ÉCOLE DE GUERRE

PROMOTION *GÉNÉRAL GALLOIS*

2016 -2017

Quel rôle pour l'acteur militaire dans le cyberespace ?

Etude de cas comparé France/Etats-Unis

Commandant Frédérick Zimmermann

Sous la direction de :

M^me^ Delphine Deschaux-Dutard

Maître de conférences en science politique à l'Université de Grenoble-Alpes

Contenu

Introduction 4
Qu'est-ce que le cyberespace? 7
Historique et évolution du cyberespace 7
Un espace hybride s'appuyant sur les autres espaces tout en les englobant 7
En constante évolution 9
Aux caractéristiques propres 10
Les acteurs présents 11
Les individus 11
Les groupes 12
Les Etats et institutions supranationales 13
Pourquoi l'acteur militaire doit investir le cyberespace? 15
En dépit des frontières floues, le cyberespace constitue un nouvel espace à défendre 15
Car il représente un enjeu de premier ordre pour les Etats et les citoyens 15
A l'instar des autres milieux, il constitue un espace de conflictualité 16
A l'instar des autres milieux, sa maîtrise constitue un avantage 17
Les menaces existantes 18
Les principaux types d'attaque 18
Les cibles visées 19
Le profil des attaquants 20
Stratégie française et américaine 21
La stratégie française 21
La stratégie américaine 24
Comment l'acteur militaire peut intervenir dans le cyberespace? 25
Organisation française 25
Doctrine militaire 25
Structure 29
Relation avec les partenaires civils, étrangers 30
Organisation américaine 32
Doctrine militaire 32
Structure 33
Relations avec les partenaires civils, étrangers 35
Similitudes et différences majeures 36
Conclusion : 39

Résumé

Le cyberespace, création virtuelle et humaine, résultant des progrès de l'informatique et de l'électronique, occupe une place importante au sein des sociétés humaines. La grande majorité de nos échanges relationnels, scientifiques ou encore financiers, transitent à travers cet espace, et désormais de plus en plus de machines en sont tributaires pour leur bon fonctionnement. L'interconnexion globale des réseaux offre des nouvelles opportunités et s'accompagne de nouvelles formes de risques. De nombreux acteurs sont présents dans cet espace, avec des motivations très variées. Or les caractéristiques propres du cyberespace permettent à ces acteurs d'exprimer leur volonté et d'accomplir leurs desseins en contournant les traditionnelles défenses existantes. Il est donc primordial que les armées dont le rôle est de protéger la Nation et ses intérêts, s'organisent afin de prendre en compte les menaces provenant du cyberespace. La France et les Etats-Unis, pour répondre à ces enjeux, ont développé des stratégies globales et ont confié, selon des modalités particulières, à leur appareil militaire leur défense dans le cyberespace.

Abstract

Cyberspace, virtual and human creation, resulting from advances in computer science and electronics, occupies an important place in human societies. The vast majority of our relational, scientific and financial exchanges pass through this space, and now more and more machines depend on it for their proper functioning. Global network interconnection offers new opportunities and is accompanied by new forms of risk. Numerous actors are present in this space, with very varied motivations. However, the specific characteristics of cyberspace allow these actors to express their will and accomplish their purposes by circumventing traditional defenses. It is therefore essential that the armies whose role is to protect the Nation and its interests are organized in order to take into account threats from cyberspace. To meet these challenges, France and the United States have developed global strategies and have entrusted their defense system to cyberspace in a particular way.

Introduction

Lundi 12 décembre 2016, le ministre de la Défense, Jean-Yves Le Drian, à l'occasion de la visite de la Direction générale de l'armement-Maîtrise de l'information (DGA-MI), déclare que « l'émergence d'un nouveau milieu, d'un champ de bataille cyber, doit nous amener à repenser profondément l'art de la guerre » et ajoute que « le combat numérique est devenu une arme à part entière des armées françaises »[1]. Le ministre, par sa déclaration, entérine une évolution débutée récemment sur la place des armées françaises dans le cyberespace et qui doit aboutir à la création d'un commandement des opérations militaires cyber dès le 1er janvier 2017. A l'instar de la France, les Etats-Unis d'Amérique ont également pensé à la place de leurs armées dans le cyberespace et avait créé dès 2010 le « United States Cyber Command ». Ainsi, ces deux pays, démontrent par ces créations récentes que l'acteur militaire possède un rôle dans le cyberespace. Cela démontre aussi que le cyberespace possède désormais une valeur vitale pour les Etats. Sinon, pourquoi confier la défense de ce nouveau territoire aux forces armées qui constituent le dernier argument des rois.

