ÉCOLE DE GUERRE

PROMOTION *GÉNÉRAL GALLOIS*

2016 -2017

De la pensée cybernétique à la défense du cyberespace : pour une armée chargée de la maîtrise de l'espace cybernétique.

Chef de bataillon Cyrille LACROIX

Sous la direction de :

CF Audrey HERISSON

Professeur à l'Ecole de Guerre

Résumé

Le cyberespace, nouveau milieu stratégique ? La question ne se pose plus. Tant pour les armées que pour la société civile, l'enjeu consiste à utiliser les formidables capacités de ce monde numérique, sans pour autant être victime de sa propre dépendance, identifiée par de potentiels concurrents ou adversaires. Alors, au sein du ministère français de la Défense, faut-il intégrer de manière transverse cette problématique au sein des autres milieux de confrontation : terre, air, mer et espace ? Ou, est-il nécessaire de considérer l'importance de la question pour apporter une réponse forte, passant par la création d'une armée dédiée ? C'est tout le sujet de cette étude, qui apporte un éclairage historique et scientifique sur l'appréhension de ce nouveau défi. En établissant un pont entre les théories originelles de la cybernétique de la fin de la Seconde Guerre Mondiale et l'état actuel des actions menées dans le monde militaire pour assurer la défense du cyberespace, c'est une vision globale qui est mise en avant.

Les principes fondamentaux issus de la pensée cybernétique sont utilisés pour qualifier les mises en place actuelles de capacités d'opération sur le cyberespace, proposer des orientations, justifier de la pertinence de la création d'un domaine CYBER militaire et d'une armée dédiée.

Abstract

Is cyberspace a new strategic environment? The answer is of course yes, there remains no more ambiguity. For both military forces and civil society, the challenge is to take advantage of the newest capabilities of this digital world, without being a victim of its own dependency, identified by the potential competitors or opponents. Regarding the French Ministry of Defense, is it necessary to integrate this problem inside each of the components individually: ground, air, maritime and space? Or, due to the sensitivity of the question, is it more reasonable to answer strongly by the creation of a dedicated army? This is the whole subject of this study, which brings historical and scientific insights into the apprehension of this new challenge. Establishing a bridge between original theories of cybernetics, born at the end of the Second World War, and the current state of affairs in the military world to ensure cyberspace defense, leads to a promotion of a global vision.

Fundamental principles of cybernetic thinking are here used in order to qualify the current affairs concerning cyberspace operations, to propose orientations, to justify the relevance of creation of a military CYBER domain and of a dedicated service.

Plan

Introduction

Le terme « cyber » est aujourd'hui utilisé pour décrire des outils ou phénomènes très récents : cyberespace, cybersécurité, cybercriminalité, *etc*. et se place au centre de nombreux enjeux sécuritaires : protection de la vie privée, intégrité des systèmes financiers, défense, confidentialité des décisions politiques, notamment. Il paraît donc utile de revenir sur la science à l'origine de ce terme : la cybernétique. Ce besoin naît de deux volontés : celle de savoir si la direction donnée au développement technologique nous permet de rester optimiste face aux enjeux sécuritaires et éthiques ; et celle de savoir si les principes établis par la pensée cybernétique sont toujours respectés dans ce développement technologique et plus particulièrement dans la défense des outils technologiques placées au cœur de nos organisations humaines actuelles.

Pour Norbert Wiener, le créateur de cette science, la cybernétique est « *la théorie de la commande et de la communication* » entre machines ou êtres vivants[1]. La pensée cybernétique consiste à travailler par analogie, selon Louis Couffignal, pour obtenir une « *efficacité dans le guidage de l'action* »[2]. Pour lui, « *la cybernétique est l'art de rendre efficace l'action* »[3]. Dès la naissance de cette science, à la fin de la Seconde Guerre Mondiale, les travaux de Norbert Wiener sont transdisciplinaires, visant la recherche de mécanismes biologiques, physiques ou humains réutilisables dans le domaine technologique et surtout, pouvant être automatisés par une machine. Au final, la cybernétique couvre bien le champ de développement des machines, des robots, des ordinateurs, de l'intelligence artificielle, permettant de reproduire les capacités humaines, les compléter ou les dépasser. Mais cette science ne se réduit pas à ce champ, car elle s'intéresse et s'appuie sur tous les domaines connexes permettant de décrire les relations entre les créations humaines et l'homme : théorie de l'information, réseaux de neurones, économie, ou éthique, notamment. La difficulté de définition de cette science est résolue par Wiener lui-même, en utilisant le terme grec « *kubernêtês* » (pour cybernétique), signifiant le pilote ou le gouverneur[4]. La cybernétique est l'étude des mécanismes automatisés, des mécanismes de commande et de communication, permettant de décrire l'origine des comporte-

[1] WIENER Norbert, *La Cybernétique, information et régulation dans le vivant et la machine*, Paris, Seuil, 2014, 370, p.70 : « *Nous avons décidé de donner à la théorie entière de la commande et de la communication, aussi bien chez l'animal que dans la machine, le nom de cybernétique* ». Il faut noter que pour l'auteur, dans un cadre scientifique, l'homme fait partie des animaux, dans cette définition.
[2] COUFFIGNAL Louis, La Cybernétique, Paris, PUF, « Que sais-je ? » n°683, 3 ed., 1968, 130p., p.76
[3] *Ibid*., p.23
[4] WIENER, *op. cit.*, p.70.

ments et leur signification, ainsi que leur capacité à transmettre de l'information à une autre entité. C'est donc dans cette optique que les résultats scientifiques et le développement technologique sont obtenus dans le cadre de la cybernétique. Mais quels sont les principes nés de la pensée cybernétique ? Sont-ils toujours d'actualité et comment sont-ils pris en compte aujourd'hui dans les études ou les réalisations technologiques ?

Dans un cadre plus contemporain, le cyberespace, défini selon l'Agence Nationale des Systèmes d'Information (ANSSI) comme un « *espace de communication constitué par l'interconnexion mondiale d'équipements de traitement automatisé de données numériques* »[5], innerve la vie des États, tant dans leur dimension sociale que régalienne. Il devient alors pertinent de s'interroger sur ce développement, et aussi sur toutes les innovations automatisées pouvant se relier à lui pour acquérir de plus grandes capacités. La défense du cyberespace, absolue nécessité pour maintenir les capacités offertes par des outils devenus indispensables, est en France dévolue à l'ANSSI[6]. Elle est déclinée pour le volet militaire au niveau de l'Etat-Major des Armées sous le commandement de l'officier général « cyberdéfense », qui coordonne l'action d'unités des armées ou de la Direction Interarmées des Réseaux d'Infrastructure et des Systèmes d'Information (DIRISI), selon le domaine de compétence[7]. Si les armées défendent les systèmes technologiques qu'ils déploient, en métropole ou en opération à l'étranger, elles s'engagent conjointement avec la société civile avec une réserve citoyenne cyber et un pôle d'excellence cyberdéfense regroupant centres de recherche, entreprises et unités militaires, participant ainsi à la défense des intérêts nationaux sur le cyberespace. Mais au-delà de cette vision opérationnelle concernant sa défense, il est bien question de s'interroger sur la pertinence du système mis en place au sein des armées pour appréhender le cyberespace. Est-ce que le modèle est pertinent et répond aux besoins, actuels et futurs ? Doit-on définir un nouveau domaine de commandement, de gestion humaine et d'opération, lié au cyberespace ? Est-ce que cette vision est opportuniste, reflète une réalité ou se trouve, au contraire, limitative ?

Alors même que la cybernétique est née de travaux demandés par les armées américaines, il n'y a plus de domaine de recherche et développement revendiquant ce nom, dans le monde civil ou militaire, mais une multitude de domaines qui utilisent la pensée cyberné-

[5] Voir sur le glossaire de l'ANSSI : https://www.ssi.gouv.fr/particulier/glossaire/c/ consulté le 10 février 2017
[6] Loi n°2013-1168 du 18 décembre 2013, « *le Premier ministre définit la politique et coordonne l'action gouvernementale en matière de sécurité et de défense des systèmes d'information. Il dispose à cette fin de l'autorité nationale de sécurité des systèmes d'information* ».
[7] COUSTILLERES Arnaud (Vice amiral), *in* RAUFER Xavier, *La Première Cyber-guerre mondiale ?*, Micro Application, Paris, 2015, 300 p., p.42 – 48.

tique : transmission de l'information, réseaux de neurones, intelligence artificielle, drones,… D'une science transdisciplinaire qui attirait tous les regards dans les années 50[8], seuls les travaux initiaux sont restés, et peu poursuivent la réflexion scientifique sur ce sujet. Dans le domaine militaire, si cette remarque reste valable, il serait intéressant de voir l'apport de cette pensée, après deux décennies d'informatisation de toutes les capacités militaires – numérisation – et une résonnance forte au niveau des opérations : nécessité d'une cyberprotection puis naissance de la cyberdéfense.

Avec la montée en puissance au sein des armées françaises des unités, doctrines, centres d'analyses et de recherche, et commandement liés à la cyberdéfense, la réflexion sur le sens de ce déploiement est utile. La raison de vouloir cette multiplication de moyens et de personnes compétentes n'est plus à justifier : elle est réelle et liée à la menace directe sur la nation et ses armées. Mais, il est nécessaire de s'interroger sur la direction et la pérennité, à long terme, de ces décisions, organisations et même procédures et outils.

Afin de d'analyser la défense du cyberespace au prisme de la pensée cybernétique, les recherches se sont orientées vers différents types de documents. Tout d'abord, les écrits historiques, ceux qui permettent d'avoir une description précise de la cybernétique comme définie à son origine. Ainsi, ce sont les écrits de Norbert Wiener, mais aussi de Louis Couffignal en tant que transmetteur de cette science en France, qui serviront à établir les principes de la pensée cybernétique. Dans la même veine, ce sont les ouvrages plus contemporains de Joël de Rosnay, et les mémoires de l'Ecole Supérieure de Guerre datant de l'époque du développement de cette science qui serviront à inscrire ces principes dans un cadre plus pragmatique. Enfin, une étude de la pensée d'Alan Turing est également intéressante puisqu'il s'agit du fondateur du premier ordinateur et des premiers travaux sur l'intelligence artificielle. Pour relier ces travaux au présent et surtout au domaine militaire qui nous préoccupe, deux auteurs majeurs sur l'étude des organisations militaires, de leur efficacité sur le champ de bataille, du commandement et de ses outils serviront de référence : Colin S. Gray et Martin Van Creveld. Dans son approche variée sur les origines et la nature des changements de la guerre, Béatrice Heuser analyse l'évolution de la stratégie dans le temps. Cette vision apporte également un éclairage sur le rapport entre stratégie et technologie. Ensuite, les ouvrages les plus récents concernant le cyberespace et la cyberdéfense ont permis de mettre en perspective historique la pensée cybernétique dans un contexte actuel. La lecture critique d'œuvres visant à instituer le

[8] LE ROUX Ronan, *Présentation de l'édition française*, in WIENER Norbert, *La Cybernétique, information et régulation dans le vivant et la machine*, Paris, Seuil, 2014, 370p., p.11 -22.

cyberespace comme espace de confrontation (Olivier Kempf) ou la cyberdéfense comme nouvel outil stratégique (Stéphane Dossé, Aymeric Bonnemaison, Daniel Ventre) ont nourri de manière pertinente et concrète cette réflexion. Pour résumer la méthode employée, cette étude met en application les principes majeurs de la pensée cybernétique, née à la fin de la Seconde Guerre Mondiale, sur l'essor des technologies de communication de l'information depuis la fin du XX^{ème} siècle. Il s'agit donc bien de créer un pont entre passé et présent, en mettant en avant les idées conçues il y a plusieurs dizaines d'années, afin de caractériser, de comprendre, voire d'orienter le sens du développement technologique actuel.

Cette étude a pour objectif de démontrer la nécessité de la création, au sein de la Défense française, d'un domaine CYBER pour les armées et incluant une recherche civilo-militaire ayant pour milieu d'opération l'espace cybernétique. Cet espace est défini comme une compréhension systémique du cyberespace, incluant également les utilisateurs, les outils, les usages de ces outils, leurs implications, opportunités et risques sur l'organisation, ainsi que la direction donnée à son développement. Pour la partie militaire, les capacités du domaine CYBER peuvent ainsi être intégrées dans une armée nouvellement créée, ayant pour mission la maîtrise de l'espace cybernétique.

Pour cela, nous établissons d'abord comment l'analyse systémique, méthode de travail essentielle dans les recherches menées par la cybernétique, permet d'élargir le spectre du cyberespace à un espace cybernétique. Ensuite, la résistance au changement, ou homéostasie, en tant que phénomène de rétroaction étudié par la cybernétique, met en relief les difficultés et le rôle du décideur dans la transformation du modèle militaire pour prendre en considération cet espace cybernétique. Enfin, c'est le rôle de l'homme, à la fois gouvernail et terreau des conflits, qui est affirmé dans la notion de commande, ou direction, dans les rapports entre guerre et technologie, pour le développement du cyberespace.

1. Pour une vision systémique du cyberespace au niveau militaire

« *Technology does not just represent an assemblage of hardware but a philosophical system.* »[9]

Ainsi Martin Van Creveld décrit-il la technologie et plus particulièrement son utilisation au profit des organisations militaires, destinées à dissuader ou faire la guerre. Cette vision, établie à parti d'études historiques approfondies sur le commandement en opération, les outils permettant ce commandement, et l'évolution des structures militaires pour intégrer ces outils, fait écho à l'un des grands principes issu de la cybernétique : l'analyse systémique. Selon Joël de Rosnay, « *un système est un ensemble d'éléments en interaction dynamique, organisé en fonction d'un but* »[10]. Cette définition est d'ailleurs reprise par les études de doctrine des armées françaises[11]. L'analyse systémique s'emploie donc « *à définir les limites du système à modéliser ; à identifier les éléments importants et les types d'interactions entre ces éléments, puis à déterminer les liaisons qui les intègrent en un tout organisé* »[12].

Comme il l'écrit dans l'introduction de son ouvrage définissant la cybernétique, Norbert Wiener souligne l'importance d'une approche mettant en avant les relations entre éléments avant de connaître le fonctionnement intrinsèque de chaque élément. Quand il décrit ses études sur les liaisons et réactions nerveuses humaines, il comprend que le sujet est bien le système nerveux dans sa globalité et non chaque élément constitutif. Les échanges d'information et mouvements qui en découlent sont d'abord à analyser du point de vue global pour comprendre le sens général des réactions.

Affirmant le besoin de cohérence globale dans le domaine militaire, Martin Van Creveld poursuit sa pensée en concluant que « *war itself became an exercise in managing the future, and the most successful commanders were not those most experienced in the ways of the past, but, on the contrary, those who realized that the past would not be repeated* »[13]. L'historien souligne ici le besoin de création, d'innovation pour s'adapter, non pas aux méthodes passées, mais à celles pouvant à l'avenir se réaliser.

---

[9] « *La technologie ne représente pas juste un assemblage de matériel, mais un système philosophique.* » Traduction du rédacteur, in VAN CREVELD Martin, *Technology and War, From 2000 BC to the present,* n.c, Simon and Schuster, 2010, 352p., p.218

[10] ROSNAY Joël (de), *Le Macroscope, vers une vision globale,* Paris, Seuil, 1975, 376 p., p.101

[11] CICDE, *Réflexion doctrinale interarmées RDIA-008_AS Eléments d'analyse systémique pour la planification opérationnelle,* 2012.

[12] *Ibid*. p.122

[13] « *La guerre elle-même est devenue un exercice ayant pour but la gestion du futur, et les commandeurs ayant le plus de succès n'ont pas été les plus expérimentés dans les méthodes du passé, mais, au contraire, ceux qui ont compris que le passé ne se répéterait pas.* » Traduction du rédacteur, in VAN CREVELD, *op. cit*., p.218.

De la même manière, nous affirmons qu'il est nécessaire de définir, au sein des Armées et du ministère de la Défense, une organisation permettant de répondre de manière pérenne et globale au déploiement du cyberespace, son utilisation actuelle et future, et sa défense.

Définir cette organisation, c'est d'abord comprendre le lien entre la pensée cybernétique et le développement du cyberespace. C'est ensuite affirmer qu'une meilleure utilisation des principes nés de la pensée cybernétique, et de l'analyse systémique en particulier, met en défaut l'organisation militaire actuelle dans la mise en œuvre, l'utilisation et la défense du cyberespace. C'est enfin expliquer comment un domaine dédié à ces opérations serait mieux à même de garantir la pérennité d'outils indispensables aux Armées et au fonctionnement de la société.

1.1. Le lien entre la pensée cybernétique et le développement du cyberespace : des sciences et de la littérature.

Pourquoi lier la pensée cybernétique au développement du cyberespace ? Est-ce que la racine « cyber » constitue une raison suffisante ? Pourquoi vouloir appliquer les principes d'une science au développement d'un milieu ?

La démonstration de cette étude repose sur le lien entre la pensée issue des recherches sur la cybernétique et l'appréhension du cyberespace par les forces armées. Cette clarification permet de définir une relation utilisable tout au long de la démonstration.

La cybernétique est, parmi d'autres développements, à l'origine du cyberespace connu aujourd'hui, tant dans le domaine scientifique et technique, que sur le plan des idées littéraires.

Il est d'abord nécessaire de définir la cybernétique pour affirmer que des principes fondamentaux s'en dégagent. Attachons-nous ensuite à caractériser le cyberespace pour comprendre comment aborder ce nouveau milieu de conflictualité. Puis, avec un bref aperçu de la littérature de science-fiction, voyons de quelles manières l'imagination met un lien naturel entre les questionnements de la cybernétique et les développements imaginés au sujet du cyberespace.

En effet, née formellement en 1947 avec la parution de l'œuvre de Norbert Wiener, la science nommée cybernétique est par nature transdisciplinaire. Si, dès son origine, elle s'est appuyée sur de nombreuses autres spécialités scientifiques, ces domaines ont par la suite profité de cet apport et se sont développés indépendamment. Réalisant des études au profit de l'armée américaine, Wiener situe le début de la cybernétique lors de recherches sur la défense anti-aérienne. C'est l'apparition, dans son esprit de mathématicien de génie[14], de la formalisation du phénomène de rétroaction (*feedback* en anglais). Pour anticiper une trajectoire de canon anti-aérien, il faut définir un mouvement et se servir d'une donnée de retour (le mouvement de l'avion) pour modifier le mouvement initial du canon. Ce principe de base née de la cybernétique sera ensuite réutilisé sans limite dans de nombreux domaines : réaction d'un individu en fonction de facteurs externes ou internes en biologie, réaction d'un composant électrique selon son état de sortie en électronique afin de stabiliser une situation, réaction du déroulement d'un programme selon un capteur d'environnement en informatique, etc. La rétroaction envahit alors tous les domaines scientifiques et d'ingénierie. Mais, si la rétroaction permet une adaptation du modèle initial (de la trajectoire dans le cas du canon anti-aérien), Wiener se concentre également sur ce modèle initial. La définition de ce modèle consiste selon lui à rechercher le mécanisme de « commande », c'est-à-dire la direction ou la volonté de l'automatisme créé. Ainsi naît la cybernétique : il s'agit de savoir pourquoi un comportement va avoir lieu pour pouvoir le modéliser. Et dans cette recherche de la « commande », ce sont les résultats dans des domaines variés, comme la biologie, qui vont aider le chercheur à affiner sa capacité à décrire cette volonté intrinsèque. En réalisant que l'activité du système nerveux ne peut être expliquée indépendamment du fonctionnement des muscles ou d'autres parties du corps, il en conclut la nécessité de l'analyse systémique.

> « *Le système nerveux central n'apparaît plus comme un organe indépendant, recevant les données sensorielles et renvoyant des décharges aux muscles. Au contraire, certaines de ses activités les plus caractéristiques ne peuvent s'expliquer qu'en tant que processus circulaires, émergeant du système nerveux par les organes sensoriels, qu'ils soient proprioceptifs ou organes des sens spéciaux. Cela nous a semblé marquer un nouveau pas dans cette partie de la neurophysiologie qui concerne non seulement les processus élémentaires des nerfs et synapses, mais aussi les performances du système nerveux en tant que totalité intégrée.* »[15]

Encore une fois, la boucle de rétroaction entre capteurs (organes sensoriels) effecteurs (muscles) et système de commande (nerfs et cerveau), s'impose comme principe fondamental

[14] Admis à l'université à 11 ans pour étudier les mathématiques, il poursuit à Harvard et obtient son doctorat en 1912, âgé de 18 ans. Voir la biographie de CONWAY Flo et SIEGELMAN Jim, *Héros pathétique de l'âge de l'information : en quête de Norbert Wiener, père de la cybernétique*, Paris, Hermann, 2012, 422p.
[15] WIENER, *op. cit.*, p 65-66

et appuie celui qui vient d'être décrit : l'analyse systémique, ou comment étudier un phénomène comme une « *totalité intégrée* ». Pour Joël de Rosnay également[16], l'analyse systémique est une approche absolument nécessaire pour comprendre l'évolution d'un système par rapport à son environnement (dynamique) et non pas le fonctionnement de réactions isolées et indépendamment du temps (statique). Et c'est bien la notion de message qui apparaît comme fondamentale dans la définition de cybernétique, en dernier lieu. Les chercheurs travaillant avec Norbert Wiener dans le cadre d'une approche cybernétique ont mis en avant la notion de message dans le phénomène de communication.

