

Cyber, cyber... Vous avez dit cyber ?

BRENNUS 4.0

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

publié le 15/03/2020

Sciences & technologies

«Ce que l'on conçoit bien s'énonce clairement, et les mots pour le dire arrivent aisément.»

Nicolas Boileau (1636 – 1711)

Cybernétique, cyberdéfense, cyberattaque, cyberprotection, cybersécurité : autant de termes utilisant le préfixe « cyber- ». Ce préfixe qui « sert à former de nombreux mots relatifs à l'utilisation du réseau Internet »[1] est pourtant trop souvent utilisé seul, sans qu'aucune adjonction n'y soit associée pour constituer un mot dérivé à la signification bien précise. Cette utilisation abusive est génératrice de nombreuses interrogations, voire d'incompréhensions et nuit à l'appropriation de termes pourtant clairs et intelligibles.

Aussi convient-il de faire l'effort nécessaire pour être précis dans les termes employés afin que « les mots nous arrivent aisément » et que l'action se conçoive avec une claire vision de l'esprit de la mission.

Avant la cyberdéfense, il y a eu la cybernétique dont le dictionnaire Larousse donne la définition suivante : « science de l'action orientée vers un but, fondée sur l'étude des processus de commande et de communication chez les êtres vivants, dans les machines et les systèmes sociologiques et économiques. »

Ainsi l'adjectif cybernétique désigne-t-il ce qui est relatif à la cybernétique.

Platon, dans ses dialogues, utilisait déjà le terme « kubernêtikê », issu du verbe « kubernân », gouverner, qu'il illustrait de nombreux exemples, allant du pilotage d'un navire au gouvernement des hommes. Il avait saisi la structure de tous les processus d'action orientés vers un but, fondée sur la comparaison de l'évolution du système gouverné avec son évolution désirée.

À compter de 1834, le mathématicien, physicien, chimiste et philosophe français André-Marie Ampère[2] use du nom cybernétique pour désigner « la science du gouvernement des hommes ».

Au cours de la Seconde Guerre mondiale, des spécialistes américains du radar appliquent leurs connaissances des chaînes de réaction électroniques à la conception de systèmes capables de suivre une cible et de la détruire sur ordre d'un calculateur de tir. Les échanges entre physiciens, électroniciens et mécaniciens, auxquels se joignent biologistes, sociologues, économistes, se poursuivent sous l'égide du mathématicien Norbert Wiener[3] (1894-1964) qui définit alors la cybernétique comme une science qui étudie exclusivement les communications et leurs régulations dans les systèmes naturels et artificiels.

Dans les années 1980, le terme de cyberspace – en français, cyberespace ou espace cybernétique – apparaît sous la plume de l'auteur de science-fiction américain William Gibson[4]. Repris par de nombreux auteurs du genre, le terme de cyberespace déborde du seul milieu de l'anticipation pour irriguer celui des sciences et de l'information.

Ainsi, pour le philosophe, sociologue et chercheur en sciences de l'information et de la communication français Pierre Lévy, « le cyberespace désigne l'univers des réseaux numériques comme lieu de rencontres et d'aventures, enjeu de conflits mondiaux, nouvelle frontière économique et culturelle. [...] Le cyberespace désigne moins les nouveaux supports de l'information que les modes originaux de création, de navigation dans la connaissance et de relation sociale qu'ils permettent »[5]. Pour l'ensemble de ceux qui oeuvrent dans ce domaine, la définition courte communément admise du cyberespace se résume à l'espace numérique communiquant.

Ces définitions étant posées, qu'en est-il de la cyberdéfense ?

Selon l'agence nationale de la sécurité des systèmes d'information (ANSSI), la cyberdéfense désigne « l'ensemble des mesures techniques et non techniques permettant à un État de défendre dans le cyberespace les systèmes d'information jugés essentiels ».

Elle regroupe donc l'ensemble des moyens physiques et virtuels mis en place par un pays dans le cadre de la guerre informatique menée dans le cyberespace.

À l'instar de la défense qui comporte deux piliers[6], la cyberdéfense s'articule autour des actions militaires et des actions non militaires dans le cyberespace.

Au niveau des armées, alors que le sujet avait été pratiqué dès les années 2008-2009, le concept de cyberdéfense promulgué en juillet 2011 (CIA-6.3_CYBERDEF) a permis de donner la définition suivante de la cyberdéfense : « ensemble des activités conduites par le ministère de la défense afin d'intervenir militairement ou non dans le cyberespace pour garantir l'efficacité de l'action des forces armées, la réalisation des missions confiées et le bon fonctionnement du ministère ». Le cyberespace y est vu comme un nouveau milieu de confrontation dans lequel peuvent être conduits divers types d'actions malveillantes, par un large spectre d'auteurs potentiels aux motivations variées. S'appuyant sur les mesures de protection des systèmes d'information, la cyberdéfense regroupe la défense active et en profondeur des systèmes d'information, la capacité de gestion de crise cybernétique et une capacité de lutte dans le cyberespace.