Le cyberespace, défini dans le livre blanc sur la défense et la sécurité nationale en 2008 (LBDSN 2008), comme le maillage de l'ensemble des réseaux, demeure un espace difficilement mesurable (en 1978, la cartographie des équipements de l'internet tenait sur une feuille A4, de nos jours, cartographier le cyberespace s'avère un exercice périlleux[2]), mêlant machines artificielles et pensées humaines. Assimilé aux moyens d'information et de communication, le cyberespace est comparé, toujours dans le LBDSN 2008, « aux systèmes nerveux de nos sociétés, sans lesquels elles ne peuvent plus fonctionner ». Ce qui était dans un premier temps un simple réseau d'échange d'information entre deux universités, est désormais considéré au même titre qu'un territoire puisqu'il faut le défendre. En effet, le cyberespace constitue le support de nombreuses activités humaines. Si nous considérons comme définition du cyberespace, celle d'Olivier Kempf dans son *Introduction à la Cyberstratégie* : « le cyberespace est l'espace constitué des systèmes d'informatiques de toute sorte connectés en réseaux et permettant la communication technique et sociale

[1]LE DRIAN Jean-Yves, *Discours du ministre de la Défense le lundi 12 décembre 2016 prononcé à l'occasion de la visite de la Direction générale de l'armement-Maîtrise de l'information*, consultable sur le site 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

[2]VENTRE Daniel, *Cyberespace et acteurs du cyberconflit*, Paris, Lavoisier, 2011, p38

d'informations par des utilisateurs individuels et collectifs »[3], nous pouvons saisir l'ampleur de cet espace, qui ne s'arrête pas à des ordinateurs connectés en réseaux. Dans cet espace est échangé de l'information, sous forme de données, qui impacte également le réel. A travers, il est possible, par exemple, d'effectuer des transactions financières ou encore de commander des systèmes asservis à distance. Or, à la vue des enjeux et des opportunités qu'offre ce nouvel espace, il aurait été naïf de penser que la criminalité et que la conflictualité ne puissent également s'exprimer. Les exemples de l'expression de la conflictualité, bien que récents, sont multiples, nous pourrons retenir les attaques informatiques contre l'Estonie en 2007 puis contre la Géorgie en 2008 visant les sites administratifs de ces pays afin de les paralyser[4].

Face à ces épreuves d'un genre nouveau, il apparaît naturel que les Etats s'organisent pour se défendre. Communément, la défense d'un Etat est confiée aux forces armées sous le contrôle de l'autorité civile. Dans le cadre de ce travail, il s'agit d'étudier et d'expliquer de quelle façon s'organise la défense pour répondre à ces formes de menace en prenant les exemples de la France et des Etats-Unis d'Amérique et de relever les spécificités de chacun.

Avec le nombre exponentielle d'attaques commisses chaque jour et leur exposition médiatique, de nombreux ouvrages, blogs, et articles, en français et en langues étrangères, se sont emparés de cette problématique et fournissent d'intéressants et plus qu'utiles éclairages pour la compréhension de cet enjeu. De plus, les Etats communiquent davantage sur leurs intentions dans le cyberespace afin d'une part de rassurer leurs concitoyens et leurs alliés, d'autre part pour mettre en garde, dissuader les éventuels agresseurs. Des Etats, comme les Etats-Unis, la France ou encore des organisations internationales publient stratégies et doctrines dans ce domaine. Les sources pour aborder ce sujet sont donc multiples et se séparent en deux grandes catégories : les documents officiels émanant des Etats et de leurs institutions puis les ouvrages et études académiques publiés par des chercheurs civils et militaires. Si la première catégorie permet de comprendre la politique des Etats dans le cyberespace, la seconde catégorie donne les clés de compréhension du cyberespace, permettant une lecture plus critique de la première. En revanche, comme le cyberespace permet de mener des actions clandestinement, la protection du secret demeure un enjeu capital