> « *Sur le plan de l'ingénierie des communications, il nous était déjà clairement apparu […] que les problèmes de l'ingénierie de la commande et ceux de l'ingénierie des communications étaient inséparables, et centrés autour non pas de la technique du génie électrique, mais de la notion beaucoup plus fondamentale de message, que celui-ci soit transmis par des moyens électriques , mécaniques ou nerveux. Un message est une séquence discrète ou continue d'événements mesurables répartis dans le temps – précisément ce que les statisticiens appellent une série temporelle.* »[17]

Si ce discours apparaît absolument trivial de nos jours, c'est grâce à la théorie de l'information développée par le mathématicien Claude Shannon[18] parallèlement à la cybernétique, et dont l'apport est majeur dans nombre d'autres sciences.

Attachons nous désormais au cyberespace pour comprendre et définir son lien avec la pensée cybernétique. Chaque État, organisation nationale, ou internationale possède une définition du cyberespace. L'ANSSI, qui correspond à l'organisme « tête de chaîne » de la défense du cyberespace – sous la responsabilité du SGDSN – définit le cyberespace comme un « *espace de communication constitué par l'interconnexion mondiale d'équipements de traitement automatisé de données numériques* ». Dans cette acception, qui paraît axée sur le volet physique (« *interconnexion mondiale d'équipements* »), il ne faut pas oublier le volet logique (« *traitement automatisé de données numériques* ») qui donne vie à la finalité : le volet informationnel (« *espace de communication* »). Comme le décrivent de nombreux auteurs (Olivier Kempf[19], Daniel Ventre[20]), en commençant par les doctrines nationales de pays occidentaux (France[21], Etats-Unis[22], Royaume Uni[23]), cet espace peut être appréhendé comme un milieu

[16] ROSNAY Joël (de), *op. cit.*, p.119.
[17] WIENER, *op. cit*., p.66
[18] SHANNON Claude E., *A Mathematical theory of communication*, Bell System Technical Journal, vol.27, n°3, 1948, p.379-423.
[19] KEMPF Olivier, *Introduction à la cyberstratégie*, Economica, Paris, 2012, 176 p.
[20] VENTRE Daniel, *Cyberattaque et Cyberdéfense*, Lavoisier, Paris, 2011, 312 p.
[21] *Doctrine interarmées de cyberdéfense*, 2013.
[22] Joint Publication 3-12 (R), *Cyberspace Operations*, 05/02/2013
[23] *The UK Cyber Security Strategy, Protecting and promoting the UK in a digital world*, 25/11/2011

en partie matériel, comme le milieu terrestre, aérien ou maritime, et en partie immatériel, pour la vaste étendue d'idées et de connaissances qui y est créée. La vision communément partagée est donc une décomposition de cet espace en trois couches : physique, logique et informationnelle. Cette vision, très actuelle, du cyberespace doit être confrontée à son passé et au développement des différentes disciplines ayant engendré cet espace. En effet, il est indéniable que de nombreuses sciences ont participé à la création des différentes couches mentionnées précédemment : l'informatique et l'intelligence artificielle avec Alan Turing, les réseaux avec Von Neumann, la théorie de l'information avec Shannon, la cryptologie pour des aspects de sécurisation, la théorie du langage pour la couche logique en programmation, *etc*. Toutes ces sciences ont hérité du travail de la cybernétique, ou adopté une approche cybernétique, ou constitué un pan de réflexion dans la pensée cybernétique. Enfin, et de manière très pragmatique, les recherches menées par la DARPA[24] afin de fournir à la Défense américaine la possibilité de commander sous la contrainte d'une attaque nucléaire, ont également été à l'origine de la réalisation d'un réseau de machines nommés ARPANET[25], l'ancêtre de l'Internet. La technologie déployée et son mode d'emploi associé, l'Internet Protocol (I.P.), se sont alors diffusés dans tous les domaines : développement de l'Internet, de réseaux d'entreprises, domestiques ou d'objets connectés. Si l'Internet et l'I.P. sont présents au quotidien dans la vie des individus, ils créent néanmoins une dépendance des sociétés occidentales au bon fonctionnement de ce cyberespace, et rendent les États supérieurs technologiquement d'autant plus sensibles à une faille de leurs systèmes. Si ce risque est accepté, c'est parce que la capacité technologique ne constitue pas la finalité. La capacité à échanger des idées, commander, influencer une population ou occuper un espace informationnel constitue le véritable objectif dans les avancés techniques mises en œuvre dans le cyberespace. Ainsi, le cyberespace couvre de nombreuses disciplines scientifiques, pour une finalité qui réside dans le domaine humain, la pensée, loin de toute problématique scientifique. Issues ou entrant dans le spectre de la pensée cybernétique, toutes ces disciplines ont évoluées en rapport avec la cybernétique, qui s'est quasiment éteinte depuis sa création. Le cyberespace devient alors un outil intégrateur de toutes ces sciences ; de même que la cybernétique, dans son acceptation initiale, propose cette approche transdisciplinaire et systémique afin de comprendre la nature du processus de commande. Le lien historique entre la pensée cybernétique et le développement du cyberespace se retrouve donc, tant dans l'origine du cyberespace que dans son fonctionnement.

[24] DARPA : Defense Advanced Research Project Agency. Le nom de cette agence a alterné entre ARPA et DARPA au gré des évolutions de l'opinion publique américaine sur leur Défense.
[25] ARPANET : nom donné au réseau informatique créé par l'ARPA.

Enfin, au-delà de cette vision factuelle du développement technologique dans le domaine des télécommunications, de la transmission d'information, de l'intelligence artificielle, il est intéressant d'observer l'imagination prospective des auteurs de science-fiction. Si le fondateur de la cybernétique appréciait avec difficulté cette littérature[26], ne trouvant rien de cybernétique dans l'anticipation et la création de technologies reliées à aucune réalité scientifique, il accordait néanmoins du crédit aux problématiques de fond soulevées par les rapports entre l'homme et la machine ou son environnement. Ce qui dérange Norbert Wiener dans une partie de cette littérature, c'est la caution faussement scientifique apportée aux lecteurs, qui penseront alors réfléchir de manière raisonnée aux problèmes mettant au défi l'humanité. Lorsqu'une œuvre de science-fiction réalise, en plus de son travail d'imagination, une vraie étude des rapports sur l'évolution des sociétés entre elles, ou avec leurs rapports à la machine, le scientifique accorde un intérêt pour elle. Le lien entre cybernétique et le cyberespace connu actuellement se retrouve aussi dans cette littérature, où ces visions futuristes, même si elles ne sont pas toutes réalisées, comportent une interrogation sur la capacité, les effets ou l'éthique du développement technologique. En commençant par l'auteur de référence et le plus prolifique, Isaac Asimov, nous voyons bien que les lois de la robotique sont d'une actualité prégnante. Énoncées, modifiées et mises au défit dans plusieurs de ses ouvrages et notamment son *Cycle des Robots*[27], ces lois sont, pour l'auteur, intégrées de manière natives et matérielles dans le mécanisme réflexif des robots. Elles imposent aux robots de ne pas porter atteinte à l'être humain, d'obéir à l'être humain, et de protéger, si possible, leur propre existence. Récemment, avec le développement de l'intelligence artificielle, ces lois font débat et sont une base sérieuse de réflexion[28]. Les questionnements sur la direction du temps, les rapports humains, le positionnement de l'homme, de son âme et de ses idées sont tout autant de questions partagées par la cybernétique, mises en avant par le développement du cyberespace et explorées par l'œuvre de Philip K. Dick[29]. L'œuvre *1984* de George Orwell[30] reste le symbole d'une crainte de l'utilisation de la technologie à des fins de contrôle autoritaire de la population. Plus récemment, Robert Charles Wilson met en scène dans sa trilogie *Spin*[31], *Axis*[32] et

[26] CASSOU-NOGUES Pierre, *Les Rêves cybernétiques de Norbert Wiener*, Paris, Seuil, 2014, 284 p., p.126-128.
[27] ASIMOV Isaac, *Le Grand Livre des Robots, Tome 1 : Prélude à Trantor*, Presses de la Cité, Paris, 1990 et *Le Grand Livre des robots : Tome 2 : La Gloire de Trantor*, Presses de la Cité, Paris, 1991.
[28] Voir article d'ORSINI Alexis, *Les « 23 principes d'Asilomar » veulent encadrer le développement de l'intelligence artificielle*, disponible sur le site http://www.numerama.com/tech/22857-les-23-principes-dasilomar-veulent-encadrer-le-developpement-de-lintelligence-artificielle.htm/amp consulté le 02/02/2017
[29] Pour une biographie et un éclairage sur la pensée créatrice de Philip K. Dick, voir CARRERE Emmanuel, *Je suis vivant et vous êtes morts*, Paris, Seuil, 1993, 420p.
[30] ORWELL George, *Nineteen eighty-four*, n.d., Penguin Books, 1949, 254p.
[31] WILSON Robert Charles, *Spin*, TOR, New York, 2005, 460 p.
[32] WILSON Robert Charles, *Axis*, Denoël, Paris, 2009, 490 p.

Vortex[33], la version ultime du transhumanisme, où l'âme de l'homme se transfère dans un réseau d'intelligence pure, à vocation atemporelle et de conservation de l'espèce. La commande, cette volonté de l'homme recréée dans la machine, est inhérente au développement du cyberespace et de son utilisation.

1.2. Apport de la pensée cybernétique dans l'étude des domaines militaires liés à la défense du cyberespace.

Qu'apporte la pensée cybernétique dans notre étude sur l'adaptation des armées françaises au cyberespace ? Quelle utilisation des principes nés de cette science souhaitons-nous vérifier ou mettre à l'épreuve dans la défense actuelle du cyberespace ?

En poursuivant notre comparaison temporelle entre la cybernétique et le développement du cyberespace, nous proposons d'appliquer ces principes issus de la pensée cybernétique sur le système constitué par le cyberespace et son environnement militaire. Considérant le système formé par le cyberespace, par les outils nécessaires à son développement, son exploitation et sa défense, nous allons donc apprécier l'organisation mise en place par le ministère de la Défense et les armées françaises. Loin d'apporter un jugement sur l'efficacité actuelle des opérations menées dans le cyberespace (protection, défense ou attaque), cette appréciation critique portera sur la cohérence du système établi pour exploiter toutes les opportunités et faire face à tous les risques, dans une perspective de permanence et d'amplification de l'utilisation de cet espace. Nous établissons, de la même manière que Martin Van Creveld l'écrit, que : « *the successful of the new weapons often involves a conceptual side-stepping, … a rethinking not merely of tactics but of operations and even of the goals of the conflict. It is not a question of doing the same better, but of doing something altogether different.* »[34] Nous affirmons donc, comme nous allons le démontrer, qu'il faut plus qu'une addition de capacités pour faire différemment.

Les fonctions militaires SIC, RENS et OPS ne permettent pas d'apporter une réponse efficace et globale au déploiement, à l'utilisation actuelle et future, et à la défense du cyberespace.

[33] WILSON Robert Charles, *Vortex*, Denoël, Paris, 2012, 400 p.

[34] « Le succès des nouvelles armes implique souvent un virage conceptuel… une nouvelle étude, pas simplement des tactiques, mais des opérations et aussi des objectifs du conflit. Il ne s'agit pas de faire la même chose en mieux, mais de faire quelque chose tout à fait différemment. » Traduction du rédacteur, in VAN CREVELD, *op. cit.*, p.227

Démontrons cette assertion en utilisant les principes que J. de Rosnay définit dans son ouvrage majeur sur l'approche systémique. Ainsi pour l'auteur, la relation entre les deux disciplines est telle que « *l'approche systémique s'appuie sur la cybernétique et la théorie des systèmes* »[35]. Parmi *« les dix commandements de l'approche systémique* »[36] définis par cet auteur de référence, retenons trois axes assurant une bonne appréhension d'un système. Nous verrons en premier lieu comment la centralisation inhérente à la création d'un commandement Cyber, tourné vers les opérations et le renseignement, verrouille la liberté intellectuelle. Puis, nous expliquerons pourquoi l'organisation en « silo » de domaines ne permet pas de répondre à la nouvelle problématique liée au cyberespace. Enfin, nous conclurons sur la nécessité de décentralisation pour se servir pleinement de l'énergie de commande.

Tout d'abord, retenons comme Joël de Rosnay qu'une trop forte centralisation n'offre pas la variété nécessaire à la stabilité. Pour l'auteur, cette stabilité, garantie de pérennité d'un système, est obtenue par la variété, qu'il s'agit de ne pas restreindre par un commandement trop fortement centralisateur. « *En économie et en gestion, toute centralisation excessive entraîne une simplification des canaux de communication et un appauvrissement des interactions entre individus. Ce qui induit le désordre, le déséquilibre et l'inadaptation à des situations rapidement changeantes.* »[37] Si la centralisation est inhérente à la hiérarchie militaire, où les comptes rendus doivent remonter à l'échelon supérieur et les ordres descendre vers les niveaux subordonnés, rien n'interdit de laisser une part d'autonomie aux échelons subordonnés. Cette capacité est même un atout non négligeable dans une manœuvre ou une opération, par exemple lorsque les communications sont altérées. Or, le commandement exercé sur les opérations, la doctrine et le développement du cyberespace militaire est aujourd'hui centralisé au niveau de l'Etat-Major des Armées (EMA), au sein du commandement cyber. L'annexe 1 présente le modèle de commandement actuel adopté par les armées françaises pour exploiter le cyberespace comme milieu de conflictualité. Si le commandement cyber fournit les capacités de commandement et de prospective sur le domaine, les unités de manœuvres sont mises sous son commandement opérationnel, sans y être affecté organiquement. Quelles soient de l'armée de Terre, de l'armée de l'Air, de la Marine, de la DIRISI, ou appartenant directement à une structure interarmées comme l'EMA (cas du CO Cyber[38]), les unités ayant comme mission une action sur le cyberespace, voient leurs actions directement commandées par

[35] ROSNAY, *op.cit.*, p.100
[36] ROSNAY, *op. cit.*, p.132-139
[37] ROSNAY, *op.cit.*, p.133
[38] CO Cyber : centre d'opération Cyber.

l'échelon centralisateur. Cette nécessité, justifiée par l'unicité de commandement, mais surtout pour conserver la cohérence des actions menées sur le cyberespace, entraîne de manière concomitante la raréfaction des idées et l'appauvrissement de la capacité de prise d'initiative.

Ensuite, la mise en tuyau d'orgue du modèle des armées pour les fonctions opérationnelles concernées au premier plan par l'exploitation du cyberespace ne permet pas de résoudre le nouveau problème apporté par cet espace. Ce format en « silo » convient pourtant bien aux autres fonctions, tant en interarmées qu'au sein de leur armée. En effet, dans tous les états-majors opérationnels français, sont représentées de façon plus ou moins exhaustive les fonctions suivantes : 1-personnel, 2-renseignement[39] ou RENS, 3-opérations ou OPS, 4-logistique, 5-planification, 6-système d'information et de communication ou SIC[40], 7-préparation opérationnelle et retour d'expérience, 8-budget et finances, 9-action civilo-militaire. Cette organisation assure d'abord une efficacité née de la concentration de spécialiste au sein d'une filière : efficacité endogène de la fonction. Il rend enfin toute sa plus-value par le travail matriciel produit au sein des états-majors, permettant de croiser les visions spécialisées au profit d'un objectif opérationnel : efficacité exogène des fonctions. Cependant, pour l'appréhension du cyberespace, plusieurs visions peuvent et méritent d'être apportées : la vision « mise en œuvre » fournie par la fonction SIC, la vision « confrontation technique » et « renseignement d'origine cyber » (ROC) fournie par la fonction RENS et la vision « exploitation » ou « confrontation opérationnelle » permettant l'appui à des opérations dans les milieux physiques pour la fonction OPS. Pour J. de Rosnay, le principe défendu pour une organisation efficace est celui de différencier pour mieux intégrer : « *seule l'union dans la diversité est créatrice. Elle accroît la complexité, conduit à des niveaux plus élevés d'organisation.* »[41] Tout en conservant la spécialité de chacun des apports de fonction et d'armées, il s'agirait donc d'unifier le système pour complexifier la vision du cyberespace. Ce système ne serait donc pas seulement un espace physique où les opérateurs des trois armées mettent en œuvre du matériel de communication, de réseaux informatiques ou satellitaires. Il ne serait pas non plus seulement un espace logique où les bases logicielles sont implémentées et la lutte s'exerce entre le contournement des protections et la recherche des agresseurs. Il ne peut se composer seulement d'un espace informationnel, où les idées qui s'en dégagent sont

[39] RENS : renseignement
[40] SIC : systèmes d'information et de communication. *« Système intégré d'appui au commandement destiné à fournir dans les délais requis aux autorités et à leur état-major les données nécessaires à la planification, à la conduite et au contrôle des activités. Note : le SIC intègre le personnel, les équipements, l'organisation, les procédures, les liaisons et les éléments de doctrine.* » selon le CICDE, *Glossaire interarmées de terminologie opérationnelle.*
[41] ROSNAY, *op.cit.*, p.136

l'enjeu. Ce système ne se réduit pas à une seule vision et n'est pas une simple addition de ces visions. Une intégration des visions permet de faire naître une compréhension plus complexe de ce milieu.

Enfin, et de manière plus conceptuelle, « *savoir utiliser l'énergie de commande* »[42] garantit une démultiplication de puissance et donc d'efficacité. Ce concept est directement issu de la pensée cybernétique et de son rapport avec la théorie de l'information. Pour Norbert Wiener, l'information est même au centre des questions d'organisation : « *Tout comme la quantité d'information est la mesure de son degré d'organisation, l'entropie d'un système est son degré de désorganisation ; l'un étant simplement le négatif de l'autre.* »[43] Dans un deuxième ouvrage ouvrant la réflexion de la cybernétique sur de nombreux champs humains, le scientifique précise son idée sur l'information : « *De même que l'entropie est une mesure de désorganisation, l'information fournie par une série de messages est une mesure d'organisation. En fait, il est possible d'interpréter l'information fournie par un message comme étant essentiellement la valeur négative de son entropie, et le logarithme négatif de sa probabilité. C'est-à-dire, plus le message est probable, moins il fournit d'information. Les clichés ou les lieux communs, par exemple, éclairent moins que les grands poèmes.* »[44] Cette définition de l'information comme « *valeur négative de son entropie* » est traduite par *néguentropie* dans les études sur l'information, succédant à Norbert Wiener[45]. Pour J. de Rosnay, « *l'information aussi, c'est de l'énergie. Mais une forme particulière d'énergie, puisqu'elle permet de libérer et de contrôler la puissance.* »[46] Information et énergie ne sont pourtant pas équivalentes, mais une relation existe et il faut « *obligatoirement dépenser de l'énergie pour acquérir des informations* » et on est obligé « *d'utiliser de l'information pour collecter et domestiquer l'information.* »[47] Utiliser l'énergie de commande correspond à la volonté de décentraliser pour ne pas agir au plus haut niveau, mais faire agir les échelons subordonnés pour décupler l'énergie initiale. Nous revenons, par ce principe, aux premières réflexions sur les effets négatifs d'une trop forte centralisation. La décentralisation n'est pas pour J. de Rosnay une absence de contrôle, ou de commandement. Elle permet d'abord le rétablissement d'équilibre : « *le rétablissement rapide des équilibres exige que les écarts*

[42] ROSNAY, *op.cit*., p.138
[43] WIENER Norbert, *La Cybernétique, information et régulation dans le vivant et la machine*, Paris, Seuil, 2014, 370, p.69
[44] WIENER Norbert, *Cybernétique et société, L'usage humain des êtres humains*, Paris, Seuil, 2014 (texte de 1954), 226p., p.53
[45] ROSNAY, *op.cit*. p.194
[46] ROSNAY, *op. cit.*, p.189
[47] *Id.*

soient détectés aux endroits même où ils se produisent et que l'action correctrice s'effectue de manière décentralisée. »[48] Mais les contraintes sont nécessaires : « *la liberté et l'autonomie ne s'obtiennent qu'à travers le choix et le dosage des contraintes : vouloir à tout prix les éliminer, c'est risquer de passer d'un état contraignant mais accepté et maîtrisé, à un état incontrôlable conduisant rapidement à la destruction du système.* »[49] Au final, ce principe aboutit à l'autonomie et la subsidiarité. L'énergie de commande ne peut être décuplée que si des échelons intermédiaires de commandement existent. Cette existence, dans le cas de la cyberdéfense, fait référence à des échelons de commandement organiques mais aussi déployés en opération. L'autonomie de décision et de proposition aux échelons supérieurs doit également être une réalité.

1.3. Création du domaine militaire CYBER : vers une armée de l'espace cybernétique

Après cette utilisation des principes de la pensée cybernétique au développement d'un espace de conflictualité, que pouvons-nous conclure sur l'organisation militaire liée au cyberespace ? Quelles réponses concrètes sont proposées pour se conformer aux enseignements cybernétiques ? Faut-il améliorer les efforts importants fait en matière de cyberdéfense en France ?

L'objectif de cette réflexion est bien d'apporter un axe, une direction au développement des capacités de défense du cyberespace. Certes, ces capacités sont aujourd'hui, pour la France, en plein essor et un réel effort étatique existe pour soutenir tant le volet militaire, qu'industriel et de recherche. Dès 2014, un pacte Défense Cyber[50], comprenant 50 mesures, est pris dans ce sens. Mais, pour la Défense en particulier, l'appréhension de ce nouvel espace de conflictualité ne répond pas toujours aux principes mêmes de la science qui en est pourtant à l'origine. C'est donc, plus qu'une addition de capacités, une nouvelle approche qui assure une direction de développement prenant en compte la vision systémique du cyberespace.

Associer le cyberespace à son utilisation et son développement permet d'appréhender de façon systémique les problèmes liés à la défense de ce milieu.