Le concept d'emploi des forces du 12 septembre 2013, CIA-01(A)_CEF(2013), fait référence au cyberespace en tant qu'un des deux champs d'affrontement immatériel, le

second étant le champ des perceptions. Le cyberspace représente ainsi un cinquième milieu, avec les milieux aéroterrestre, maritime, aérien et l'espace exo-atmosphérique, d'où le terme 5D couramment employé pour le désigner.

S'appuyant sur le concept d'emploi des forces, les opérations dans le cyberspace font l'objet d'une doctrine interarmées actualisée et promulguée le 5 septembre 2018, la DIA-3.20(A)_OPS-CYBER(2018), Opérations dans le cyberspace.

Le cyberspace y est considéré comme « le substrat sans lequel quasi aucune activité n'est possible dans les autres milieux. Il possède par ailleurs des intersections avec d'autres champs de confrontation (environnements électromagnétique et informationnel). Il est à la fois un espace de vulnérabilité dans lequel la menace ne cesse de se perfectionner, mais également un espace d'opportunités qui permet aux forces armées d'acquérir du renseignement et d'obtenir des effets sur un ensemble d'acteurs ».

Dans ce cadre, l'action militaire dans le cyberspace s'organise autour de deux grands piliers : la cybersécurité et la cyberdéfense militaire.

La cybersécurité est un état recherché, qui permet au ministère des Armées de continuer à fonctionner, y compris sous agression informatique. Elle repose sur la combinaison de la cyberprotection, synonyme de sécurité des systèmes d'information (SSI), de la résilience de nos systèmes et de nos organisations en cas d'attaque et de la lutte informatique défensive (LID)[7].

La cyberdéfense militaire représente, quant à elle, l'ensemble des actions menées dans ou au travers du cyberspace afin de préserver la liberté d'action d'une force dans le cyberspace et/ou réaliser des effets en vue d'atteindre les objectifs du commandant de la force considérée. La cyberdéfense militaire n'est pas le volet militaire de la cyberdéfense. Elle est spécifique au ministère des Armées. En effet, son périmètre comprend des actions d'engagement et de renseignement.

Fort de l'ensemble de ces définitions, il convient désormais de faire preuve de clarté dans l'emploi des termes et de bannir le barbarisme cyber qui, tout en faisant référence au domaine cybernétique, induit de nombreuses traductions mentales et de multiples incompréhensions. De la même manière qu'un spécialiste en mécanique définit son référentiel d'étude avant d'aborder et résoudre un problème, la précision dans les termes relevant du domaine cybernétique sera gage d'une meilleure compréhension par l'ensemble des acteurs de la cyberdéfense, et donc d'une efficacité renforcée dans les actions dans le cyberspace, notamment dans le cadre de la mise en oeuvre de la stratégie française de cyberdéfense.

[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, marque le début du développement de la cybernétique. Cet ouvrage présente les principaux concepts et méthodes scientifiques apparus pendant et après la Seconde Guerre mondiale, liant les domaines alors naissants de l'automatique, de l'électronique et de l'informatique à des problématiques propres au

fonctionnement des êtres vivants. Norbert Wiener est l'un des pères de la théorie de l'information, de l'informatique, et de la théorie mathématique de l'électronique, des communications et de l'automatique.

[4]. Burning Chrome (en français Gravé sur Chrome), nouvelle publiée en juillet 1982 dans la revue Omni : le cyberspace est alors défini comme une représentation abstraite des relations entre les systèmes de données.

[5]. L'intelligence collective. Pour une anthropologie du cyberspace, 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) – stipule en effet que la défense repose sur la défense militaire (mesures et postures prescrites pour assurer la défense du territoire et de ses approches, dans tous les espaces matériels et immatériels, face à une agression armée) et la défense non militaire (défense civile et défense économique).

[7]. Pour être pleinement exact, la LID chevauche officiellement la cybersécurité et la cyberdéfense et elle représente une source de confusion qu'il conviendrait de lever : intégration de la LID dans la cyberdéfense ? Suppression du terme ?

Titre :	Par le colonel Jean-Michel Fouquet, directeur de l'enseignement militaire supérieur scientifique et technique du CDEC
Auteur(s) :	Par le colonel Jean-Michel Fouquet, directeur de l'enseignement militaire supérieur scientifique et technique du CDEC
Date de parution	12/03/2020

EN SAVOIR PLUS