[3] KEMPF Olivier, *Introduction à la cyberstratégie,* Paris, Economica, novembre 2012, p25

[4] BONNEMAISON Aymeric et DOSSE Stéphane, *Attention :cyber !Vers le combat numérique,* Paris, Economica, décembre 2013, p62-63.

et limite de fait les connaissances disponibles pour le grand public. Il est donc nécessaire de conserver une certaine réserve face aux écrits relatifs aux opérations menées dans et à travers le cyberespace.

La première partie cet étude est d'abord consacrée à la nature et aux caractéristiques du cyberespace afin de présenter les possibilités (risques, opportunités) offertes par ce milieu. Fort de ces premières constatations, nous étudierons ensuite les raisons qui militent pour une prise en compte par l'acteur militaire de cet espace, ce qui nous amènera à observer les réponses françaises et américaines, l'aspect stratégique. Enfin, nous examinerons comment se décline cet aspect stratégique dans les organisations retenues par ces deux Etats.

Qu'est-ce que le cyberespace?

Historique et évolution du cyberespace

Un espace hybride s'appuyant sur les autres espaces tout en les englobant

Pour pouvoir comprendre les raisons qui nécessitent de s'investir dans le cyberespace, il est nécessaire d'en saisir son histoire, sa géographie, et les ressources qu'il abrite, c'est-à-dire ses représentations.

La mise en garde de Bertrand Boyer dans son second ouvrage relatif à la conflictualité dans le cyberespace résonne tel un avertissement face aux tentatives de simplification hâtive[5]. Le cyberespace n'est donc pas un espace physique tel que les milieux terrestre, maritime, aérien et spatial. On pourrait également penser que la naissance du cyberespace débute avec l'ancêtre d'Internet ou plutôt sa première forme moderne en 1969[6]. Tel que présenté en introduction, les définitions officielles du cyberespace élargissent cet espace bien au-delà de l'Internet, qui en devient l'une de ses parties. Ainsi, le pacte de cyberdéfense du ministère de la défense français le définit de la façon suivante : « le cyberespace est un domaine global constitué du réseau maillé des infrastructures des technologies de l'information, des réseaux de télécommunications, des systèmes informatiques, des processeurs et des mécanismes de contrôle intégrés. Il inclut l'information numérique transportée ainsi que les opérateurs des services en ligne. ». Aux Etats-Unis, d'après le document de doctrine Joint Publication 3.12 de 2013, le cyberespace consiste aussi bien en de nombreux réseaux différents et se chevauchant, qu'en des nœuds sur ces réseaux (tout équipement ou emplacement logique avec une adresse IP, ou autre identifiant analogique), ou encore qu'en des systèmes de données

[5] Le cyberespace, qui regroupe donc l'ensemble des réseaux interconnectés et les infrastructures physiques associées, n'est pas un espace tel que les sciences physiques le comprennent. En effet, la pensée physique s'appuie généralement sur la notion d'espace comme étant le théâtre dans lequel les phénomènes sont observés. De Newton à Einstein, de la physique classique à la relativité générale, cette vision a fondé le socle de notre compréhension de l'univers. L'espace a donc été intimement lié à une conception géométrique, indépendante des événements qui s'y déroulent et de la connaissance que l'on peut en avoir. Tenter de penser le cyberespace comme un espace classique reviendrait donc à reprendre le long cheminement qui a mené les scientifiques à remettre en cause notre vision intuitive de l'espace pour y substituer une approche quantique. BOYER Bertrand*, Cybertactique. Conduire la guerre numérique*, Paris, nuvis, janvier 2014, p27

[6] ARPA first inveted the precursor to the Internet in 1969. Department of Defense, *Department of Defense Cyberstrategy*, Washington, avril 2015, p5
L'ARPA (Advanced Research Projects Agency, renommée DARPA en 1972 pour Defense Advanced Research Projects Agency) est l'agence du département de la Défense des Etats-Unis chargée de la recherche et développement des nouvelles technologies destinées à un usage militaire.