[48] *Ibid.* p.135
[49] *Ibid*. p.136
[50] Voir http://www.defense.gouv.fr/actualites/articles/presentation-du-pacte-defense-cyber, consulté le 28/02/2017

En effet, la compréhension du cyberespace comme un espace cybernétique redéfinit le modèle en englobant tous les moyens connectés à l'activité humaine, les usages et la commande. Nous verrons ensuite comment cette vision systémique s'applique à l'organisation des armées. Enfin, la création d'un domaine CYBER et d'une armée intégrant les capacités développées au plus près des opérations sont un préambule à l'efficacité du modèle militaire pour intégrer le cyberespace dans son spectre d'action.

« *To look at the matter from a "cybernetic" point of view, the cardinal result of the invention of the invention, and the accelerated pace of technological innovation, was a vast increase of information needed to "run" any military unit, make any decision, carry out any mission, conduct any operation, campaign, or war.* »[51] Pour Martin Van Creveld, l'utilisation croissante de la technologie crée, au sein des états-majors opérationnels et des unités de manœuvre, un accroissement indéniable de flux d'information. Ce qui a été recherché, obtenir plus d'information, a créé un nouveau besoin : gérer ces flux d'information, et pas seulement dans leur transmission. La protection, la recherche d'information sur les réseaux ennemis, le brouillage des transmissions ennemies sont, par exemple, partie prenante de ce modèle Comprendre l'usage de la technologie ne revient donc plus seulement à déployer des capacités de traitement de l'information ou d'action sur les réseaux ; cela revient surtout à appréhender l'espace créé par la technologie comme un espace cybernétique. Cet espace cybernétique englobe tant le cyberespace que les usages des outils et l'activité humaine qui s'y réfère ou qui en est modifiée. Pouvoir anticiper les conséquences de l'utilisation de technologies est le but de cette vision systémique. Ainsi, dans un ouvrage de l'historien plus particulièrement centré sur le commandement[52] : l'exemple du système de transmissions et d'automatisation mis en place par les États-Unis pendant la guerre du Vietnam a simplement aboutit à un ralentissement considérable de la boucle de décision au niveau opératif. Michel Goya reprendra cet exemple pour illustrer la saturation informationnelle issue de cette accumulation d'outils technologiques. En déployant le premier système de communication entièrement automatisé au Vietnam en 1964[53], l'armée des Etats-Unis voit pourtant une paralysie des états-majors opérationnels, suite à une trop grande remontée d'information[54]. « *Les lignes de communications deviennent si encombrées que chaque service tente de contourner la difficulté en créant*

[51] « *Pour regarder le sujet d'un point de vue "cybernétique", le résultat cardinal de l'invention de l'invention, et le rythme accéléré de l'innovation technologique, fut une augmentation considérable d'information nécessaire pour "faire tourner"* toute unité militaire, prendre toute décision, conduire toute opération, campagne, ou guerre » traduction de l'auteur, in VAN CREVELD, *Ibid.* p.235
[52] VAN CREVELD Martin, *Command in War*, USA, Harvard University Press, 1985, 339p.
[53] VAN CREVELD, *Technology and War, op.cit.*, p.240
[54] VAN CREVELD, *Command in War, op. cit.*, p.249-251

son propre réseau et un PC opérations d'un état-major de division finit ainsi par comprendre pas moins de 35 lignes différentes. Cet engorgement, associé à la complexité des structures, a pour première conséquence de ralentir considérablement la planification. Une opération offensive de 30 000 hommes comme Cedar Falls en 1967 demande quatre mois de préparation. L'armée la plus moderne au monde est ainsi la plus lente à s'organiser, du fait même de son modernisme. »[55]

Alors, si comme Martin Van Creveld le souligne, *« the increase in the demands made on command systems is due to the greatly enhanced complexity, mobility and dispersion of modern armed forces* »[56], il devient de plus en plus nécessaire de penser les moyens de commandement d'une force et d'exploitation du cyberespace. Cette vision d'un espace cybernétique ne peut être conçue que par une organisation centrée sur ce modèle La complexité, la mobilité et la dispersion ne sont pas les seuls facteurs entraînant un accroissement du besoin de moyens d'information pour les armées : « *the enormously swallen number of specialized troops, units, functions, and pieces of equipment that make up a modern technological army […] has made overall coordination and control both more important and more difficult.* »[57] Cet accroissement concerne d'ailleurs tant les moyens de commandement que les moyens d'exploitation du cyberspace. Comme le soulignent Aymeric Bonnemaison et Stéphane Dossé dans leur réflexion sur le combat dans le cyberespace, « *ce type de combat ne permettra pas à lui seul de gagner la guerre. Ce sera une condition nécessaire pour obtenir la victoire.* »[58] Intégrer les capacités de transmissions, de protection et d'exploitation offensive du cyberespace, mais également de l'intégration du cyberespace dans l'activité de planification, de conduite des opérations et de combat correspond à la vision systémique de l'espace cybernétique des armées contemporaines. Cette vision systémique de l'utilisation de la technologie se retrouve dans l'histoire militaire. Lorsque les armées prussiennes se sont lancées contre les armées autrichiennes en 1866 puis françaises en 1870[59], le comte Von Moltke (dit Moltke l'Ancien), chef d'État-Major des armées prussiennes entre 1857 et 1871, a laissé à ses subor-

[55] Article de Michel Goya sur son blog « La voie de l'épée », http://lavoiedelepee.blogspot.com/2012/12/letouffement-informationnel-le-cas-de.html, consulté le 12/01/2017

[56] « *L'accroissement des demandes fait aux systèmes de commandements est dû à la complexité grandement évoluée, la mobilité et la dispersion des forces armées modernes.* » Traduction de l'auteur, *in* VAN CREVELD, *Command in War*, p.2

[57] « Le nombre absolument gigantesque de troupes spécialisées, unités, fonctions, et équipements qui constituent une armée moderne t technologique ont engendré une coordination et une supervision à la fois plus importantes et plus difficiles. » Traduction du rédacteur, *Id.*

[58] BONNEMAISON Aymeric et DOSSE Stéphane, *Attention : Cyber ! Vers le combat cyber-électronique, Economica*, Paris, 2014, 222 p., p.10

[59] CREVELD, *Technology and War, op. cit.*, p.103-147

donnés une autonomie toute calculée. Affrontant des armées possédant des armements d'une grande efficacité (canons autrichiens et fusils français Chassepot), le stratège accorda une indépendance à ses unités, tout en utilisant au maximum les capacités du télégraphe, pour avoir une vision des opérations depuis son état-major. Il ne tomba pas, cependant, dans l'excès technologiste : « *it made use of the best that contemporary technology had to offer but did not allow itself to become the slave of that technology.* »[60] Cette vision du chef sur le commandement de son armée en fonction des outils disponibles et des conséquences sur le type de contrôle à mettre en œuvre est l'illustration parfaite d'une approche systémique de son organisation militaire.

Au final, si cette vision systémique aboutit sur une maîtrise de l'espace cybernétique né du cyberespace et de son usage par l'homme, les armées ont le devoir de s'adapter selon cette approche. Actuellement, les fonctions SIC, RENS et OPS possèdent leurs propres commandements organiques selon les armées et services interarmées. La convergence des actions dans le cyberespace et l'accroissement du besoin de coordination entre ces domaines fait naître le besoin d'engendrer un domaine intégrant ces capacités. Selon le ministre de la Défense, est créée dès 2017 « *une nouvelle composante au sein des armées pour asseoir notre souveraineté et notre indépendance nationales, et rester ainsi maîtres de notre destin* »[61]. Un commandement des opérations cyber ou CYBERCOM est formé, sous le commandement direct du chef d'état-major des armées, avec pour mission la conduite des opérations militaires offensives et défensives dans le cyberespace. Or, ce positionnement ne crée pas de commandement organique, ne décrit pas une intégration de la mise en œuvre des capacités de transmission de l'information, ni de l'usage des outils d'exploitation du cyberespace. Pourtant, le commandement organique permet de garantir la prise en compte de l'intégralité du modèle DORESE[62] tel que défini par la doctrine des armées françaises. Seul le lien hiérarchique direct permet de créer une synergie pour toutes les unités dont le champ d'action se situe dans le cyberespace ou à sa périphérie. Cette synergie se traduit par une communauté de pensée et d'action. Au-delà de ce commandement organique, l'intégration des domaines concernant la mise en œuvre, l'exploitation du cyberespace et l'utilisation des outils engagera la

[60] « *Il a tiré parti du meilleur de ce que la technologie contemporaine avait à offrir, mais ne s'est pas laissé devenir esclave de cette technologie.* » Traduction de l'auteur, in VAN CREVELD, *Command in War*, p.147

[61] Discours de Jean-Yves Le Drian - Lundi 12 Décembre 2016, à l'occasion de la visite de la Direction générale de l'armement – Maîtrise de l'information (DGA-MI), http://www.defense.gouv.fr/ministre/prises-de-parole-du-ministre/prises-de-parole-de-m.-jean-yves-le-drian/cyberdefense-discours-de-jean-yves-le-drian-lundi-12-decembre-2016 , consulté le 12 février 2017

[62] DORESE : doctrine, organisation, ressources humaines, équipements, soutien, entraînement. Voir CICDE, *Doctrine d'emploi des force, DIA-01*, 12/06/2014, p.25

réflexion stratégique et tactique sur ce domaine cyber dans la complexité : complexité des modes d'actions, des opérations et des stratégies. Pour intégrer l'espace cybernétique dans le spectre des actions militaires, il s'agit donc d'aller plus loin que les opérations dans le cyberespace. La création du commandement cyber ne constitue donc pas une vision systémique de l'engagement des armées dans cet espace de confrontation. Ce commandement répond néanmoins au besoin actuel d'opérations dans cet espace en conduisant « *les missions de notre appareil militaire et de défense, que l'on peut classer en trois catégories: les missions de renseignement et investigation, celles de protection/défense, celles de riposte et neutralisation* »[63]. Il constitue une première étape indispensable à la compréhension et la constitution des outils défensifs, offensifs et capacités d'opérations. Mais il mérite d'être étendu à l'usage du cyberespace, sa mise en œuvre et son développement pour ne pas rester dans une problématique restreinte. Ce domaine CYBER, intégrant le domaine SIC et les parties des domaines RENS et OPS traitant de ROC, pourrait *in fine* aboutir à la création d'une composante d'armée indépendante, opérant dans l'espace cybernétique. Cette armée trouve sa justification dans la capacité à garantir la maîtrise de l'usage de l'espace cybernétique, support des opérations par le développement technologique et milieu de confrontation à part entière.

Après avoir travaillé sur une application de principes issus de la cybernétique, et mis en avant un espace cybernétique par une vision systémique du cyberespace, nous concluons sur le caractère opportun de créer une armée chargée de la maîtrise de cet espace cybernétique. Mais créer implique de transformer une organisation existante et il est utile de s'intéresser au processus de changement. En effet, bien souvent, le changement au sein des organisations fait naître une résistance, voire des blocages internes.

[63] Discours de Jean-Yves Le Drian, *op.cit.*

2. Les armées : une organisation homéostatique par essence

« *Tout ouvrage complet sur la cybernétique devrait contenir une discussion approfondie des processus homéostatiques.* »[64]

Pour Norbert Wiener, le fondateur de la cybernétique, l'homéostasie est un principe essentiel à considérer dans toute approche systémique. Avant toute modification d'un modèle, la description de son fonctionnement doit également s'attacher à mettre en évidence les mécanismes de résistance au changement. Issue de la recherche biologique et physiologique, l'homéostasie est d'abord découverte par Claude Bernard[65] puis étudiée en détail par Walter Bradford Cannon[66] et W. Ross Ashby[67]. Cette propriété des cellules vivantes est un phénomène de régulation interne aux variations externes, dans le but de maintenir les conditions optimales de survie. Reprise dans de nombreux domaines et *de facto* en cybernétique, qui agit par analogie, l'homéostasie devient pour l'analyse systémique un phénomène incontournable. L'étude des mécanismes de rétroaction fournit de nombreux exemples où des variations se réalisent pour que le système automatisé reste dans des conditions d'équilibres : pesanteur, intensité électrique, chaleur, ou toute autre mesure physique. Cette rétroaction particulière garantit autant la stabilité d'un système qu'elle n'induit une résistance à tout changement provenant d'un signal ou stimulus extérieur.

Ce paradoxe mérite aussi d'être étudié dans le cadre des organisations militaires. Dans le cas plus particulier de notre réflexion sur la transformation des armées pour intégrer l'espace cybernétique comme nouvel espace de conflictualité, ce paradoxe joue un rôle important. Un changement d'organisation de cette nature ne peut en effet n'être conduit qu'en comprenant le fonctionnement de cette propriété. Si comme l'affirme Victor Hugo dans la conclusion de l'*Histoire d'un crime*[68], « *on résiste à l'invasion des armées, on ne résiste pas à l'invasion des idées* », voyons comment les armées elles-mêmes peuvent se faire envahir par de nouvelles idées.

Vouloir faire évoluer les armées, c'est d'abord comprendre la nécessaire mais indéniable résistance du modèle.

[64] WIENER, *La Cybernétique, information et régulation dans le vivant et la machine, op. cit.*,p.217
[65] BERNARD Claude, *Introduction à l'étude de la médecine expérimentale*, 1865. Dès 1950, l'auteur étudie le milieu intérieur des organes et les phénomènes de régulation par rapport au milieu extérieur.
[66] CANNON Walter Bradford, *The Wisdom of a body*, 1932.
[67] ASHBY William Ross, *Principles of the self-organizing dynamic system* in *Journal of General Psychology*, volume 37, p.125-128, 1947
[68] HUGO Victor, *Histoire d'un crime*, Editions Abeille et Castor, Angoulême, 2009, 505p.

Le conservatisme de l'organisation militaire revient d'abord à une nécessité de résilience mais aussi une justification de la validité du système. Néanmoins, cette garantie de survie passe également par une résistance au changement qui peut se révéler contre-productive voire néfaste pour les opérations. Enfin, pour dépasser ce paradoxe, il faut considérer la dualité flexibilité / stabilité induite par la synergie civilo-militaire, comme un véritable atout pour les armées, dans le domaine du développement technologique.

2.1. « Résiste, prouve que tu existes »[69]

Comment qualifier le conservatisme inhérent à toute organisation militaire ? Pourquoi cette résistance au changement existe-t-elle, comme dans toute organisation ? En quoi est-elle bénéfique et dans quelle mesure s'oppose-t-elle au développement technologique ?

« *On the whole, military organizations tend to be conservative in their approach to technological innovation* »[70]. Martin Van Creveld analyse de manière très radicale l'attitude générale des armées face à la nouveauté technique. Essayons de comprendre pourquoi cette résistance à l'innovation existe au sein des armées. En effet, cette compréhension apporte la capacité de mieux appréhender le moyen de faire évoluer l'organisation afin de répondre à de nouveaux défis. Et deux traits caractérisent ce conservatisme militaire.

L'homéostasie, propriété caractéristique des organisations, se manifeste autant pour assurer la survie que pour montrer la validité du système existant.

Pour démontrer cette double caractéristique, nous commencerons par expliquer comment cette propriété de survie existe dans toute organisation. Nous verrons ensuite que le phénomène d'autojustification n'est pas non plus à écarter. Enfin, nous soulignerons les rapports entre l'innovation technologique et son utilisation dans les armées pour illustrer une évolution non linéaire, due à cette homéostasie.

Lorsque Norbert Wiener introduit l'homéostasie dans le champ de la cybernétique, il la caractérise comme une « *application physiologique importante du principe de rétroaction* »[71]. Pour lui, le principe d'homéostasie « *s'avère encore plus essentiel à la continuation de la vie* »[72], que tout autre forme de rétroaction. En s'attachant à l'étude des systèmes, Joël

[69] BERGER Michel, *Résiste*, 1981, chanson interprétée par France GALL
[70] « *De manière générale, les organisations militaires tendent à être conservatrices dans leur approche de l'innovation technologique.* » Traduction du rédacteur, in CREVELD, *Technology and War, op. cit.*, p.223
[71] WIENER Norbert, *La Cybernétique, information et régulation dans le vivant et la machine, op.cit.*,p.215
[72] *Id.*

de Rosnay explique que toute organisation, étudiée comme un système, comporte cette propriété fondamentale[73]. Comme toute cellule ou organisme vivant, un système d'hommes tel qu'une société ou une compagnie privée est régi par cette volonté de survie. Face aux événements extérieurs qui viennent perturber le bon fonctionnement ou le fonctionnement optimal de l'organisation, des actions de régulation (rétroaction) sont effectuées. Quelles soient prises au plus haut niveau de l'organisation ou par les niveaux inférieurs, des mesures sont prises pour rétablir un ordre connu et une continuation de l'activité habituelle. Dans ce cadre, et en imaginant une organisation dont cette propriété soit fortement développée, Joël de Rosnay conclut que « *les systèmes homéostatiques sont ultra-stables ; toute leur organisation interne, structurelle, fonctionnelle contribue au maintien de cette même organisation.* »[74] Pour les armées, le conservatisme face aux nouvelles idées, et notamment face au changement, fait partie intégrante de la propriété d'homéostasie. Si le travail de doctrine s'adapte évidemment aux réalités du temps présent, la résistance induite par ce conservatisme n'est pas irraisonnée. Elle vise d'abord à garantir la survie d'un système qui fonctionne, face à un changement d'organisation qui pourrait être pris de manière trop hâtive. Pour Daniel Ventre, qui étudie les stratégies liées au cyberespace, « *le techno-scepticisme (ou prudence salutaire) est de mise dans nombre de milieux, le milieu militaire n'échappant pas au phénomène* »[75]. Si cette caractéristique assure une résilience absolument fondamentale pour les armées, l'organisation ne pourra évoluer que s'il est démontrable que l'agression extérieure peut prendre le système à défaut. Ainsi, « *disposer d'une technologie nouvelle c'est avoir un avantage sur l'adversaire, tant que celui-ci n'a pas rattrapé son retard en se dotant des mêmes nouveautés.* »[76]

Mais, même en ayant reconnu l'éventualité d'une avancée potentiellement dangereuse de la part d'un agresseur extérieur à l'organisation, il n'est pas sûr que les instances décisionnelles décident d'un changement radical. Si la solution du changement paraît évidente au premier abord, Joël de Rosnay démontre toutefois que le maintien dans un ordre établi peut être la réponse la plus répandue. En effet, la non-renonciation à un modèle existant et qui a fonctionné, le maintien d'une habitude dans laquelle toute l'organisation travaille de manière plus rapide, ou la volonté orgueilleuse d'imposer ses choix historiques sont bien souvent un frein à toute tentative de changement. Cette tendance à se concentrer sur les acquis et les fonctionnements existants se retrouve aussi dans le domaine militaire comme le prouve l'histoire.

[73] ROSNAY, *op. cit.*, p.128
[74] *Id.*
[75] VENTRE Daniel, *Cyberattaque et Cyberdéfense*, Lavoisier, Paris, 2011, 312 p., p.205
[76] *Ibid*. p.203

Lorsque le maréchal Philippe Pétain est reçu à l'académie française le 31 janvier 1931, Paul Valéry rappelle sa compréhension réaliste de la puissance de la mitrailleuse et de l'artillerie. Il faut pourtant attendre les premiers carnages dus à une doctrine en vigueur préconisant l'offensive à outrance, pour faire évoluer les modes d'actions.

> « *Vous avez découvert ceci : Que le feu tue…*
>
> *Je ne dirai pas qu'on l'ignorât jusqu'à vous. On inclinait seulement à désirer de l'ignorer.[…]*
>
> *Il vous parut, Monsieur, que les règlements tactiques en vigueur ne donnaient point de ce feu qui tue une idée très importante. Les auteurs y voyaient surtout quantité de balles perdues, et de temps perdu à les perdre. On enseignait un peu partout que le feu retarde l'offensive, que l'homme qui tire se terre, que l'idéal serait d'avancer sans tirer ; […] Vaincre, c'est avancer, disait-on. On eût pu dire : Vaincre, c'est convaincre.[…]*
>
> *Le feu tue, disiez-vous… Votre formule à présent paraît bien modérée. […]La mitrailleuse, au premier rang, quoique peu rustique et dévorante, a transformé toutes-les possibilités et décimé les prévisions comme les êtres. […]*
>
> *Ayant fait votre découverte, Monsieur, vous ne pouvez que vous n'en tiriez les conséquences. Vous vous faites une tactique séparée ; bien différente de celle que l'on enseigne, et dont les formules que vous en donnez s'opposent nettement aux préceptes qui commandaient le mouvement sans conditions.*
>
> *Vous résumez votre pensée en des maximes saisissantes : l'offensive, dites-vous, c'est le feu qui avance ; la défensive, c'est le feu qui arrête. Vous dites enfin : le canon conquiert, l'infanterie occupe.* »[77]

De plus, John Keegan relève la sous-estimation des moyens nécessaires pour diriger ces formidables moyens de feu. De par le manque de recherche dans le domaine des transmissions et la quasi absence de sécurité des communications, « *les généraux se trouvent alors à la merci de retards et d'incertitudes, comme aux périodes les plus reculées de la guerre. (…) Avec le recul, et malgré l'optimisation de la puissance de feu qu'elle promet, il apparaît que cette technique balbutiante n'est pas assez développée pour faire la différence* »[78]. Cette résistance n'aboutit pas sur une défaite stratégique, et d'autres évolutions seront nécessaires pour arriver à une victoire face à un agresseur réagissant avec les mêmes tendances à l'innovation et résistances systémiques. Il faut cependant reconnaître que cette volonté de conservation des procédés établis peut être comprise de manière psychologique comme un refus d'accepter son erreur initiale. Résister est alors à la fois une nécessité pour la survie de son système social, mais aussi un mouvement de revendication du bien-fondé de son opinion, indépendamment, ou en dépit des évolutions du monde extérieur.

