same way that a mechanical specialist defines his or her frame of reference before tackling and solving a problem, precision in terms relating to the cybernetic field will ensure that the problem is solved.a better understanding by all the actors of cyber defence, and therefore a better efficiency in actions in cyberspace, especially in the framework of the implementation of the French cyber defence strategy.

———————-

[1]. Dictionnaire Larousse 2016.

[2]. Essai sur la philosophie des sciences ou Exposition analytique d'une classification naturelle de toutes les connaissances humaines, 1834.

[3]. Cybernetics, or Control and Communication in the Man and the Machine, 1948, marks the beginning of the development of cybernetics. This book presents the main scientific concepts and methods that emerged during and after the Second World War, linking the then nascent fields of automation, electronics and computer science with problems specific to the functioning of living beings. Norbert Wiener is one of the fathers of information theory, computer science, and the mathematical theory of electronics, communications and automation.

[4]. Burning Chrome (in French Gravé sur Chrome), short story published in July 1982 in the journal Omni: cyberspace was then defined as an abstract representation of the relations between data systems.

[5]. Collective intelligence. Pour une anthropologie du cyberespace, Paris, La Découverte, 1997.

[6]. La doctrine interarmées d'emploi des armées sur le territoire national du 28 juin 2016 - DIA-3.60_EATN(2016) - states that defence is based on military defence (measures and postures prescribed to ensure the defence of the territory and its approaches, in all material and immaterial spaces, against armed aggression) and non-military defence (civil and economic defence).

[7]. To be fully accurate, the LID officially overlaps cybersecurity and cyber defence and represents a source of confusion that should be removed: integration of the LID into cyber defence? Removal of the term?

Title : Par le colonel Jean-Michel Fouquet, directeur de l'enseignement militaire supérieur scientifique et technique du CDEC

Author (s) : Par le colonel Jean-Michel Fouquet, directeur de l'enseignement militaire supérieur scientifique et technique du CDEC

Release date 12/03/2020

FIND OUT MORE