(tels que des tables de routage) qui les appuient[7]. Ces deux définitions soutiennent bien l'idée de globalité du cyberespace ainsi que ses aspects physiques et virtuels. Pour appréhender ces dimensions, de nombreux auteurs et documents officiels décomposent le cyberespace en trois couches : la couche physique, la couche logique et la couche informationnelle aussi qualifiée de sociale[8] :

- La couche physique comprend les matériels nécessaires aux échanges et au traitement de l'information, ce sont non exhaustivement les ordinateurs, les serveurs, les routeurs, les câbles transocéaniques ou encore les satellites de communication[9] ;
- La couche logique comprend les données transitant par les équipements de la couche physique[10] ;
- Enfin la couche informationnelle[11] résulte des interactions entre les équipements et les usagers humains.

A la fois physique et immatériel, le cyberespace est donc présent sous différentes formes : équipements informatiques, données numériques, ondes électromagnétiques ou encore informations et dans tous les autres espaces : terrestre, maritime, aérien et spatial.

[7] Cyberspace consists of many different and often overlapping networks, as well as the nodes (any device or logical location with an Internet protocol address, or other analogous identifier) on those networks, and the system data (such as routing tables) that support them.
Joint Chief of Staff, *Joint Publication 3.12*, Washington, février 2013, p5

[8] Cyberspace can be described in terms of three layers: physical network, logical network, cyber-persona.
Joint Chief of Staff, *ibid*, p5

[9] La couche physique ou matérielle est constituée de tous les ordinateurs et systèmes informatiques, mais aussi de toute l'infrastructure nécessaire à l'interconnexion. Il s'agit des différents câbles et fils de liaison (cuivre ou optique), mais aussi les liaisons par ondes, soit de proximité, sot à distance. Elle inclut les systèmes de routage, les appareils de stockage (et donc ce qu'on nomme les serveurs et les centres de données), les systèmes de transmission (émetteurs et récepteurs électromagnétiques), et tous les relais (satellites). Elle comprend enfin tous les dispositifs de contrôle de chacun de ces éléments et de leur interconnexion.
KEMPF Olivier, *Introduction à la cyberstratégie,* Paris, Economica, novembre 2012, p11

[10] Il s'agit de tous les « programmes » informatiques qui traduisent l'information en données numériques, qui utilisent cette information, et qui la transmettent.
KEMPF Olivier, *ibid,* Paris, Economica, novembre 2012, p12

[11] La couche sémantique [ou informationnelle] du cyberespace intègre la dimension informative : ce qui est dit compte autant que les moyens qui l'expriment ou qui la transportent. Le cyberespace est alors également la résultante de ce qui est prononcé en son sein. Le cyberespace n'est pas seulement le vecteur, le véhicule, il est aussi l'information transportée,
KEMPF Olivier, *ibid*, novembre 2012, p14

En constante évolution

Si de prime abord, le cyberespace semble une création récente, il est possible d'en faire remonter les origines bien avant 1969 avec la création de l'internet.