[77] Réponse de M. Paul Valéry au discours de M. le maréchal Pétain, https://fr.wikisource.org/wiki/R%C3%A9ponse_de_M._Paul_Val%C3%A9ry_au_discours_de_M._le_mar%C3%A9chal_P%C3%A9tain , consulté le 24 janvier 2017

[78] KEEGAN John, *La Première Guerre Mondiale*, Perrin, Paris, 2003, 560p., p.34-35

Pour mettre en relief cette homéostasie au regard de l'histoire, mais surtout dans l'acceptation par les armées des innovations technologiques, intéressons-nous au travail de Béatrice Heuser sur les raisons de cette résistance au cours du temps. En effet, pour l'auteur[79], l'évolution de la stratégie ne s'effectue pas selon une relation continue en fonction de l'évolution technologique : il n'y a pas de linéarité entre les deux évolutions. Cette thèse traduit directement l'effet de l'homéostasie sur les organisations militaires. Un combat d'idée entre tenants de l'ancien modèle et prometteurs de nouvelles idées naît à chaque révolution technologique. En présentant l'état des idées stratégiques avant la Première Guerre mondiale, Béatrice Heuser démontre comment l'étude des stratégies napoléoniennes est alors au centre des attentions françaises : « *Tout comme les hommes de la Renaissance avaient ressenti le besoin de faire appel à la sagesse des anciens et de modeler leurs stratégies sur celles des grands généraux de l'Antiquité, l'imitation du mode de guerre napoléonien devint le fil directeur de la stratégie durant la période 1860-1918* »[80]. Mais, si les avancées technologiques importantes dues à la révolution industrielle sont comprises, elles ne sont pas introduites sans réticences : « *leur importance ne fut pas remise en cause. Cependant leurs conséquences faisaient débat. […] La technologie devint au milieu du XIX*^{ème} *siècle un sujet ardemment débattu et le resta* »[81]. L'adoption du changement n'est donc pas immédiatement consécutive de l'invention technique. Ce phénomène est toujours d'actualité et doit être pris en compte dans toute tentative de faire évoluer un système. Dans le cas plus particulier du développement de l'espace cybernétique et de l'adaptation des armées à ce paradigme, notons avec intérêt la conclusion de Norbert Wiener sur la résilience d'une organisation. « *Parmi tous les facteurs anti-homéostatiques que comporte la société, le contrôle des moyens de communication est le plus efficace et le plus important. L'une des leçons de ce livre est que tout organisme maintient sa cohésion par la possession de moyens d'acquisition, d'usage, de rétention et de transmission de l'information.* »[82] Nous comprenons par cette affirmation que les armées déployées en opération, tout autant que les états-majors situés sur le sol national obéissent à cette règle, qui est tout autant un principe de résilience qu'une source de faiblesse. La maîtrise de l'espace cybernétique devient un véritable enjeu, que ce soit pour commander les unités subordonnées, maintenir la cohésion de l'ensemble, ou agresser son ennemi. Il s'agit donc, au final, de prendre en compte l'homéostasie inhérente aux armées pour réaliser que le change-

[79] HEUSER Béatrice, *Penser la Stratégie, de l'Antiquité à nos jours*, Picard, Paris, 2013, 434 p., p. 134-151
[80] *Ibid*. p.134
[81] *Ibid.* p.135
[82] WIENER Norbert, *La Cybernétique, Information et régulation dans le vivant et la machine*, op.cit., p.287

ment à mettre en œuvre pour appréhender l'espace cybernétique touche au fondement même de l'institution militaire : résister et combattre une agression violente.

2.2. Quand la résistance ne gagne pas

Cette propriété favorisant le conservatisme est-elle idéale en toutes circonstances ? Vers où peut mener cette résistance au changement ? Comment valoriser une vision nouvelle dans l'appréhension de l'espace cybernétique ?

Alors que l'homéostasie assure une régulation qui a pour but le maintien en vie du système, nous avons vu comment cette fonction de survie se concentre bien souvent sur la survie d'un mode de fonctionnement connu. Si d'autres modes de fonctionnement existent et garantissent les conditions de survie du système, ils seront défavorisés par processus homéostatique par rapport au mode nominal. Cette résistance à la nouveauté peut donc être un handicap, lorsque seule la nouveauté permet de rester concurrentiel, en opposition avec le but initial de ce comportement conservateur. Après avoir justifié le caractère homéostatique des armées et le bénéfice de cette propriété, attachons nous désormais au revers de la médaille.

Cette résistance au changement peut, malgré tout, mener à la perte de tout le système.

En effet, il est indéniable qu'une réflexion sur le changement est nécessaire pour adapter un modèle aux évolutions technologiques. Nous verrons ensuite comment un trop fort attachement à un modèle existant peut mener à la défaite. Enfin, pour faire évoluer les armées confrontées à un nouvel espace de conflictualité, nous étudierons les pistes d'un changement structurel.

Ainsi, il est nécessaire de réfléchir au changement technologique, et notamment aux innovations liées aux technologies de télécommunication, de l'informatique et leurs usages, pour une maîtrise de l'espace cybernétique par les armées en opération. Cette affirmation reprend les conclusions obtenues précédemment et apparaît peut-être d'une rare simplicité. Réfléchir à la nouveauté technologique n'est pas un fait nouveau, comme nous l'avons vu précédemment avec Béatrice Heuser. A l'heure où les outils de communications, l'informatique en réseau, les moyens de se connecter et de partager des idées sur des applications en ligne se généralisent, il peut paraître banal d'appeler à une réflexion générale sur ces innovations. Et pourtant, tant la portée sociale de l'invention, que ces conséquences sur l'organisation de la société ou des armées ne peuvent être perçues *a priori*. Il devient donc utile, d'abord dans une

vision systémique, puis en comprenant la résistance inhérente au système, de réfléchir aux conséquences des choix sur la pérennité de son organisation. Comme l'analyse Van Creveld au sujet de la transformation due à la technologie, « *had it been rapid, both the process itself and its social consequences would surely have received greater attention* »[83]. En poursuivant son étude sur le commandement et les opérations militaires, l'historien identifie la dispersion des unités comme le facteur principal engendrant la difficulté de commandement. Cette vision d'ensemble du combat, et notamment dans les tranchées de la Première Guerre mondiale, met au final en relation les capacités de transmissions et de commandement avec les capacités offensives et offensives des unités combattantes.

> *Of these* [factors], *the most important was probably extreme dispersion, which caused each soldier and each unit to spread out more than before. Dispersion in its turn led to problems in command and control, particularly on the move and in offensive warfare, when wire-band communication systems could only be used with difficulty, and sometimes not at all. Though, few historians have discussed these problems at any length, they did as much to shape trench warfare in World War I as did barbed wire and machine gun.*[84]

De plus, au-delà d'une inadéquation entre volonté et capacité, comme pour les stratégies offensives de la Première Guerre mondiale ou la maîtrise du spectre informationnel aujourd'hui, le véritable danger se situe dans les conséquences de cette inadéquation. La perpétuation d'un système qui ne prend pas en compte les évolutions extérieures peut mener à la perte du système. Insister dans un mode de fonctionnement dépassé par les possibilités d'agressions adverses, en ne faisant qu'amplifier les variables d'un mécanisme déjà éprouvé, peut mener à la chute de toute l'organisation. Loin de constituer à lui seul la chute des armées allemandes lors de la Première Guerre mondiale, nous pouvons illustrer le maintien d'un système établi, dans le domaine des moyens de commandement allemands. Si la maîtrise de l'information avait été un point fort des campagnes précédentes pour les armées prussiennes, la même organisation, les mêmes procédés, les mêmes outils perdurèrent entre 1871 et 1914. Puisque l'ensemble s'était révélé efficace pour vaincre la France une première fois, l'armée allemande conservera donc en 1914 un système de commandement qui contenait de profondes lacunes. Ces lacunes n'étaient donc pas intrinsèques, puisqu'inexistantes en 1870, mais dues à

[83] « S'ils avaient été rapides, le processus lui-même comme ses conséquences sociales auraient sûrement reçu une plus grande attention. » Traduction du rédacteur, *in* VAN CREVELD, *Technology and War*, *op. cit.*, p.218

[84] « *De tous ces facteurs, le plus important était probablement l'extrême dispersion, qui entrainait un étalement sans précédent des soldats et des unités. La dispersion, à son tour, conduisit à des problèmes de commandement et de contrôle, particulièrement dans les phases de mouvement et d'offensive, quand les systèmes de communication filaire ne pouvaient être utilisés qu'avec difficulté, et parfois pas du tout. Cependant, même si peu d'historiens ont discuté sur ces problèmes d'une manière ou d'une autre, ils ont autant participé à façonner les tranchées de la Première Guerre Mondiale que le fil de fer barbelé ou la mitrailleuse.* »Traduction du rédacteur, *in ibid.*, p.265

deux facteurs : une inadaptation avec la manœuvre envisagée mais surtout une confiance trop grande accordée à la technologie. Ainsi, selon le comte Alfred Von Schlieffen, général prussien, chef d'État-Major des armées allemandes de 1891 à 1906: « *The warlord will be located farther in the near, in a house with spacious offices, where wire and wireless telephone, and signaling equipment are available. […] There, seated on a comfortable chair, in a front of a large desk, the modern Alexander will have the entire battlefield under his eyes on a map. From there he telephones inspiring words, receives the reports of army and corps commanders, captive balloons, and dirigibles, which all along the front watch the enemy's movements and register his positions* »[85]. Succédant à Von Schlieffen, malgré ses réticences à cette vision, Helmuth Von Moltke (dit Moltke le Jeune et neveu de Moltke l'Ancien) lance l'invasion allemande en direction de la France, en 1914, selon cette vision technologiste[86]. Son Quartier Général se situe donc bien en arrière du front, au Luxembourg, quand ses troupes combattent sur le sol français. La doctrine préconise une liaison de l'avant vers l'arrière, laissant un travail considérable aux hommes déjà sous le feu, ralentissant d'autant plus la mise en œuvre de lignes télégraphiques, quand les transmissions ne sont pas brouillées. Moltke se retrouve coupé du commandement de ses armées, incapable d'envoyer des ordres et même d'avoir connaissance de la situation. Conserver les méthodes du passé, pousser au maximum le modèle existant sans réaliser les conséquences de son inadaptation, conduisent ici à une erreur fatale. Sans pouvoir commander, Moltke envoie donc un officier d'état-major, le lieutenant-colonel Hentsch, pour s'informer de la situation tactique. Arrivé sur le front, ce dernier décide, sans en référer au Grand Quartier Général, du sort de l'offensive allemande, aux dépends d'une planification minutieuse faite en amont. Le manque d'information, dû à la conservation d'un modèle existant, entraîne une mauvaise prise de décision par un échelon qui ne peut être commandé. Alors que les transmissions jouent un rôle prépondérant dans les campagnes victorieuses allemandes entre 1866 et 1870, une confiance aveugle dans l'ancien modèle et une surévaluation des capacités technologiques réduisent à néant cet avantage lors de la Première Guerre mondiale.

[85] « *Le chef de guerre sera situé bien à l'écart du front, dans une maison avec de vastes bureaux, où les téléphones à fil et sans fil, ainsi que le matériel de transmission seront disponibles. […] Là, assis sur un fauteuil confortable, devant un large bureau, cet Alexandre moderne aura la totalité du champ de bataille devant ses yeux, sur une carte. Depuis ici, il téléphone pour envoyer ces pensées inspirantes, reçoit des comptes rendus des commandants d'armée et de corps d'armée, des ballons captifs, des dirigeables, qui, tout au long de la ligne de front, surveillent les mouvements de l'ennemi et enregistrent ses positions.* » Traduction du rédacteur, cité par VAN CREVELD, *Command in War, op. cit.* p.153

[86] *Ibid.* p.153-154

Donc, notre étude se doit d'explorer les pistes de changement établies pour la transformation des armées, dans le but de maîtriser l'espace cybernétique avec lequel et dans lequel le combat est mené. Après avoir exposé les principes d'intégration et de décentralisation à des fins d'autonomie, tout en assurant un contrôle, voyons quel type d'organisation est possible. Notons tout d'abord, comme nous l'avons expliqué précédemment, que le cadre ne serait plus limité aux opérations dans le cyberespace comme actuellement, mais serait élargi à la maîtrise de l'espace cybernétique, comprenant les outils de mise en œuvre, les usages de ces outils, les opérations dans le cyberespace et le développement de ce cyberespace. Si la direction donnée au développement du cyberespace est traitée plus loin, tentons de qualifier un modèle novateur dans la maîtrise de cet espace cybernétique. En avril 2016, le ministère fédéral de la Défense allemand décide de créer une cinquième armée, de rang équivalent à l'armée de Terre, de l'Air, à la Marine ou l'armée des Services. En mettant sur un pied d'égalité cette armée Cyber et les autres armées, l'idée est bien de placer le cyberespace sur un même niveau d'importance que les autres milieux de conflictualités. L'annexe 2 détaille l'organigramme ainsi que l'explication des choix relatifs à cette décision. L'organisation souhaitée consiste en une intégration dans une même structure des unités traitant de la mise en œuvre du cyberespace (les unités de transmissions), des unités permettant les opérations sur le cyberespace (les unités de renseignement et de guerre électronique et informatiques), ainsi que des échelons de décisions. Deux étapes marquent cette réorganisation : d'abord la création d'une division « Cyber et SIC » au sein du ministère en octobre 2016, puis la mise en place en avril 2017 d'une armée « Cyber et 5ème dimension » aux côtés des autres armées. En affectant les unités existantes dans les autres armées et services à cette nouvelle armée, le ministère fédéral de la Défense allemand souhaite créer un véritable pôle de réflexion, de travail et d'opérations sur la maîtrise du cyberespace. Si cette vision paraît avant-gardiste, certaines questions restent en suspens concernant notamment la répartition des missions relevant des opérations dans le cyberespace. Le fonctionnement et surtout la réalité des effets produits par cette structure aux côtés des autres armées restent donc à prouver. Mais, si personne ne peut s'engager sur l'avenir, il est néanmoins certain que la synergie créée par cette intégration des différentes visions du cyberespace engendre, *de facto*, une plus grande complexité dans les réflexions et développements liés aux opérations dans ce milieu.

2.3. La force d'un modèle réside dans la dualité flexibilité et stabilité.

Les armées peuvent-elles et doivent-elles encore jouer un rôle dans le développement technologique ? La dualité civilo-militaire apporte-elle un bénéfice à l'innovation ? Comment

et pourquoi vouloir des relations renforcées entre monde civil et militaire sur le sujet des outils liés au cyberespace ?

Imaginer une organisation au sein des armées capable de répondre aux enjeux du cyberespace, c'est, comme nous l'avons vu, s'intéresser aussi bien aux opérations actuelles qu'aux futurs outils, usages et implications. Or, de nos jours, et pour de nombreux pays, la recherche et le développement de l'espace cybernétique n'est plus une responsabilité ou une prérogative étatique, ni même militaire. Loin de nier le fait que l'initiative privée puisse être un formidable moteur de l'innovation technologique, il importe toutefois pour les armées, et donc pour l'État, au minimum de connaître ses propres limites, au mieux de maîtriser les concepts naissants. Pour cela, une relation étroite entre le monde civil de la recherche technologique et la Défense existe de manière historique. Notre étude montre que la redynamisation de cette relation au sujet du cyberespace est une solution pour capter les qualités requises à l'innovation.

L'association de la flexibilité du monde civil et de la stabilité apportée par le monde militaire favorise le développement technologique.

Nous commencerons par établir que le monde militaire fut un temps initiateur de la recherche et du développement technologique, notamment pour l'invention du cyberespace. L'étude d'un modèle intégrateur de tous les aspects de la maîtrise de l'espace cybernétique éclaire sur la plus-value d'inclure la définition des besoins futurs. Nous nous engagerons enfin sur une proposition pour renforcer aujourd'hui cette relation civilo-militaire.

Les rapports entre monde civil et militaire sont anciens et traditionnels sur le sujet de l'innovation technologique. De par le caractère régalien des actions militaires et de la défense d'une Nation, les armées ont toujours cherché et eu la capacité, donnée par les décideurs politiques, d'utiliser les nouveautés technologiques à des fins guerrières. Il en va ainsi de la volonté et de la mission des décideurs d'assurer la résilience et la survie de la Nation. Outre les débats liés aux usages militaires des inventions, et l'homéostasie inhérente à l'organisation des armées, la Défense est donc un moteur de l'innovation de par la nécessité à continuer de progresser pour ne pas se faire dépasser par un adversaire ou ennemi. Pour mettre en œuvre certaines stratégies militaires, au service d'une politique de maîtrise de son environnement géopolitique, la Défense est même à l'origine de véritables ruptures technologiques. De véritables bonds technologiques ont en effet lieu à l'occasion des recherches pour obtenir une capacité de feu nucléaire crédible et résilient. C'est dans cette optique que les États-Unis

d'Amérique, au travers de leur Défense, participent grandement à la naissance du cyberespace. Engagée dans un affrontement de démonstration de puissance contre le bloc soviétique (la guerre froide), la Défense américaine souhaite avoir la capacité de commander depuis tous points de décision, situés sur tout le pays, en imaginant la destruction de l'un d'entre eux. Dans cet affrontement où l'arme nucléaire est brandie comme première et dernière réponse, la capacité de commander mais aussi de diriger les frappes est alors une priorité. Deux avancées majeures dans le domaine des communications, issues des recherches de la DARPA, ont donc comme origine cette stratégie nucléaire : Internet et le Global Positioning System (GPS). ARPANET, l'ancêtre technique de l'Internet[87] comme le montre le schéma original en annexe 3, répond techniquement aux besoins des armées de communiquer à distance des données entre terminaux informatiques. De même, afin de pouvoir situer avec précision les lanceurs de la composante sous-marine de la force de dissuasion nucléaire, et de cibler avec la même précision les objectifs stratégiques, la DARPA participe aux recherches sur le positionnement géographiques à l'aide de satellites. Ces révolutions, aujourd'hui amplifiées et généralisées par les utilisations civiles promues par le secteur économique, sont à l'origine issues de recherche de réponse à des besoins militaires.

Comme nous l'avons démontré, et comme l'écrit Martin Van Creveld[88], c'est la nature de la guerre, son caractère imprévisible, qui impose aux organisations militaires de s'appuyer sur des structures rigides : subordinations, discipline, hiérarchie. L'innovation, quant à elle, sera favorisée par une flexibilité des esprits et des organisations. Ainsi, dans le cas des technologies duales entre monde civil et militaire, tout en bénéficiant d'un terreau fertile au sein de centre de recherches publics ou d'entreprises privées, l'invention peut s'appuyer sur la structure rigide militaire. Les avantages induits sont importants : capacité d'essai, projet sur le long terme, puissance financière étatique, *etc*. La dualité civilo-militaire du développement technologique constitue avant tout une dualité de propriétés : flexibilité du monde civil qui peut s'appuyer sur la stabilité du monde militaire, avant d'être une dualité d'utilisation et de débouchés économiques : déploiements dans les armées et réinvestissement pour des usages civils. Dans cette complémentarité réside à la fois le besoin des armées pour acquérir une supériorité sur son adversaire au moyen de la technologie, et les conditions nécessaires à une recherche coûteuse. En reprenant notre étude sur l'organisation des armées françaises, nous

[87] WALDROP Mitch, *DARPA and the Internet revolution*, publié sur le site de la DARPA et disponible sur le lien http://www.darpa.mil/attachments/%282O15%29%20Global%20Nav%20-%20About%20Us%20-%20History%20-%20Resources%20-%2050th%20-%20Internet%20%28Approved%29.pdf consulté le 14/01/2017

[88] VAN CREVELD, *Technology and War, op. cit.*, p.220

avons vus comment l'intégration de toutes les unités SIC, et des unités RENS et OPS axées sur le cyberespace engagent une véritable synergie pour la maîtrise du cyberespace connu. Au-delà de l'évaluation des risques, menaces futures et de la veille sur les technologies prometteuses, une véritable maîtrise du cyberespace implique d'inclure la définition d'une vision sur le futur de l'espace cybernétique. Il ne s'agit pas seulement de penser les outils de demain, mais également les usages et implications intrinsèques sur le commandement, les opérations à mener sur l'ennemi et les vulnérabilités induites. Dans son rapport final de 2014 sur la *Vulnérabilité et résilience du C2 moderne*[89], la Fondation sur la Recherche Stratégique établit une cartographie assez exhaustive des moyens de commandement, d'actions sur les réseaux, mais aussi les conséquences sur les processus ou les effets liés à la densification et complexification de l'environnement informationnel. Les bénéfices des outils de communication et informatiques sont réels pour les opérateurs qui voient une rapidité de leur action. Pour les niveaux supérieurs, où l'information s'accumule et devient omniprésente, la rapidité ou l'opportunité de la prise de décision est moins évidente. Que ce soit par entrisme, effet tunnel ou suppression des relations formelles, le commandement est contraint par une technologie qui n'apporterait pas avec son déploiement un mode d'emploi, des limites, une capacité de travail en mode dégradé, et une capacité de simulation pour appréhender cet environnement. En plus de la complémentarité entre flexibilité et stabilité issue de la dualité civilo-militaire, la capacité à redevenir moteur de technologies de rupture au sein du cyberespace repositionnerait la Défense dans un rôle de précurseur sur la vision à long terme des technologies, et non en réaction face aux menaces.

Au final, cette réflexion sur le modèle de la Défense française pour appréhender le cyberespace dépasse les seules capacités militaires. Elle déborde sur les relations avec le monde civil de la recherche afin de disposer d'une faculté de reprendre l'ascendant intellectuel sur l'innovation et ne pas subir les seuls outils issus des seules entreprises privées. De plus, croire à la neutralité des plus grands groupes privés, ou être contraint de se fournir en outils auprès de ces groupes est, dans les deux cas, une renonciation à la maîtrise de son environnement informationnel. L'exemple[90] de la DGSI[91] révélant être forcé d'utiliser un logiciel de surveillance de l'Internet provenant de la société américaine Palantir ne peut que nous convaincre de

[89] GROS P., JOUBERT V. et COSTE F., *Vulnérabilité et résilience du C2 moderne*, rapport n°305/FRS/C2 du 2 juillet 2014

[90] Voir l'article *Les renseignements français cèdent à l'américain Palantir la surveillance du Web*, disponible sur le lien http://lexpansion.lexpress.fr/high-tech/les-renseignements-francais-cedent-a-l-americain-palantir-la-surveillance-du-web_1858835.amp.html consulté le 12/12/2016

[91] DGSI : Direction Générale de la Sécurité Intérieure.

cet échec. Il illustre d'autant plus ce problème, que la société américaine, liée aux intérêts du président américain élu en 2017 et *de facto* par la loi sur le renseignement américain, offre un accès aux informations de la lutte anti-terroriste française aux services américains. À défaut de prédire une maîtrise complète de son environnement informationnel à court terme, la Défense n'a pas intérêt à s'engager dans une perte totale de son autonomie d'appréciation de situation en se reposant sur des outils non souverains. Nous avons vus comment les États-Unis d'Amérique, aves les moyens financiers dont ils disposent, ont dédié à la DARPA, une agence dépendant de la Défense, la réflexion et le lancement des programmes innovants, sources de ruptures technologiques. En France, la Direction Générale pour l'Armement (DGA) a pour mission, au sein du ministère de la Défense, d'équiper les forces armées, préparer l'avenir et promouvoir les exportations d'armement. En relation avec la DGA, deux organismes civilo-militaires sont engagés dans la recherche et le développement de technologie. Il s'agit de l'ONERA pour les technologies liées à l'aéronautique at au spatial, et de l'Institut Saint-Louis, centre de recherche franco-allemand sur les matériaux, projectiles, électromagnétisme. Pour le cyberespace, aucun institut ou centre de recherche de même envergure n'a été créé. Avec le pacte Cyber mis en place en 2014 par le ministre de la Défense, le pôle d'excellence cyber rapproche géographiquement en région Bretagne le pôle Maîtrise de l'Information de la DGA (DGA-MI), l'Ecole des Transmissions de l'armée de Terre et deux unités de l'armée de Terre opérant dans ce milieu. La synergie entre opérateurs, concepteurs, développeurs et testeurs est évidemment une plus-value pour la validation d'outils et la réactivité engendrée. Néanmoins, après avoir étudié les bénéfices et la raison du rapprochement civilo-militaire dans le domaine scientifique, la création d'un organisme dédié à la recherche sur l'espace cybernétique est opportune pour la Défense. Centre de recherche civil dirigé par les intérêts militaires, ou structure minimaliste pour l'incubation et le soutien de sociétés privées nationales travaillant sur domaine prometteur (comme la DARPA), les modèles sont multiples pour mettre en place une synergie civilo-militaire au niveau le plus haut. Si la DGA-MI coordonne certaines activités de recherche proposées par les industriels, cette branche de la DGA ne fait que répondre aux besoins opérationnels définis par les états-majors centraux des armées. Parfois, une rupture peut naître d'un besoin non identifié par l'utilisateur, dont l'attention est centrée sur le présent des opérations. La flexibilité instituée par un centre de recherche, ou une structure dédiée au ciblage des sociétés novatrices et au soutien de leurs recherches sera garante d'une plus grande diversité dans les résultats, ainsi qu'une capacité à évaluer en interne les conséquences sur le fonctionnement des armées en opération.

À l’issue de cette étude de l’homéostasie, propriété caractérisant les organisations, nous pouvons établir que ce phénomène est particulièrement prégnant au sein des armées, et que son appréciation est nécessaire avant de mener toute conduite du changement. Cette résistance aux faits nouveaux, aux pratiques ou aux idées nouvelles, qui trouve sa légitimité au sein d’une institution attachée à sa résilience, mérite d’être équilibrée par une approche civile plus souple dans ses facultés à tester et réfléchir différemment. Si une répartition entre ces deux caractéristiques : stabilité et flexibilité est obtenue par une coopération civilo-militaire, c’est bien pour répondre aux questions de nature militaire. Et dans ce cadre, étudier l’objectif ou plutôt la manière de l’obtenir, la direction empruntée, devient un élément primordial.

3. Définir la direction, ou inscrire au premier plan la volonté humaine

« *Si l'on programme une machine pour gagner la guerre, il faut être bien certain de ce que l'on entend par gagner.* »[92]

Lorsque Norbert Wiener poursuit ces travaux à l'issue de la Seconde Guerre mondiale, un inévitable doute subsiste en lui quant au rôle des scientifiques au profit de la création d'armes. Cette conscience d'une interaction entre les hommes de science et la réalité humaine introduit la notion de responsabilité. À travers cette citation, son auteur lie de manière définitive technologie et volonté humaine. Génie scientifique, il est marqué par les horreurs de la guerre, horreurs de l'industrialisation de l'extermination humaine dans les camps de concentration, ou par la puissance de l'atome et les horreurs du combat, enfin, avec son lot de morts, mutilés, traumatisés physiques et mentaux qu'il a tenté d'aider par ses recherches sur les prothèses. Il sait par expérience personnelle et par une réflexion définitivement orientée vers le sens de ses inventions, que cela est bien la seule question à se poser : que veut-on obtenir ? Et pour quelles raisons ? Ceci avant même de définir les technologies qu'il semble utile de développer.

Pragmatique, Norbert Wiener sait bien que l'éthique ne sera pas la ligne directrice de tous les chercheurs. Il sera de tous temps facile d'en trouver pour poursuivre des recherches sans regarder la finalité. C'est bien cet écueil que nos sociétés doivent éviter, et nos armées, défendant les « intérêts supérieurs de la Nation », ont le devoir de participer à cette réflexion : dans quelle direction et pour quelle finalité engager l'effort national ? De même, réorganiser les armées dans l'objectif d'acquérir une maîtrise de l'espace cybernétique ne peut échapper au besoin de définir d'une direction générale, déclinant les décisions politiques dans ce domaine.

Afin de donner une direction au développement technologique, le domaine CYBER créé doit inclure une structure de recherche permettant d'inscrire au premier plan la volonté humaine.

Penser la direction du développement technologique à des fins militaires, c'est d'abord affirmer la primauté de l'homme dans le combat. Ensuite, pour ne pas perdre cette particularité humaine, un juste équilibre entre spécialisation et centralisation doit être réalisé lors de l'intégration des spécialités militaires au sein du domaine CYBER. Finalement, la primauté de

[92] WIENER, *La Cybernétique, information et régulation dans le vivant et la machine, op.cit.*, p.309

l'homme dans la bataille ne peut être intégré dans le développement technologique qu'en l'inscrivant comme principe fondamental de la fonction de commande de l'espace cybernétique : c'est l'humanisation du développement technologique.

3.1. Oui, l'homme fait le réel

Comment évaluer l'effet de la science sur la guerre ? La supériorité technologique est-elle suffisante pour assurer la victoire ? Existe-t-il un horizon où la machine prendra le pas sur l'homme dans la guerre ?

Depuis l'invention des armes de guerre, des techniques de combat nécessitant des outils pour les mettre en œuvre, ou des innovations permettant des ruptures tactiques ou stratégiques, l'homme cherche dans la science la capacité de vaincre son adversaire. Cette recherche, comme nous l'avons vu, est soumise aux débats moraux de chaque époque, avant d'être mise en œuvre par les armées, ou interdite dans un le cadre d'accords politiques. L'homme continue cette poursuite de l'amélioration de ces outils guerriers parce que la réalité impose cette course à l'armement. Les facteurs sont multiples mais convergent vers cette ligne de perfectionnement irrémédiable : des agresseurs ou de possibles menaces qui se dotent des mêmes outils technologiques, une volonté d'avoir des armées crédibles au sein de relations internationales basées sur la puissance, la capacité technologique créant parfois le besoin. Si cette recherche des outils technologiques est intemporelle, supprime-t-elle pour autant le rôle de l'homme dans le combat ? L'issue d'une guerre se définit-elle exclusivement par le rapport entre niveaux technologiques ? Nous pouvons voir comment cette course à l'évolution ne change pas le sens de la guerre.

L'homme est au centre de tout conflit. La technologie ne change pas cet axiome.

L'analyse historique du courant de pensée technologiste du XX^{ème} siècle nous prouve que cette appréciation scientifique de la guerre n'est pas nouvelle ou issue seulement des technologies de communication et des progrès l'informatique. De plus, l'exemple américain de transformation des armées sous le prisme technologiste démontre un égarement vers une confiance absolue dans l'informatisation. Finalement, si la technologie accompagne l'homme dans le combat, ce sont bien les capacités de compréhension et les facteurs humains qui influent majoritairement sur la victoire.

La vision technologiste de la guerre est souvent associée à la suprématie militaire américaine contemporaine. Pourtant, Colin S. Gray démontre de manière très détaillée que cette

course scientifique dans un but de transformation militaire est issue de la rivalité entre États-Unis d'Amérique et Russie[93]. Et cette pensée technologiste, c'est-à-dire pouvoir automatiser les actions de guerre, correspond initialement aux idées soviétiques des années 30. Sans informatique, au moment où le char de combat remplace la force des chevaux sur le champ de bataille, et où vitesse et puissance redeviennent fondamentales, la mécanisation est une théorie développée par le bloc soviétique. Selon ces promoteurs, cette théorie tend à optimiser l'action des forces mécanisées en créant des schémas d'engagements opératifs et tactiques garantissant le succès dans l'affrontement. La Révolution dans les Affaires Militaires (RMA en anglais pour *Revolution in Military Affairs*) trouve son origine dans cette volonté de transformer le système militaire en profondeur pour obtenir un modèle opérationnel qui garant le succès. Plus que l'utilisation de la technologie pour dépasser tactiquement, et pour un moment donné, son adversaire, la RMA est une décision politique de changer durablement le fonctionnement, les procédés et les organisations afin de s'assurer des victoires sur une longue période. Cette pensée idéologique prônant la rationalité à l'extrême dans des situations où l'irrationalité, le hasard et le *« brouillard de la guerre »*[94] sont des données d'entrée, contient ce défaut intrinsèque. De plus, la conviction d'obtenir une victoire, par une action militaire basée sur des effets purement cinétiques et destructeurs, dans un temps limité, et en limitant aussi le nombre de pertes amis – la guerre zéro mort – simplifie l'équation pour le politique. Posséder un outil capable de résoudre un problème selon un mode d'emploi donné et selon un schéma connu implique une relative, mais trompeuse, tranquillité politique : pour obtenir un résultat, il suffit d'envoyer une force en quantité suffisante et technologiquement supérieure pour vaincre. Ce mythe est combattu notamment par Colin Gray qui relève la réduction voire l'annulation, dès lors, de la réflexion stratégique. L'auteur ne pense pas, au vu des résultats déplorables des campagnes menées par des forces pourtant en supériorité technologique, que l'équation magique existe. La RMA aurait donc vendu une transformation des armées pour obtenir des victoires stratégiques, alors que, si la transformation est bien systémique, elle doit être contrôlée, car ne mène qu'à une supériorité tactique, si les facteurs humains ne sont pas pris en compte dans une crise. Et Colin Gray va plus loin en condamnant la hiérarchie et les décideurs de l'armée américaine de se laisser aveugler par ce mythe, où tout, au final ne pourrait se résoudre que par une accélération de la boucle OODA[95], les tirs de précisions en pro-

[93] GRAY Colin S., *La Guerre au XXIème siècle, Un nouveau siècle de sang et de feu*, Economica, Paris, 2008, 423p., p88-112
[94] CLAUSEWITZ Carl Von, *De la Guerre*, Chapitre 2.
[95] OODA : Orientate, Observe, Decide, Action. Concept inventé par le pilote de chasse américain John Boyd en 1960, cette boucle de décision permet de schématiser les phases nécessaires pour réagir face à un ennemi.

fondeur sur les cibles stratégiques, les opérations basées sur les effets, *etc*. La RMA a créé un « *autisme stratégique* », selon lui, et l'action militaire n'est plus conçue comme la poursuite d'un but politique[96].

Si la recherche d'une transformation des armées en profondeur pour obtenir une réponse *a priori* plus efficace contre l'adversaire sur le terrain n'est pas née d'un concept américain, intéressons-nous tout de même à la RMA instituée au sein des armées des États-Unis dès la fin du XX^{ème} siècle. Pour reprendre le stratège britannique John Frederick Charles Fuller cité par Martin Van Creveld, l'idée qui sous-jacente à cette vision est que « *weapons, if only the right ones can be found, constitute ninety percent of victory* »[97]. La transformation des armées américaine commence avant la généralisation des communications satellitaires. C'est sous l'influence de Robert Mac Namara[98] que la Défense américaine se convertit à l'informatisation, notamment pour garantir ce « *cost effectiveness* » (ou rentabilité) recherché à l'instar des grandes compagnies privées. Sous le commandement du général Westmoreland, la guerre du Vietnam[99] fut, elle aussi marquée par la prédominance de l'informatisation et de la fourniture d'indicateurs numériques à outrance, pour tenter de qualifier tous les aspects de la guerre : l'économie, la logistique, les pertes, *etc*. Après la première Guerre du Golfe, les américains s'engagent vers l'emploi généralisé de moyens satellitaires jusqu'aux plus bas échelons afin de pouvoir commander avec des élongations dépassant les capacités de faisceaux hertziens dirigés[100]. Cette plus-value indéniable, obtenue dès la seconde Guerre du Golfe de 2003, est née de l'analyse du déploiement de l'opération *Desert Storm* de 1991 par le commandement militaire et le monde politique américain. En effet, il aura fallu imposer un rapport de force très favorable, avec une préparation de cinq mois et une projection de 500 000 hommes, pour vaincre. Par rapport au coût financier, la question se pose d'une révolution des affaires militaires permettant un usage systématique de la technologie pour obtenir plus rapidement, et à moindre frais, la décision[101]. En 1998, dans leur publication *Network*

[96] « *Qui plus est, malgré toute les alléchantes promesses, le concept de RMA explique bien trop peu la richesse et la complexité du caractère multidimensionnel de la guerre et de la stratégie.* » p.137
[97] « *Les armes, pour peu que les bonnes puissent être trouvées, constituent 90% de la victoire.* » Traduction du rédacteur, *in* VAN CREVELD, *Technology and War, op. cit*., p. 225
[98] *Ibid.* p.247
[99] Pour une description détaillée de la guerre du Vietnam du point de vue des Transmissions et du combat des communications, voir RAINES, *Rebecca Robbins, Getting the Message Through, A Branch History of the U.S Army Signal Corps*, Center of Military History United States Army, Washington D.C., 1996, 488p., p.359 à 390.
[100] Les liaisons de Faisceau Hertzien sont des liaisons dirigées permettant, pour les systèmes tactiques militaires, d'atteindre environ 30 km, ou de faire plusieurs bonds de 30km, en installant des relais. Les systèmes d'infrastructures peuvent atteindre au maximum 100km. Néanmoins, la liaison ne doit pas être perturbée par le relief, la végétation, des constructions ou des perturbations électromagnétiques.
[101] MAULNY Jean-Pierre, *La guerre en réseau au XXIe siècle*,Le Félin, Paris, 120p., p 31-36

Centric Warfare : its Origin and Future, le vice-amiral Arthur Cebrowski de l'US Navy et John J. Garstka donnent le nom du mythe mobilisateur technocentré à l'âge des nouvelles technologies de l'information et de communication : les opérations réseaux centrées. Ainsi, la guerre d'Irak de 2003 devient la première guerre où les moyens satellitaires sont déployés à grande échelle, tant pour le renseignement que pour la transmission de l'information au sein des chaînes hiérarchiques jusqu'aux plus bas échelons[102]. Cette RMA, basée sur les technologies de communication et de l'information, continue de créer une dépendance forte et une fascination des décideurs des armées occidentales pour un mythe de suprématie.

Mais, dans un univers où l'accélération du cycle décisionnel est devenue le *graal* de toute action armée, l'oubli des facteurs humains inhérents à toute situation conflictuelle et à l'action armée elle-même est une erreur tragique. Ainsi, Martin Van Creveld insiste sur le fait que notre raisonnement s'établit à l'aune des outils qui nous sont donnés pour résoudre un problème. L'émergence et le développement de l'informatique, fonctionnement par la gestion de données numériques (« *data processing* ») n'a fait que restreindre ou orienter nos réflexions et nos méthodes de travail vers des solutions apportant des solutions numériques. « *Since numbers are all that computers can work with, there is a tendency of computer-based quantitative analysis to disregard every factor that cannot be quantified. Armed conflict, however, is dominated above all by stress, danger, hardship, suffering, deprivation, and pain. Everything else being equal, the best army will be the one which possesses a thorough understanding of these factors and uses that understanding in order to cope with them* »[103]. Cette analyse n'est pas une opposition catégorique à l'utilisation de la technologie au profit des actions militaires. Elle implique juste la nécessité de concevoir les facteurs humains comme primordiaux dans tout conflit. La guerre se déroule entre hommes ou sociétés humaines et son déclenchement, son déroulement et la victoire ne peuvent être compris que dans un cadre humain et non uniquement scientifique. Cette vision de la guerre rejoint celle du colonel Ardant du Picq lorsqu'il écrit, dans ses *Etudes sur le combat* : « *Le combat est le but final des ar-*

[102] « *La guerre du Golfe qui s'est déroulée en 1990-19991 a vu les Américains mettre en œuvre une douzaine de satellites de reconnaissance photographique, d'écoute électronique et d'alerte avancée. Lors de la guerre du Kosovo, en 1998-1999, les Américains disposent de quarante-huit satellites quand les Européens n'en alignent que deux. Pendant la Seconde Guerre d'Irak en 2003, […] pour la première fois, les armées américaines disposent d'une information satellitaire 24 heures sur 24.*», VILLAIN Jacques, *A la conquête de l'espace : de Spoutnik à l'homme sur Mars,* Vuibert, Paris, 2008, 310p., p.202-206

[103] « *Alors que les ordinateurs ne peuvent travailler qu'avec des nombres, il y a une tendance pour l'analyse quantitative basée sur l'informatique de mépriser chaque facteur qui ne peut être quantifié. Pourtant, le conflit armé est dominé par-dessus tout, par le stress, le danger, la difficulté, la souffrance, la privation, et la douleur. Toute chose étant égale par ailleurs, la meilleure armée sera celle qui possèdera une compréhension approfondie de ces facteurs, et utilisera cette compréhension dans le but de les prendre en compte.* » Traduction du rédacteur, *in* VAN CREVELD, *Technology and War, op. cit.* p.247

mées, et l'homme est l'instrument premier du combat ; il ne peut être rien de sagement ordonné dans une armée, – constitution, organisation, discipline, tactique, – toutes choses qui se tiennent comme les doigts d'une main, – sans la connaissance exacte de l'instrument premier, de l'homme, et de son état moral en cet instant définitif du combat. […] Etudions donc l'homme dans le combat car c'est lui qui fait le réel »[104]. Pour lui, les forces morales sont fondamentales au combat. Au final, nous voyons bien que, malgré les efforts d'intégrer au maximum la technologie dans le domaine militaire, les victoires contre des ennemis réputés inférieurs ne sont pas garanties. Les guerres asymétriques, les petites guerres ou guérillas sont toujours menées par une armée ou des groupes ayant une forte cohésion ou idéologie, contre des armées comptant sur leur supériorité technologique. Et, comme le constate Martin Van Creveld avec la guerre menée au Vietnam ou avec l'impossibilité pour l'armée allemande de la Seconde Guerre mondiale de vaincre la guérilla menée par Tito, le résultat n'est généralement pas en faveur des armées conventionnelles. Si la technologie est un atout indéniable, elle ne doit pas être comprise comme la totalité de l'engagement ou la finalité de la recherche de solution. Dans le cadre du développement et de la maîtrise de l'espace cybernétique par les armées, ce principe doit rester fondateur de toute recherche et exploitation. Comme nous l'avons vu pour la maîtrise des communications dans les exemples historiques, la recherche d'outils permettant l'exploitation et le combat sur les espaces informationnels, ou les implications sur l'organisation doivent être dominés par l'idée de soutenir la compréhension des mécanismes humains.

3.2. Un juste équilibre entre esprit de corps et efficacité centralisée

L'intégration des différentes spécialités est-elle une garantie unique pour assurer une compréhension d'ensemble de l'espace cybernétique ? Comment intégrer la prise en compte des forces morales dans un combat situé dans un espace majoritairement immatériel ? La lutte dans le cyberespace peut-elle rester déconnectée du combat physique ?

Après une analyse historique de la relation entre la technologie et le domaine militaire, nous avons vu comment la compréhension des facteurs humains est primordiale. La technologie ne peut qu'appuyer le combat où les forces morales prévalent. De plus, l'appréciation de la situation selon des indicateurs issus de capteurs techniques ne remplace pas complètement l'analyse des facteurs psychologiques intrinsèques à la crise. Dans ce cadre, le combat dans le domaine cybernétique ne doit lui non plus pas se transformer en une compréhension unique-

[104] DU PICQ Ardant, Colonel, *Etudes sur le Combat*, Hachette, Paris, 1880, 304p., p.7-10

ment numérique du monde réel. La recherche de l'efficacité de l'organisation des unités militaires engagées dans un domaine CYBER nouvellement créé doit donc écarter cet égarement vers un fonctionnement uniquement tourné vers une efficacité dénombrable. Pour cela, les hommes et femmes participant à ce domaine de lutte doivent aussi savoir que leur réussite passe par la qualité de leurs forces morales.

Il est nécessaire de conserver un lien entre les missions cinétiques et les combattants d'un domaine CYBER intégrant toutes les spécialités liées à l'espace cybernétique.