Dans leur modèle en couches, visant à expliciter la nature du cyberespace, Aymeric Bonnemaison et Stéphane Dossé[12] situent sa création avec les débuts de la vie sur terre et les premiers échanges d'informations entre les êtres vivants. Ils décrivent cette couche comme étant le cybersocle. La couche suivante, le cyberprimaire débute avec l'apparition du langage, « qui permet d'interconnecter les êtres humains, de développer les groupes sociaux, l'économie, la culture, la religion, la politique et aussi la guerre […] Ainsi, les informations sont stockées par les êtres humains qui peuvent les transférer de proche en proche par le langage, dans l'espace et dans le temps, malgré une altération parfois importante des informations »[13]. Le cybersecondaire apparaît avec l'écriture et les mathématiques. Ces deux inventions permettent de stocker l'information dans le temps et de la dupliquer de manière fiable. Ce sont le développement de l'imprimerie puis des enregistrements sur disque et bandes magnétiques avec l'abolition progressive des distances par le développement des techniques de télécommunication (télégraphie optique puis électrique, téléphonie, radiophonie) qui font entrer l'humanité dans le cybertertiaire ou l'interconnexion mondiale des hommes. Les temps de communication sur des longues distances sont drastiquement réduits et font que les grandes régions du monde sont désormais connectées. Enfin le cyberquaternaire, couche de la convergence homme-machine est marqué par le développement de l'électronique, de l'informatique et de l'Internet qui bouleverse durablement et profondément les sociétés humaines. Ce modèle en couches décrit de façon chronologique l'évolution du cyberespace et permet d'en saisir le caractère non seulement technique et technologique mais aussi profondément humain, car plus qu'aucun autre espace ou milieu, ce sont bien les hommes qui font le cyberespace.

L'avènement et le développement de l'intelligence artificielle viendront peut-être démentir cette dernière assertion. Le mouvement d'interconnexion se poursuit avec d'une part l'*IoT* (*Internet of Things*, Internet des objets) qui fait que des objets du quotidien (voitures, équipements électroménagers,…) sont intégrés dans le cyberespace et d'autre part la

[12] BONNEMAISON Aymeric et DOSSE Stéphane, *Attention :cyber !Vers le combat numérique,* Paris, Economica, décembre 2013, p84

[13] BONNEMAISON Aymeric et DOSSE Stéphane, *ibid,* Paris, p85.

numérisation de l'être humain qui porte sur lui de plus en plus de technologie connectée (smartphones, bracelets d'activités, montres connectées,…).

Aux caractéristiques propres

A l'instar des autres milieux, le cyberespace possède ses propres caractéristiques qui influent sur les actions possibles. La connaissance de ces caractéristiques s'avère capitale pour tout acteur souhaitant exploiter le potentiel du cyberespace.

Les auteurs d' « Attention : Cyber ! Vers le combat électronique »[14], en le comparant aux autres espaces tirent les conclusions que le cyberespace « présente des similitudes avec les autres espaces qui permettent de transcrire par analogie des tactiques militaires provenant d'autres espaces ; […] offre des spécificités inédites (terrain, obstacles, ressources naturelles, vitesse de déplacement) qui nécessitent de développer une stratégie de milieu qui lui est propre ». Ils ajoutent que « la transversalité du cyberespace permet d'atteindre tous les autres espaces pour les frapper et réciproquement ». A ces caractéristiques s'ajoutent également l'opacité, qui fait qu'il demeure difficile d'y détecter les attaques et surtout leur origine[15]. Contrairement aux autres espaces, il est difficile d'identifier des frontières telles que nous les concevons. Si les équipements physiques comme les datacenters[16] sont localisés à l'intérieur des territoires, il n'en est pas de même pour l'information qui s'affranchit des distances et des frontières entre les différents pays. De son côté, le Centre de Doctrine d'Emploi des Forces (CDEF) de l'armée de Terre, s'appuyant sur un rapport de Fred Schreir[17], souligne comme caractéristiques que :

- le cyberespace est l'un des global commons, accessible à tous et partout, permettant l'accès à des systèmes vulnérables depuis une infinité de lieux,

- le cyberespace est un espace sans frontières,

---

[14] BONNEMAISON Aymeric et DOSSE Stéphane, *ibid*, p88

[15] BAUD Michel, *Cyberguerre. En quête d'une stratégie*, Focus stratégique n°44, mai 2013, p10

[16] Centre de traitement de données : lieu physique regroupant un ensemble d'ordinateurs et des systèmes de télécommunications afin de stocker, traiter et diffuser des informations. Sa fonction principale est d'assurer une bonne connexion réseau et un haut niveau de disponibilité des ressources. Les datacenters sont, par exemple, un élément essentiel des entreprises de l'Internet au premier rang desquelles figure Google […] BOYER Bertrand, *Cybertactique. Conduire la guerre numérique*, nuvis, janvier 2014, p249