Intégrer la dimension humaine dans ce domaine CYBER, c'est d'abord comprendre les missions sur lesquelles les combattants de ce domaine sont engagés. C'est ensuite s'assurer que l'organisation choisie conserve un lien avec une tradition d'unité assurant le maintien de la cohésion et des forces morales des combattants. Enfin, c'est considérer que l'intégration ne peut réussir qu'après une spécialisation inhérente à l'acquisition de compétences.

En premier lieu, considérons, comme nous l'avons vu dans notre réflexion sur les principes fondamentaux de la pensée cybernétique, une intégration des unités opérant sur le cyberespace. Le domaine CYBER ainsi créé, avec une mise sous tutelle organique et opérationnelle de ces unités au profit d'un échelon de commandement, doit aussi intégrer la prise en considération des facteurs humains pour s'engager avec succès dans le combat. Et cette intégration des facteurs humains ne peut s'effectuer qu'au regard des missions de ces unités. Toutes les unités incluses dans ce domaine ne travaillent en effet pas pour les mêmes objectifs, et il ne s'agit pas nier cette différence. La question se pose également sur le périmètre des unités comprises dans ce domaine. Dans les armées françaises, la mise en œuvre technique du cyberespace se distingue entre les unités des armées permettant le déploiement de réseaux de communication et informatiques au profit des opérations extérieures ou intérieures, et la DIRISI, opérateur et fournisseur de service mettant en œuvre les réseaux sur le territoire national et assurant les liens vers les opérations. Pour les opérations de protection du cyberespace, la Défense française scinde encore opérations et protection des réseaux en métropole. Dans cette lutte informatique défensive, les SOC (Security Operating Center) de la DIRISI assurent une veille sur les réseaux, alors que le CALID (Centre d'Analyse et de Lutte Informatique Défensive) possède de véritables compétences de recherche de l'agresseur et de réaction. En opérations, le commandement Cyber a récemment commencé la projection de moyens et de personnel au plus près des réseaux tactiques, qui font partie d'unité des armées. Pour le domaine

renseignement sur le cyberespace, les unités ont également des rôles différents, entre capacités tactiques et écoutes stratégiques. Quant à la lutte sur le domaine informationnel, la Défense possède un pôle principal d'action sur cet espace et des centres spécialisés pour le renseignement, permettant d'utiliser les outils numériques sur lesquels l'adversaire exprime ses opinions. L'exploitation du cyberespace implique donc de multiples entités au sein des armées et services de la Défense, et chacune possède ses spécialités. La destruction de cette organisation complexe au profit d'une structure intégratrice n'a pas été souhaitée jusqu'à présent, afin de laisser les opérateurs et les procédures se rôder. Une intégration de ses unités au profit de la maîtrise de l'espace cybernétique ne doit en effet pas effacer toute caractéristique des métiers très différents que nous avons évoqués, même si au final, l'étude tend vers cette création de domaine permettant un commandement, une gestion humaine et des procédures communes. Si les spécialités sont différentes, c'est bien la mission commune de maîtrise de l'espace cybernétique qui doit être mise en avant pour apporter de la cohésion à ce système.

En second lieu, après avoir vu la multiplicité des acteurs de l'espace cybernétique, intéressons-nous à la manière dont la prise en compte des facteurs humains doit être effectuée. Insuffler un esprit de corps est bien une fonction prioritaire de l'organisation des unités militaires en métropole. Si, bien souvent, les unités déployées en opération sont construites avec un assemblage des spécialités nécessaires, c'est parce que les déploiements répondent à une logique de coût et de stricte suffisance. L'unité organique, cette cellule de base en métropole, est le terreau pour instruire, former et projeter les hommes et femmes au service de la défense de la France et de ses intérêts. Et l'histoire des projections et des missions réalisées rejaillit sur l'unité organique pour construire un esprit de corps. Pouvoir donner une référence, une histoire à laquelle se référer, un état d'esprit dans la manière de conduire les missions, l'envie de se dépasser pour ses anciens et ses pairs, et au final garantir la cohésion lorsque le combat altère les capacités physiques ou de réflexion, tels sont les objectifs de cet esprit de corps. Alors, si comme le pense Ardant du Picq en démontrant que les aspects manœuvriers de la tactique ou la masse sont certes importants, mais que les facteurs moraux sont primordiaux au combat, il faut prendre garde à conserver au sein du système créé des repères efficaces aux combattants du cyberespace. Ainsi, les traditions créées par les unités militaires constituent un atout indéniable. Les conserver et les utiliser, même dans le cadre d'opérations qui ne pouvaient exister dans le passé, sont un moyen de tisser le lien entre passé et futur. L'intégration des unités au sein d'une même armée chargée de la maîtrise de l'espace cybernétique, ne doit pas tirer un trait sur l'histoire des combattants ayant participé au maintien de la liaison dans

les tranchées ou aux écoutes faites contre les puissances ennemies lors de la Première Guerre mondiale[105]. Mais, assurer une cohésion au sein d'une entité unique permettant une multiplicité des points de vue pour progresser dans le domaine et ne rien omettre dans l'appréciation de la situation, du développement et de la maîtrise de l'espace cybernétique passe par la création d'une histoire commune, de missions communes. L'intégration nécessite une transformation réalisée de manière nuancée, afin de concilier nouvelles missions et traditions.

Enfin, l'idée de l'intégration ne contredit pas une spécialisation initiale pour assurer la compétence du personnel sur des missions particulières. En revanche, c'est bien la compréhension d'une mission commune et d'un engagement commun sur le cyberespace qui pourra faire naître le sentiment d'appartenance à la même entité. Que ce soit pour soutenir les opérations dans les autres milieux ou pour lutter dans les réseaux, cette mission commune de la maîtrise de l'espace cybernétique englobe toute les visions en apportant les particularités de chacune pour renforcer, par la complexité, sa réalité. Ainsi, par exemple, l'utilisation des outils informatiques déployés en opération sont à être maîtrisés par des spécialistes du domaine mettant en œuvre ces outils. Le domaine CYBER s'attache donc tant aux réseaux qu'à l'utilisation qui en est faite afin d'avoir une connaissance parfaite du déploiement de la force amie et des implications en termes de faiblesses et risques d'exploitation par l'ennemi. De même, les activités de lutte menées sur les réseaux pourraient mener à infléchir certaines procédures de mise en œuvre des réseaux. Si la lutte sur le cyberespace se situe sur tous les niveaux : physique, logique et informationnel, alors il est nécessaire de comprendre les interactions entre tous ces niveaux. Ces relations entre les différents niveaux apportent bien plus de *néguentropie*[106] et donc de stabilité au système, pour en revenir à l'étude des principes de la pensée cybernétique. Une déconnection des opérateurs des différents niveaux peut en effet mener à des situations de blocage opérationnel. Par exemple, et pour les règles en usages sur les réseaux opérationnels français, la logique de séparation physique des réseaux de différente classification, ainsi que la méconnaissance par les spécialistes de la mise en œuvre (SIC) des outils installés (au profit des opérationnels), ou la distinction entre mise en œuvre amie et exploitation des réseaux neutres ou ennemies, sont quelques manifestations de processus homéostatiques issus de la séparation de ces niveaux. Chaque exemple cité possède en soi une propriété utile, qui, engagée dans un processus de transformation, s'enferme dans une simple résistance au changement.

[105] BONNEMAISON et DOSSE, *op. cit.* p.27-29
[106] Pour rappel : « *l'information fournie par un message comme étant essentiellement la valeur négative de son entropie » in* WIENER, *Cybernétique et société, L'Usage humain des êtres humains*, op. cit., p.53

3.3. Pour une humanisation du développement technologique

Pourquoi les avancées de la technologie provoquent-elles une crainte, notamment dans le domaine militaire ? La machine se substituera-t-elle à l'homme sur le champ de bataille pour obtenir plus aisément la victoire ? Et pour obtenir quelle victoire : tactique, stratégique ou politique ? Comment intégrer la volonté de l'homme dans cette réflexion sur la maîtrise de l'espace cybernétique ?

« *Si l'on demande la victoire en ignorant ce que l'on veut dire par là, on entend un fantôme frapper à la porte.* »[107] L'utilisation de la science au profit des armées n'implique pas seulement une erreur de compréhension de la situation, dans le cas d'une approche techno-centrée oubliant le contexte humain. Elle peut également, pour les scientifiques comme Norbert Wiener, penseurs de leur temps et de leur action, aboutir sur le pire des scénarios Alors que la guerre nucléaire est au centre des imaginations à son époque, la capacité des machines à prendre le dessus sur l'intelligence et la volonté humaines nourrit désormais les débats. Notre étude termine donc son chemin sur la définition de la propriété principale de la commande, au sens cybernétique, de ce domaine militaire CYBER : quel doit être le sens donné au développement du cyberespace et de son environnement, sa direction, son gouvernail ? Pour que l'homme reste au centre du conflit, mais surtout dans sa résolution, il est nécessaire d'affirmer sa prédominance dans sa capacité à créer une victoire pérenne.

Il n'est pas judicieux de confier aux machines la primauté sur le champ de bataille.

Pour ne pas confier la primauté aux machines dans le domaine militaire, percevons en premier lieu les craintes liées au transhumanisme. Puis, en explorant la notion de victoire juste, il apparaît de manière claire la complexité de la question et la difficulté de la formuler en algorithme. Enfin, c'est bien l'homme qui doit rester au centre de la décision, tant sur le champ de bataille que dans le développement des outils utilisés pour mener la guerre de demain.

La réflexion sur la place de l'homme par rapport à la machine est inhérente au développement scientifique et à ces utilisations concrètes pour les opérations militaires. Dans le cadre d'une réflexion sur le rôle du domaine CYBER et son organisation, nous avons vu pourquoi la direction de ce développement devrait également être incluse. Pour la DGSIC, organisme pourtant chargé de donner la direction de déploiement des réseaux de communica-

[107] WIENER, *La Cybernétique, Information et régulation dans le vivant et la machine*, op. cit., p309

tion et informatiques : « *Le secteur de la Défense, sauf pour de rares exceptions, n'est plus le moteur de l'innovation technologique. Alors que l'illusion pourrait amener à croire que le ministère a le choix d'adopter ou non une nouvelle technologie SI, il sera bien souvent amené à s'adapter aux solutions proposées par le secteur privé, en recherche permanente d'efficience.* »[108] Contrairement à cette vision, notre étude conclut sur la nécessité d'engager la Défense dans une prise de responsabilité sur les outils et les procédés à utiliser concernant le cyberespace, pour notamment en connaître les conséquences sur son organisation, les opportunités et risques induits. Et le plus grand danger de cette poursuite sans contrôle pourrait bien se trouver dans le transhumanisme. Cette notion regroupe tous les procédés et courants de pensée prônant un dépassement de l'humanité par une autre entité ; dans le cas présent, les machines créées par l'homme. Pour Alan Turing, précurseur des recherches en intelligence artificielle (IA), « *nous aimerions croire que l'homme est de quelque subtile façon supérieur au reste de la Création. (…) Je ne pense pas que cet argument soit suffisamment substantiel pour rendre nécessaire une réfutation. La consolation serait plus appropriée.* »[109] Pour lui, « *nous pouvons espérer que les machines concurrenceront finalement l'homme dans tous les champs purement intellectuels.* »[110] Dans son analyse de l'automatisation de la pensée, Alan Turing prouve d'abord la validité de l'intelligence artificielle, avant de démontrer la supériorité future de la machine sur les capacités intellectuelles humaines. Etonnamment, aucune ligne ne soulève le problème du rapport entre l'homme et la machine, ou de l'éthique d'un tel développement. Si, à l'heure actuelle, l'intelligence artificielle progresse, sans toutefois avoir atteint une forme « *complète* »[111], de nombreux scientifiques s'interrogent sur les potentialités et les dangers obtenues au final. En 2014, Stephen Hawkins s'engage publiquement[112], en estimant dangereux pour l'humanité un développement de l'IA, l'évolution biologique humaine ne pouvant rivaliser avec la capacité de reconfiguration d'un système automatisé. Plus récemment en 2015, une lettre ouverte[113] est publiée demandant l'interdiction de toute forme de recherche et de développement de robots tueurs, signée par les plus grands noms de la recherche ou du développement informatique, et de l'économie numérique. Enfin en 2016, c'est

[108] Voir l'article *Quel Transformation numérique pour le ministère* in *Transmetteurs n°10* – Juin 2016
[109] TURING Alan, *Les ordinateurs et l'intelligence* in TURING A. et GIRARD Jean-Yves, *La Machine de Turing*, Seuil, Paris, 1995, 184p.
[110] Id.
[111] « *Les formes primitives d'intelligence artificielle que nous avons déjà se sont montrées très utiles. Mais je pense que le développement d'une intelligence artificielle complète pourrait mettre fin à l'humanité.* » *in* HAWKING Stephen, interview donnée à la BBC en 2014 et disponible sur le lien http://mobile.lemonde.fr/pixels/article/2014/12/03/hawking-l-intelligence-artificielle-pourrait-mettre-fin-a-l-humanite_4533135_4408996.html , consulté le 25/01/2017
[112] *Id.*
[113] Disponible sur le site https://futureoflife.org/open-letter-autonomous-weapons consulté le 28/01/207

un partenariat sur l'éthique[114] qui est lancé afin de pouvoir responsabiliser cette recherche, qui influe de manière certaine sur la vie de l'homme. La pensée cybernétique née en 1947 prend alors tout son sens dans le questionnement actuel sur le rapport entre l'homme et la machine. Le dépassement de l'homme par une de ses inventions visant à égaler ou surpasser la pensée humaine, dans un environnement en réseau permettant d'accéder à toutes les ressources vitales de la société humaine, génère une crainte légitime du transhumanisme. En étendant cette crainte aux armes dotées d'une IA, nous comprenons pourquoi la Défense doit accompagner le développement de ces recherches : afin de ne pas rester à l'écart d'enjeux cruciaux pour nos sociétés et *a fortiori* des futurs conflits.

Surtout, en reprenant l'idée précédemment mentionnée relevant l'incapacité pour les outils numériques d'apprécier la totalité d'une situation humaine, nous pouvons affirmer qu'il reste très difficile pour une intelligence artificielle d'apprécier un conflit humain sur le long terme. La notion de victoire, déjà complexe pour l'intelligence humaine, n'est pas automatisable, sinon par la destruction pure et simple de l'ennemi. Dans tous les autres cas, l'homme devra rester juge de la décision. En effet, au-delà de la victoire, c'est une victoire juste qui est recherchée par les sociétés entrant en guerre. Béatrice Heuser étudie de manière très précise la naissance et l'évolution de cette justice de la guerre et dans la guerre (« *jus ad bellum, jus in bello* ») qui caractérise l'engagement dans tous les conflits, avec, bien sûr, des nuances notables sur le respect de certaines normes relatives aux époques[115]. Cette relativité correspond à la morale de chaque société, née de son histoire et de sa culture. Car, avant de parler de victoire, les causes de la guerre et les moyens de la mener prévalent et influent sur le résultat. La légitimité de faire la guerre, d'abord, varie considérablement variée au fil du temps et des sociétés : « *les 'causes justes' de la tradition catholique d'Augustin et de Thomas d'Aquin furent ignorées par Machiavel* »[116], par exemple. Cette justification de s'engager militairement peut aussi être comprise de manière moins naïve : afficher une raison moralement avouable pour un but moins avouable. Mais elle permet de fixer un cadre sur ce qui paraît acceptable et ce qui soulève l'indignation, à une époque donnée. Les règles encadrant l'usage de la violence sont, elles, une limitation imposée afin de traiter son ennemi comme lui nous traite, de conserver le soutien de sa propre opinion publique, ou, plus pragmatiquement, pour s'imposer sans créer un sentiment de revanche indélébile. Et, là où réside une difficulté d'appréhension

[114] Voir l'article de TUAL Morgane, *Intelligence artificielle : les géants du Web lancent un partenariat sur l'éthique*, disponible sur le lien http://mobile.lemonde.fr/pixels/article/2016/09/28/intelligence-artificielle-les-geants-du-web-lancent-un-partenariat-sur-l-ethique_5005123_4408996.html consulté le 24/02/2017
[115] HEUSER, *Penser la Stratégie, de l'Antiquité à nos jours, op. cit.,* p.35-64
[116] *Ibid*., p.48

de toutes ces nuances par l'homme, le risque est grand d'obtenir une réponse algorithmiquement valide, mais humainement fausse. Le fait même de la présence d'une machine dans le système étudié – le conflit –, implique une réaction de l'environnement : ennemi, population, alliés, qui peut aller à l'encontre des buts de l'action initiale. Au niveau technique, l'appréciation quantitative d'une situation par la machine ne peut remplacer l'évaluation qualitative de l'homme. Dans le développement des armes comme dans le développement du cyberespace et de son environnement, comprendre les interactions entre la guerre et la société ne peut être dévolu qu'à l'homme.

Finalement, après avoir vu les travers et les difficultés que rencontre le développement technologique, affirmons ici que l'homme doit être au centre de la décision, tant sur le champ de bataille physique, que pour le développement des technologies. Définir la direction, cela signifie autant donner un axe qu'encadrer le mouvement au cours du temps. En expliquant l'irréversibilité de certains systèmes, Norbert Wiener en conclu l'existence d'une direction du temps et des individus : « *l'individu est une flèche pointée dans une seule direction à travers le temps, comme l'espèce l'est du passé vers l'avenir* »[117]. Pour illustrer cette affirmation, il appuie sa réflexion sur la biologie : « *la naissance n'est pas l'exact opposé de la mort* »[118]. En effet, cet aspect fondamental dans la cybernétique qu'est la recherche du mécanisme de commande, est dû au fait qu'il détermine la volonté et l'objectif du système étudié. Dans notre cas, la commande d'un système militaire ayant comme mission la maîtrise de l'espace cybernétique doit être empreint de la nécessité de conserver l'homme au centre de la réflexion. Cette approche systémique permet dès lors de comprendre pourquoi des questions essentielles comme la place de l'homme dans la robotisation, dans le développement d'armes dotées d'IA, de drones armés, ne s'éloignent guère du développement de l'espace cybernétique. Elles sont même inclues dans ce champ de réflexion. Le cyberespace est un outil intégrateur de toute les capacités technologiques développées par des sciences diverses : biologie, robotique, IA, réseaux de neurones, réseaux informatiques, cryptographie, *etc*. Ayant pris un essor indéniable grâce à la cybernétique, qui a introduit l'approche systémique, la notion de message et de rétroaction, ces sciences réaffirment plus profondément le besoin de pensée cybernétique en se combinant à travers le cyberespace. Et cette pensée conduit naturellement vers le besoin de définir l'homme comme décideur : il doit analyser selon des données fournies par la machine, décider de l'action des machines, mais ne pas subir l'implacable algorithme défini de manière

[117] WIENER, *La Cybernétique, Information et régulation dans le vivant et la machine, op.cit*. p.105
[118] Id.

arbitraire et erroné par un autre homme, ou corrigé par une machine. Jusqu'à présent, dépasser technologiquement son adversaire n'a pas été une garantie de vaincre. Ce seul objectif, placé généralement sous la bannière de l'économie des vies humaines (la guerre zéro mort), ne peut être synonyme de victoire assurée. Nul ne doute que chaque camp souhaite économiser des vies humaines. Mais, seul le camp qui comprend les ressorts intimes du conflit, et qui a la capacité d'agir, avec violence ou en dissuadant suffisamment son adversaire, a la capacité d'aboutir à ses fins. Si la stratégie est pour le général André Beaufre, « *l'art de la dialectique des volontés employant la force pour résoudre leur conflit* »[119], il ne peut donc être de victoire sans volonté humaine et sans compréhension de la volonté humaine de son adversaire. C'est bien en cela que la pensée cybernétique apporte un éclairage instructif sur le développement des moyens et des organisations mises en place pour défendre le cyberespace. Ne pas comprendre leur intégration dans un système où des relations sont réalisées avec toutes les spécialités connexes : mise en œuvre des réseaux, développement de robots, recherche sur le futur du cyberespace, implication sur la société et les usages, prive le modèle d'une complexité et de la définition d'une direction.

[119] BEAUFFRE André (Général), *Introduction à la stratégie*, Hachette, Paris, 1998, 194p., p.34

Conclusion

Dans son dernier essai prospectif[120], Joël de Rosnay propose un hyperhumanisme, dépassant le transhumanisme, où l'homme intégrera les capacités des technologies de communications et de l'information, et de la robotique pour obtenir de plus grandes capacités physiques et surtout cognitives. Dans ce cadre, il ne voit pas de compétition entre l'homme et la machine, mais bien une amélioration des capacités de l'homme par la mise en réseau des connaissances de l'humanité. Cette vision, qui n'est pas, dans son ouvrage, contrariée par une réalité géopolitique ou sociologique, permet de conserver pour l'homme le rôle d'utilisateur de technologie. Mais l'usage de la technologie n'est jamais réalisé *in vitro* : l'homme possède ses références, sa culture, son expérience et se conçoit comme source et finalité des conflits. Dans ce débat sur la place de l'homme par rapport à la technologie, la question du développement des armes est toute particulière : elle rappelle que l'homme est mortel et avec lui l'humanité. « *Nous autres, civilisations, savons maintenant que nous sommes mortelles* »[121] écrit Paul Valéry à l'issue de la Première Guerre Mondiale.

Si la guerre se déploie désormais sur le cyberespace au travers l'utilisation des réseaux informatiques, la recherche de renseignement sur ces réseaux permettant des opérations, ou la lutte contre les opinions adverses, la Défense et les armées françaises se sont adaptées. Un commandement cyber permet de planifier et commander les opérations sur le cyberespace. Néanmoins, l'étude systémique, telle qu'engendrée par la pensée cybernétique, permet d'identifier les lacunes dans l'appréhension du cyberespace. La définition d'un espace cybernétique compris comme le cyberespace, sa mise en œuvre, son développement, sa défense, les outils, usages et implications sur les organisations, met en avant une vision intégratrice de toutes les capacités employables sur cet espace. En apportant plus de complexité à la réflexion par l'intégration des domaines SIC, RENS et OPS concernés par le cyberespace dans un domaine CYBER militaire, l'objectif est bien de s'attacher à maîtriser l'espace cybernétique et non rester en réaction face aux évolutions. De plus, comprenant la résistance au changement inhérente à toute organisation humaine, et en particulier militaire, les évolutions liées à la technologie et en particulier aux communications constituent un élément capital dans la résilience d'une unité militaire. Leur prise en considération doit se situer au plus haut niveau, et

[120] ROSNAY Joël de, *Je Cherche à comprendre : Les Codes cachés de la nature et de l'univers*, Edition Les Liens Qui Libèrent, Paris, 2016, 170p.
[121] VALERY Paul, *La Crise de l'esprit, Première Lettre*, 1919.

ne pas être disséminée au gré des déploiements parcellaires de technologie, pour apporter une réponse globale et unifiée sur l'ensemble de l'organisation militaire. Ainsi, la création d'une armée dédiée à la maîtrise de l'espace cybernétique garantit une approche centrée sur le besoin des hommes pour améliorer leur compréhension de la situation, et non une appréciation de la situation uniquement numérique. Au final, le rapport entre l'homme et la machine trouve une solution dans la définition de la commande, notion cybernétique associée à la volonté du système, son objectif intrinsèque. La commande ou direction de l'organisation chargée de maîtriser l'espace cybernétique doit placer l'homme au centre de la décision dans toute réflexion, afin de conserver un lien avec le caractère profondément humain des conflits. Pour être définie, cette commande doit elle-même exister distinctement au sein de l'organisation créée.

Pour Isaac Asimov, scientifique et auteur de science fiction, « *the saddest aspect of life right now is that science gathers knowledge faster than society gathers wisdom*»[122]. Les recherches sur l'intelligence artificielle donnent des exemples toujours plus prégnants de cette affirmation. Seule une compréhension de l'usage de la technologie sera de nature à inverser la relation dans cette évolution.

[122] « *L'aspect le plus triste de la vie est que, désormais, la science engrange plus vite de savoir que la société n'amasse de sagesse.* » Traduction du rédacteur, in ASIMOV Isaac and SHULMAN Jason A., *Isaac Asimov's Book of Science and Nature Questions*, Weidenfeld & Nicolson, New York, 1988, 326p., p.281.

Bibliographie

Comme mentionné dans l'étude, les recherches se sont portées sur trois axes majeurs : la pensée cybernétique, l'actualité de la cyberdéfense et des réponses militaires, l'histoire de la stratégie dans son rapport aux technologies de communication et de l'information. En plus de ces axes majeurs, les ouvrages de stratégie générale, la littérature de science-fiction, la veille sur des sites d'information sur le développement ou les actualités du cyberespace ont enrichi notre vision de ce domaine en constante évolution.

Sur la pensée cybernétique :

- WIENER Norbert, *La Cybernétique, information et régulation dans le vivant et la machine,* Paris, Seuil, 2014 (texte de 1948), 370p., traduction et présentation de LE ROUX Ronan
- WIENER Norbert, *Cybernétique et société, L'usage humain des êtres humains*, Paris, Seuil, 2014 (texte de 1954), 226p.
- COUFFIGNAL Louis, La Cybernétique, Paris, PUF, « Que sais-je ? » n°683, 3 ed., 1968, 130p.
- TURING Alan, *Les ordinateurs et l'intelligence* in TURING A. et GIRARD Jean-Yves, *La Machine de Turing*, Seuil, Paris, 1995, 184p.
- ROSNAY Joël (de), *Le Macroscope, vers une vision globale*, Paris, Seuil, 1975, 376p.
- ROSNAY Joël de, *Je Cherche à comprendre : Les Codes cachés de la nature et de l'univers*, Edition Les Liens Qui Libèrent, Paris, 2016, 170p.
- DAVID Aurel, *La Cybernétique et l'humain*, Gallimard, Paris, 1965.
- CONWAY Flo et SIEGELMAN Jim, *Héros pathétique de l'âge de l'information : en quête de Norbert Wiener, père de la cybernétique*, Paris, Hermann, 2012, 422p.
- SHANNON Claude E., *A Mathematical theory of communication*, Bell System Technical Journal, vol.27, n°3, 1948
- BARBOTIN J. CNE, *Cybernétique et commandement*, Mémoire de l'Ecole Supérieure de Guerre 74ème promotion (1960-62), Bibliothèque patrimoniale de l'Ecole Militaire, 33p.
- LADONNE CEN, *Application des principes de la cybernétique aux problèmes d'organisation*, Mémoire de l'Ecole Supérieur de Guerre 80ème promotion (1967), Bibliothèque patrimoniale de l'Ecole Militaire.

Sur le cyberespace :

- KEMPF Olivier, *Introduction à la cyberstratégie*, Economica, Paris, 2012, 176 p.
- VENTRE Daniel, *Cyberattaque et Cyberdéfense*, Lavoisier, Paris, 2011, 312 p.
- BONNEMAISON Aymeric et DOSSE Stéphane, *Attention : Cyber ! Vers le combat cyber-électronique, Economica*, Paris, 2014, 222 p.
- COUSTILLERES Arnaud (Vice amiral), *in* RAUFER Xavier, *La Première Cyber-guerre mondiale ?*, Micro Application, Paris, 2015, 300 p.
- Présentation du pacte cyber (2014) http://www.defense.gouv.fr/actualites/articles/presentation-du-pacte-defense-cyber, consulté le 28/02/2017
- Discours de Jean-Yves Le Drian - Lundi 12 Décembre 2016, à l'occasion de la visite de la Direction générale de l'armement – Maîtrise de l'information (DGA-MI), http://www.defense.gouv.fr/ministre/prises-de-parole-du-ministre/prises-de-parole-de-m.-jean-yves-le-drian/cyberdefense-discours-de-jean-yves-le-drian-lundi-12-decembre-2016 , consulté le 12 février 2017
- Glossaire de l'ANSSI : https://www.ssi.gouv.fr/particulier/glossaire/c/
- GROS P., JOUBERT V. et COSTE F., *Vulnérabilité et résilience du C2 moderne*, rapport n°305/FRS/C2 du 2 juillet 2014
- TUAL Morgane, *Intelligence artificielle : les géants du Web lancent un partenariat sur l'éthique*, disponible sur le lien http://mobile.lemonde.fr/pixels/article/2016/09/28/intelligence-artificielle-les-geants-du-web-lancent-un-partenariat-sur-l-ethique_5005123_4408996.html consulté le 24/02/2017
- HAWKING Stephen, interview donnée à la BBC en 2014 et disponible sur le lien http://mobile.lemonde.fr/pixels/article/2014/12/03/hawking-l-intelligence-artificielle-pourrait-mettre-fin-a-l-humanite_4533135_4408996.html , consulté le 25/01/2017
- *Quel Transformation numérique pour le ministère* in *Transmetteurs n°10* – Juin 2016
- WALDROP Mitch, *DARPA and the Internet revolution*, publié sur le site de la DARPA et disponible sur le lien http://www.darpa.mil/attachments/%282O15%29%20Global%20Nav%20-%20About%20Us%20-%20History%20-%20Resources%20-%2050th%20-%20Internet%20%28Approved%29.pdf consulté le 14/01/2017

Stratégie et technologie :

- VAN CREVELD Martin, *Command in War*, USA, Harvard University Press, 1985, 339p.
- VAN CREVELD Martin, *Technology and War, From 2000 BC to the present*, n.c, Simon and Schuster, 2010, 352p.
- HEUSER Béatrice, *Penser la Stratégie, de l'Antiquité à nos jours*, Picard, Paris, 2013, 434 p.
- GRAY Colin S., *La Guerre au XXIème siècle, Un nouveau siècle de sang et de feu*, Economica, Paris, 2008, 423p.

Stratégie générale:

- KEEGAN John, *La Première Guerre Mondiale*, Perrin, Paris, 2003, 560p.
- CLAUSEWITZ Carl Von, *De la Guerre*.
- Réponse de M. Paul Valéry au discours de M. le maréchal Pétain, https://fr.wikisource.org/wiki/R%C3%A9ponse_de_M._Paul_Val%C3%A9ry_au_discours_de_M._le_mar%C3%A9chal_P%C3%A9tain , consulté le 24 janvier 2017
- BEAUFFRE André (Général), *Introduction à la stratégie*, Hachette, Paris, 1998, 194p.
- DU PICQ Ardant, Colonel, *Etudes sur le Combat*, Hachette, Paris, 1880, 304p.

Littérature :

- ORWELL George, *Nineteen eighty-four*, n.d., Penguin Books, 1949, 254p.
- WILSON Robert Charles, *Spin*, TOR, New York, 2005, 460 p.
- WILSON Robert Charles, *Axis*, Denoël, Paris, 2009, 490 p.
- WILSON Robert Charles, *Vortex*, Denoël, Paris, 2012, 400 p.
- VALERY Paul, *La Crise de l'esprit, Première Lettre*, 1919.
- ASIMOV Isaac and SHULMAN Jason A., *Isaac Asimov's Book of Science and Nature Questions*, Weidenfeld & Nicolson, New York, 1988, 326p.
- ASIMOV Isaac, *Le Grand Livre des Robots, Tome 1 : Prélude à Trantor*, Presses de la Cité, Paris, 1990.
- ASIMOV Isaac, *Le Grand Livre des robots : Tome 2 : La Gloire de Trantor*, Presses de la Cité, Paris, 1991.
- CARRERE Emmanuel, *Je suis vivant et vous êtes morts*, Paris, Seuil, 1993, 420p.

Annexe 1 : Organisation du commandement français de la cyberdéfense

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE LA DÉFENSE

ÉTAT-MAJOR
DES ARMÉES

Paris, le 19 janvier 2017
N° D 17.000517/DEF/EMA/CYBER/NP

NOTE

à l'attention de

destinataires *in fine*

OBJET : note d'organisation de l'état-major de la cyberdéfense, structure de préfiguration du commandement de la cyberdéfense.

RÉFÉRENCES : a) instruction ministérielle 900/DEF/CAB/-- du 26 janvier 2012 ;
b) instruction n°600/DEF/EMA/ESMG/CDA du 22 avril 2015 ;
c) décision ministérielle n°6188 DEF/EMA/PERF/BORG/NP du 13 juin 2016;
d) décision ministérielle n° 10131DEF/CAB/CMIN du 12 janvier 2017.

P. JOINTES : a) annexe I - organisation de l'état-major de la cyberdéfense ;
b) annexe II - organigramme de l'état-major de cyberdéfense.

Par la décision ministérielle de première référence en annexe, un état-major de la cyberdéfense, structure de préfiguration du commandement de la cyberdéfense, est créé au sein de l'état-major des armées (EMA).

Cet état-major soutient l'officier général de cyberdéfense dans l'exercice de ses responsabilités. Il a également pour mission de préciser, sous l'égide du Haut fonctionnaire correspondant de défense et de sécurité (HFCDS) du ministère, quelles seront les responsabilités du futur commandement de la cyberdéfense en matière de protection et de défense des systèmes d'information du ministère.

L'organisation décrite en annexe, moyennant les éventuels ajustements sur le domaine de la protection et de la défense mentionnés ci-dessus et le retour d'expérience de la période de préfiguration, a vocation à figurer dans l'instruction relative au fonctionnement de l'EMA une fois les textes réglementaires publiés.

MINISTÈRE DE LA DÉFENSE

Amiral Philippe Coindreau
Major général des armées

60 Boulevard du Général Martial Valin – CS 21623 – 75509 Paris Cedex 15 - 09 88 68 10 78

DESTINATAIRES :
- SC OPS ;
- SC PLANS ;
- SC PERF ;
- OG RIM ;
- OG CYBER ;
- OAMGA ;
- C2A.

COPIES :
- MINDEF CAB/CM1 ;
- CEMA/CAB ;
- DGA ;
- SGA ;
- DGSE ;
- DGSIC ;
- DPID ;
- DRM ;
- DCSSA ;
- DCSCA ;
- DCSEA ;
- DIRISI DC ;
- MGAT ;
- MGM ;
- MGAA ;
- COS ;
- CPOIA ;
- CPCO ;
- Archives générales.

ANNEXE I à la note n° D.17.000577 /DEF/EMA/CYBER/NP du 19 janvier 2017

ORGANISATION DE L'ETAT-MAJOR DE LA CYBERDEFENSE, STRUCTURE DE PREFIGURATION DU COMMANDEMENT DE LA CYBERDEFENSE

1. ATTRIBUTIONS

L'officier général cyberdéfense et son état-major sont placés sous l'autorité du chef d'état-major des armées au sein de l'état-major des armées.

L'officier général cyberdéfense assiste et conseille le ministre de la défense dans son domaine de compétence.

Il assure la défense et la protection des systèmes d'information du ministère de la défense dans le cadre prévu par l'article L 2321-2 du code de la défense et l'instruction ministérielle 900 citée en référence.

Il est en charge, sous l'autorité du sous-chef d'état-major « opérations », de concevoir, planifier, préparer et conduire les opérations militaires dans l'espace numérique. A ce titre, il contribue à la planification et à la conduite des opérations au niveau stratégique en apportant une expertise cyber au commandement des armées et en particulier au chef du Centre de planification et de commandement des opérations (CPCO) au travers de la fonction de chef cyber du CPCO.

Il contribue à la conception et à la mise en œuvre d'une politique des ressources humaines de cyberdéfense.

Il coordonne la contribution des armées et organismes interarmées à la politique nationale et internationale de cyberdéfense, notamment pour l'élaboration et la mise en œuvre des plans de coopération.

Il coordonne l'expression des besoins transverses spécifiques du domaine et assure la cohérence d'ensemble du modèle cyber du ministère.

2. ORGANISATION

Placé au sein de l'EMA, l'état-major de la cyberdéfense (EMCYBER) comprend :

- le pôle « opérations » ;
- le pôle « innovation et ressources » ;
- le pôle « développement et stratégie ».

Il dispose du « Centre des réserves et de préparation opérationnelle de cyberdéfense » (CRPOC) sur lequel il exerce son autorité hiérarchique et fonctionnelle.

Il dispose en outre de chargés de mission.

Il exerce son autorité fonctionnelle sur les unités spécialisées de cyberdéfense que sont le centre d'analyse et de lutte informatique défensive (CALID) et le centre d'audit SSI (CASSI) de la DIRISI ; le détachement d'action numérique et le groupe des opérations numériques du CIAE et la 807 CTRS de l'armée de terre. Il fixe les missions et objectifs à la capacité de lutte informatique offensive nationale.

Cet ensemble a vocation à constituer le futur commandement de cyberdéfense.

2.1. Le chef d'état-major

Un chef d'état-major est chargé d'assurer la cohérence et la coordination de l'ensemble des travaux conduits au sein de l'EMCYBER, de piloter les dossiers transverses et la montée en puissance du domaine cyber. Il est également responsable du bon fonctionnement de l'EMCYBER.

Il exerce l'autorité hiérarchique sur le CRPOC et les antennes[1] de l'EMCYBER localisées hors du site de Balard.

2.2. Le pôle « Opérations » de cyberdéfense

Le pôle « Opérations » est placé sous l'autorité d'un chef qui dispose du « centre opérationnel », d'un service « emploi » et d'un service « protection-défense ». Le chef du pôle « opérations » assume les fonctions d'adjoint cyber du CPCO. A ce titre, avec les officiers désignés de son pôle, il contribue à l'anticipation, la veille, la planification et la conduite de niveau stratégique. Ces officiers participent aux processus internes du CPCO et apparaissent dans l'organisation du CPCO où ils sont décrits en renfort.

Le centre opérationnel :

- exerce le contrôle opérationnel des unités spécialisées et de la chaîne opérationnelle de lutte informatique défensive engagées dans les opérations militaires dans l'espace numérique ;
- propose la posture de cyberdéfense ministérielle ;
- dirige la cellule de crise ministérielle et contribue aux cellules de crise interministérielles.

Le service « Protection-défense » :

- édicte une politique de sécurité des systèmes d'information et en vérifie l'application sur le périmètre définit par l'IM 900 citée en référence ;
- assure la cohérence des dispositions de protection et de défense ;
- anime le réseau des officiers de sécurité des systèmes d'information au sein des armées et organismes interarmées ;
- anime le réseau des officiers de lutte informatique défensive au sein des armées et organismes interarmées ;
- commande l'emploi du chiffre des armées.

Le service « Emploi » de la cyberdéfense :

- participe à l'élaboration et à l'évolution des concepts et de la doctrine de cyberdéfense ainsi que le retour d'expérience ;
- définit l'emploi et le niveau de préparation opérationnelle des unités spécialisées de cyberdéfense ;
- intègre les entraînements interarmées de cyberdéfense, ainsi que la participation française aux exercices internationaux de cyberdéfense, dans le cycle de préparation opérationnelle interarmées ;
- définit les objectifs de recrutement, de préparation opérationnelle et d'emploi de la réserve de cyberdéfense, opérationnelle comme citoyenne.

2.3. Le pôle « Innovation et Ressources »

Le pôle « Innovation et ressources » est placé sous l'autorité d'un chef qui dispose d'un service « Equipements spécifiques », d'un service « Ressources humaines et formation », d'un service « Ressources financières ».

Le chef du pôle « Innovation et ressources » contribue, en étroite collaboration avec la sous-chefferie « Plans », à la préparation de l'avenir du domaine de la cyberdéfense.

Le service « Equipements spécifiques » de cyberdéfense :

- contribue à l'expression des besoins en équipements spécifiques de cyberdéfense, et à la cohérence capacitaire ;
- fédère et coordonne les besoins opérationnels des unités spécialisées de cyberdéfense ;
- fait conduire des expérimentations et contribue à l'innovation dans le domaine de la cyberdéfense.

[1] Une partie des effectifs du service « protection-défense » sont implantés sur les sites d'Arcueil, Kremlin-Bicêtre et Rennes. Ces antennes ont vocation à être rassemblées à Rennes à partir de l'été 2017.

Le service « Ressources humaines et formation » de cyberdéfense :

- participe, en liaison avec les employeurs et les directions des ressources humaines du ministère à l'élaboration d'une politique de ressources humaines transverse pour le personnel qui opère dans l'espace numérique ;
- exprime, en coordination avec les armées et organismes interarmées, les besoins en effectifs pour l'ensemble des volets de la cyberdéfense ;
- contribue à définir les objectifs de formation (niveau et flux) ;
- concourt, en lien avec les employeurs et les directions des ressources humaines du ministère, au recrutement de profils susceptibles de servir dans un des métiers de la cyberdéfense.

Le service « Ressources financières » de cyberdéfense :

- contribue à la préparation du volet physico-financier cyber de la programmation militaire ;
- participe aux travaux de planification financière en liaison avec les autres divisions de l'état-major des armées ;
- suit les engagements des ressources financières allouées à la cyberdéfense.

2.4. Le pôle « Développement et stratégie »

Le pôle « Développement et stratégie » est placé sous l'autorité d'un chef qui dispose d'un service « Coopération internationale », d'un service « Coordination nationale » et d'un service « Communication ».

Le chef du pôle « Développement et stratégie » est chargé de contribuer à la conception et à l'accompagnement des dynamiques ministérielles, nationales et internationales, en matière de cyberdéfense.

Le service « Coopération internationale » de cyberdéfense :

- élabore et conduit les relations militaires bilatérales avec les armées étrangères et les organismes militaires internationaux, en concertation avec l'officier général « relations internationales militaires » qu'il tient informé ;
- veille à la cohérence des actions menées par les armées et organismes interarmées ;
- participe, en liaison avec la direction générale des relations internationales et de la stratégie, à l'élaboration des positions du ministère de la défense auprès des instances politico-militaires de l'Organisation des Nations unies, de l'Union européenne et de l'Organisation du traité de l'Atlantique Nord.

Le service « Coordination nationale » de cyberdéfense :

- représente le ministère de la défense dans les instances interministérielles ;
- siège dans les instances du « pôle d'excellence cyber » ;
- établit avec le secteur privé les liens et partenariats nécessaires à l'accomplissement de ses différentes missions. A ce titre, il entretient des relations privilégiées avec les industriels de défense et les entreprises opérant dans le secteur ;
- développe et anime le réseau de la réserve citoyenne de cyberdéfense (RCC), en liaison avec les armées et organismes interarmées ;
- suit et coordonne les travaux des chaires de cyberdéfense soutenues par les armées et l'IHEDN.

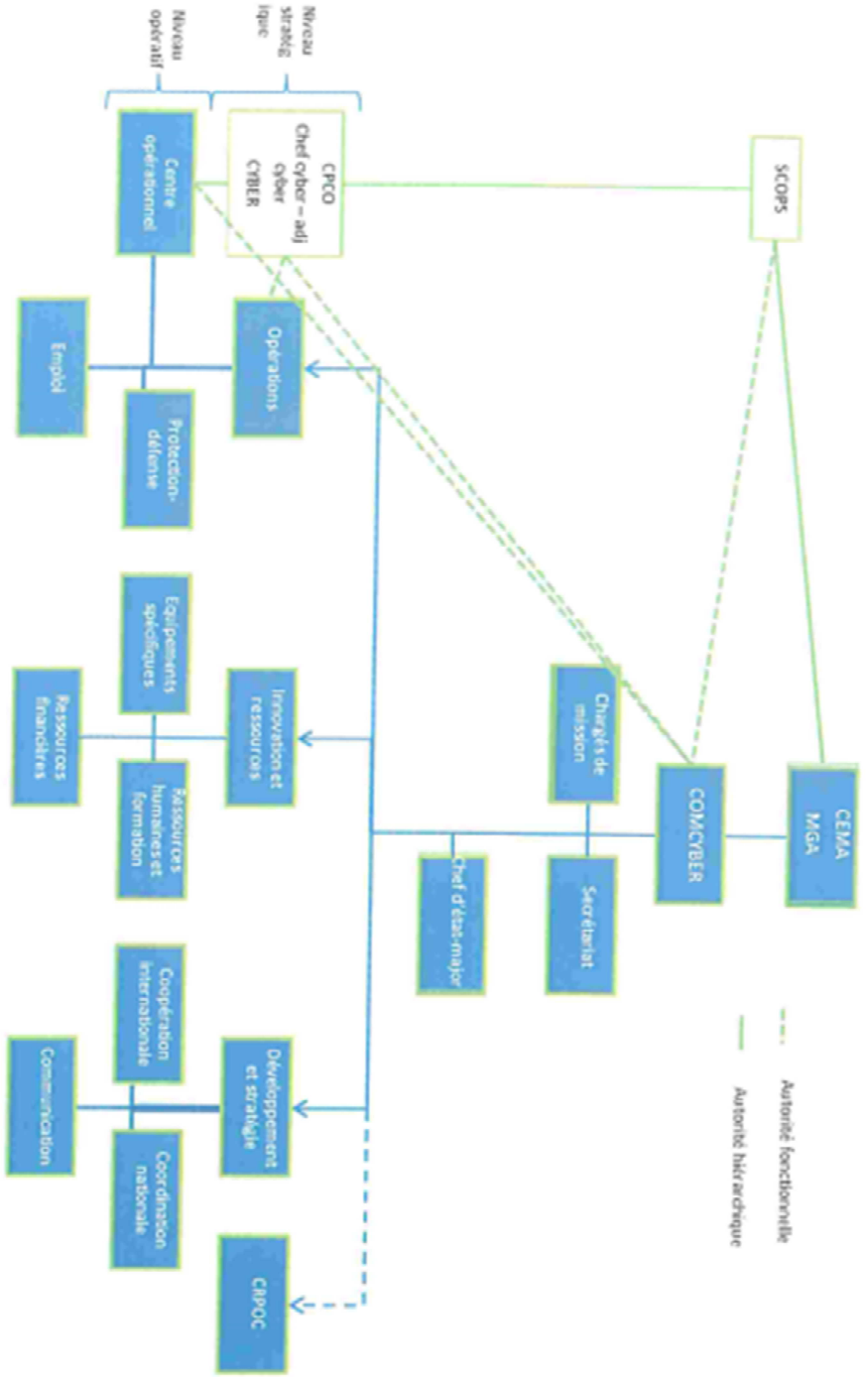
Le service « Communication » de cyberdéfense :

Le service « communication » de cyberdéfense assiste la cellule communication de l'état-major des armées pour :

- la définition d'une politique de communication sur le domaine cyberdéfense où figurent les axes d'effort mais aussi les restrictions et les niveaux de classification afférents ;
- la conduite des actions de communication de cyberdéfense (sensibilisation, prévention,...) et le soutien des armées directions et services ainsi que la réserve citoyenne de cyberdéfense ;
- la gestion de la communication en cas de crise de cyberdéfense.

ANNEXE II à la note n° D 17.000577 /DEF/EMA/CYBER/NP du 19 janvier 2017

ORGANIGRAMME DE L'ETAT-MAJOR DE CYBERDEFENSE, STRUCTURE DE PREFIGURATION DU COMMANDEMENT DE LA CYBERDEFENSE



6/6

Annexe 2 : Organisation de l'armée « Cyber et 5ème dimension » allemande

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

AMBASSADE DE FRANCE
EN ALLEMAGNE

DGRIS
DIRECTION GÉNÉRALE DES
RELATIONS INTERNATIONALES
ET DE LA STRATÉGIE

Mission de défense de Berlin

Dossier suivi par :
Marie Tritsch
marie.tritsch.ext@intradef.gouv.fr

Berlin, le 27 avril 2016
N°305/DEF/MD/BERL/AD/NP

FICHE

OBJET : **Création d'une armée « Cyber et 5ème dimension » au sein de la Bundeswehr.**

RÉFÉRENCE : Annonce officielle de la ministre fédérale de la Défense le 26 avril 2016.

P. JOINTES : a) annexe I : des défis à de nouvelles capacités ;
b) annexe II : la nouvelle organisation Cyber et 5ème dimension.

Synthèse :
La ministre fédérale de la Défense, Mme Ursula von der Leyen, a annoncé le 26 avril la réorganisation de la Bundeswehr pour mieux intégrer les enjeux « Cyber et 5ème dimension » :
- une division CIT (Cyber et SIC) sera créée fin 2016 au sein du ministère BMVg ;
- une armée CIR (Cyber et 5ème dimension) sera créée en 2017 aux côtés de la Heer, Marine, Luftwaffe, Santé et SKB (commandement interarmées des soutiens), regroupant les activités Cyber, SIC et du renseignement militaire.
Avec cette évolution, la Bundeswehr se veut exemplaire et avant-gardiste en Europe, à la veille de la publication de son prochain Weißbuch.

À l'occasion du séminaire sur le domaine cyber qui s'est tenu en septembre 2015 dans le cadre de l'élaboration du Livre blanc 2016, la ministre fédérale de la Défense a annoncé la mise en place du groupe de travail « CIR » (*Cyber- und Informationsraum*), soit « Cyber et 5ème dimension ». Placé sous la responsabilité de la secrétaire d'État à la Défense Katrin Suder, ce groupe de travail co-dirigé par le général Markus Kneip (*Generalinspekteur* adjoint) et par Gundbert Scherf (délégué au pilotage stratégique des activités armement) a été chargé d'élaborer des propositions en vue de réorganiser et fusionner les structures et les compétences de la Bundeswehr dans le domaine de la 5ème dimension.

Mission de défense près l'ambassade de France en Allemagne
Pariser Platz 5 – 10117 Berlin
16 bis avenue Prieur de la Côte d'Or – CS 40300 – 94114 Arcueil Cedex

1. NOUVELLE ORGANISATION DE LA BUNDESWEHR

Ce groupe de travail vient de remettre son rapport à Ursula von der Leyen, qui a annoncé par décision ministérielle du 26 avril 2016 la mise en œuvre des principales propositions de réorganisation au niveau du ministère et des domaines subordonnés. La nouvelle structure sera la suivante :

- **Création au 1er octobre 2016 d'une division « Cyber et SIC » (*Cyber- und informationstechnologie* – CIT) au sein du ministère fédéral de la Défense.**

  D'après la presse, elle pourrait être dirigée par une autorité civile issue du secteur privé : le manager de ThyssenKrupp Klaus-Hardy Mühleck.

  La division CIT, qui siégera à Bonn et Berlin, sera gérée par un *Chief Information Officer* ministériel (CIO-ministériel), responsable des domaines Cyber/SIC, des services SIC et de la sécurité de l'information et de l'entreprise gérant le parc information BWI.

- **Création au 1er avril 2017 d'un nouveau domaine organisationnel militaire « Cyber et 5ème dimension » (CIR), avec à sa tête un *Inspekteur* (chef d'état-major).**

  Ce nouveau commandement, à l'égal des autres armées et services préexistants (*Heer, Marine, Luftwaffe, Streitkräftebasis* et santé), siégera à Bonn et regroupera les domaines d'activité du cyber, des systèmes d'information et de communication, du renseignement militaire, des données géographiques et de la communication opérative. Dans un premier temps, 13 700 postes seront transférés dans ce nouveau commandement (dont 12 800 issus du SKB, soit l'ensemble de la division du renseignement militaire et le centre de communication opérative aujourd'hui intégré dans le commandement des missions territoriales, ainsi que l'ensemble de la division des SIC). S'ajouteront 300 postes notamment pour le commandement et le nouveau centre de cybersécurité de la Bundeswehr.

Le groupe de travail chargé de la mise en place de la nouvelle organisation (CIT et CIR) devrait être placé sous l'autorité du général de division aérienne Ludwig Rüdiger Leinhos, expert SIGINT et en fonction au SKB (*Streitkräftebasis*).

Parallèlement à la mise en place de cette nouvelle organisation, des mesures complémentaires seront prises pour mettre en œuvre les principes stratégiques de cyberdéfense (*Strategische Leitlinien Cyber-Verteidigung*), dans les domaines du personnel, du développement de la « conscience cyber » dans la Bundeswehr et de la coopération interministérielle.

2. PREMIÈRES RÉACTIONS DE PRESSE

Suite à cette annonce diffusée mardi 26 avril dans l'après-midi, la presse a publié ses premières analyses. Pour la *Frankfurter Allgemeine Zeitung*, « Ursula von der Leyen s'arme d'une troupe cyber » qui constitue une sixième composante militaire, aux côtés des trois armées de milieu, du SKB et du service de santé. Cette nouvelle structure devrait être mise progressivement en place d'ici à 2021, avec comme priorité « la défense des infrastructures et des liaisons SIC [de la Bundeswehr] » mais aussi « l'amélioration de la coordination des activités de défense virtuelles au sein du gouvernement fédéral ». Le même journal souligne que « si l'entraînement et la préparation aux attaques cyber n'est pas clairement mentionné dans le catalogue de mission », le développement de capacités techniques cyber entraîne de fait le développement de capacités d'attaque virtuelle.

Pour le *Frankfurter Rundschau*, l'Allemagne était en retard dans ce domaine par rapport à d'autres pays, au premier chef les États-Unis et Israël, et « la ministre de la Défense a décidé de passer à la vitesse supérieure ». Les journaux mentionnent également le soutien à cette initiative affiché par le SPD, partenaire de coalition, qui alerte dans le même temps sur

certains points juridiques à éclaircir, tel que l'exercice du contrôle parlementaire sur ce domaine. Pour le *Tagesspiegel*, « la tête du ministère y voit un faux problème : les opérations dans l'espace virtuel étranger doivent être mandatées comme toute autre opération armée ».

3. OBSERVATIONS

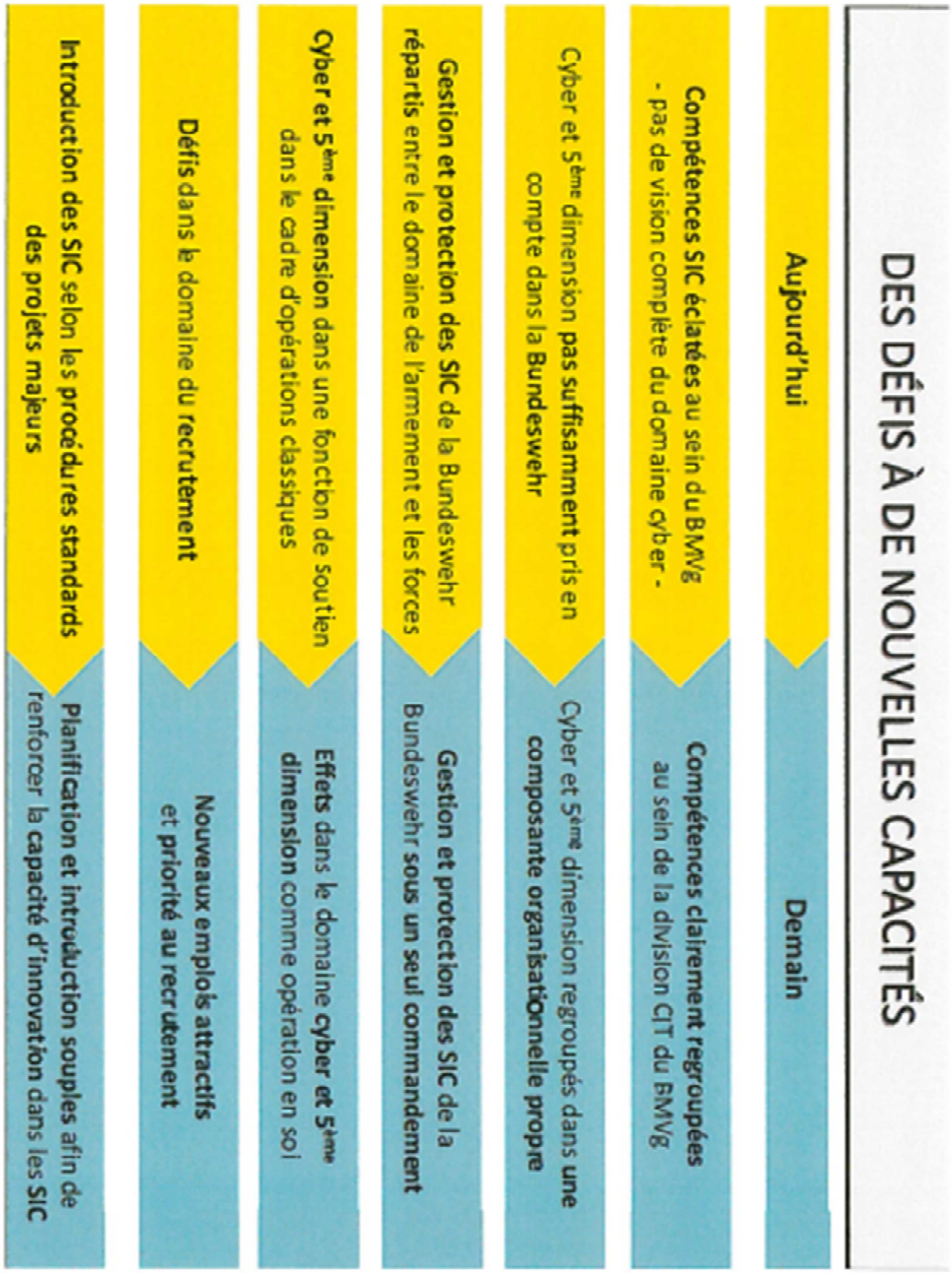
- Les opérations cyber ne relèveront pas de la nouvelle organisation, mais resteront conduites sous la responsabilité de la division ministérielle « Stratégie et opérations ».
- Des interrogations sur le nouveau périmètre du SKB, désormais amputé des divisions renseignement opérationnel et SIC devront être levées.
- La coordination des activités Cyber et la répartition claire des responsabilités sera un véritable défi pour le gouvernement fédéral, notamment parce qu'elle introduit dès le temps de paix des responsabilités nouvelles pour la défense allemande.
- Ce sujet ne manquera pas d'animer les débats politiques au Bundestag, où l'affaire NSA et les cyberattaques contre le Parlement ont suscité de vifs débats. À noter également que la commission de défense du Bundestag a auditionné le 22 février dernier sur « les risques liés au cyberattaques ».
- Avec cette nouvelle organisation, l'Allemagne se veut exemplaire et avant-gardiste en Europe, à la veille de la publication de son prochain Weißbuch.

Le général de brigade Jean-Marc Wasielewski
Attaché de défense

P. O.
Lieutenant-colonel Lipski

ANNEXE I à la note n°305/DEF/ MDD/BERL/AD/NP du 27 avril 2016

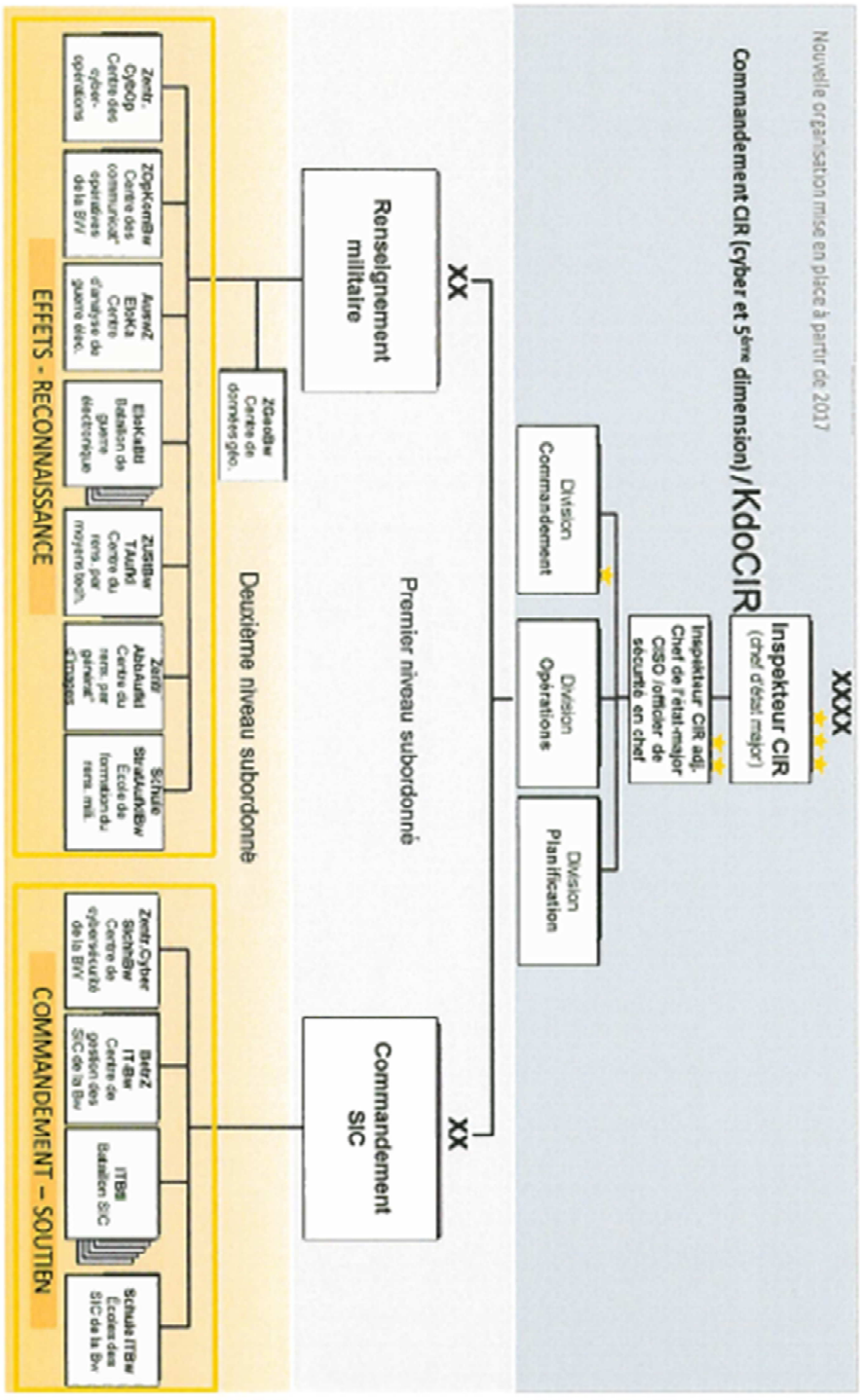
DES DÉFIS À DE NOUVELLES CAPACITÉS



4/7

ANNEXE II à la note n°305/DEF/ MDD/BERL/AD/NP du 27 avril 2016

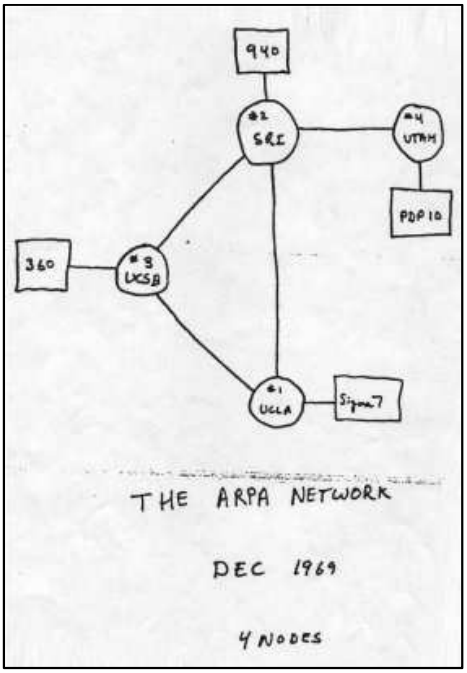
LA NOUVELLE ORGANISATION CYBER ET 5ÈME DIMENSION



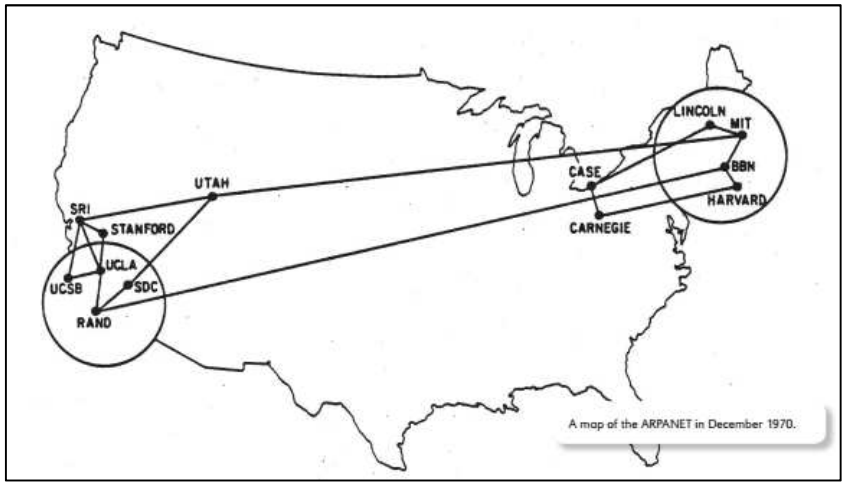
Annexe 3 : Evolution du réseau ARPANET

Schémas tirés de l'article de WALDROP Mitch, *DARPA and the Internet revolution*, publié sur le site de la DARPA et disponible sur le lien : http://www.darpa.mil/attachments/%282O15%29%20Global%20Nav%20-%20About%20Us%20-%20History%20-%20Resources%20-%2050th%20-%20Internet%20%28Approved%29.pdf consulté le 14/01/2017

ARPANET en 1969



ARPANET en 1970



ARPANET en 1977