[17] SCHREIR Fred, *The report on Cyberwarfare*, DCAF, 2012, p93-94

- le temps acquiert une nouvelle signification dans ce nouveau champ de combat où des milliers d'attaques cybernétiques peuvent atteindre leur cible simultanément, et recommencer la minute suivante, et ce pendant plusieurs jours ;

- le cyberespace donne l'avantage à l'attaquant, l'origine des attaques est sans limites géographiques, et tandis que la défense doit veiller à combler toutes les brèches de ses systèmes, l'attaquant ne se concentre que sur l'exploitation d'une seule d'entre elles pour arriver à ses fins ;

- l'évolution permanente des techniques et technologies font du cyberespace un milieu en perpétuelle évolution[18].

Ainsi, la difficulté d'attribution associée à un coût d'entrée faible, contrairement aux autres espaces et l'absence de frontière permettent à une multiplicité d'acteurs d'y être présent avec une certaine liberté d'action.

Les acteurs présents

Les individus

Une pluralité d'acteurs se croisent et se côtoient dans le cyberespace, avec des intentions qui sont leurs propres. Classiquement, ils se trouvent répartis dans les trois catégories suivantes : individus, groupes et Etats. L'évocation de ces catégories permet de comprendre quelles sont les spécificités et potentialités de chacune.

Toutefois, cette approche demeure incomplète car les séparations entre les catégories ne sont en rien étanches, des membres d'un groupe criminel peuvent par exemple mettre aux services d'un Etat leurs compétences techniques pour des raisons financières ou idéologiques. Comme l'évoque Daniel Ventre dans *Cyberespace et acteurs du cyberconflit*, « l'hacktiviste[19] est hacker[20], le cyberdélinquant est hacker, la cyberunité de l'armée est constituée de hackers, les

[18] CDEF, *Les forces terrestres et le cyberespace comme nouveau champ de bataille*, cahier du RETEX, mai 2014, p67

[19] Contraction du mot activisme qui désigne un mode d'action, souvent à connotation politique, et du terme hacking constituant une méthode utilisée par les pirates informatiques.
CDEF, *ibid*, cahier du RETEX, mai 2014, p21

[20] Les hackers sont des « pirates informatiques » : passionnés avant tout de technologie, ils étudient les failles des différents systèmes et logiciels pour déjouer les dispositifs de sécurité.
KEMPF Olivier, *Introduction à la cyberstratégie,* Paris, Economica, novembre 2012, p89

espions dans le cyberespace sont nécessairement des hackers, etc. »[21] Dans la catégorie individus se retrouvent donc des profils allant de l'internaute à l'hacktiviste, sachant que l'individu peut revêtir plusieurs attitudes simultanément[22]. Selon leur degré de dépendance et leur connaissance du milieu, ils se servent du cyberespace de façon utile, ludique, politique ou encore criminelle et peuvent constituer un premier niveau de menace. Cependant, comme le sous-entend la citation précédente, ils peuvent constituer un réservoir de compétences. C'est d'ailleurs ce que plusieurs chercheurs dans le domaine de la défense préconisent tel Michel Baud s'appuyant sur l'analyse d'Eric Filiol[23]. Les acteurs individuels dans le cyberespace disposent d'une liberté d'action retrouvée, cela est d'autant plus vrai dans les nations démocratiques. Dans les pays où le contrôle étatique sur le cyberespace en limite les accès, des individus trouvent néanmoins les ressources nécessaires pour contourner la censure technique et idéologique. Pendant les printemps arabes, les coupures des réseaux traditionnels distribuant l'internet par les gouvernements n'ont pas totalement isolé les populations du réseau mondial.

Comme l'écrit Olivier Kempf dans son *Introduction à la Cyberstratégie*, l'individu est dorénavant acteur stratégique car le cyberespace lui offre les moyens techniques de s'opposer à la volonté d'un Etat.

Les groupes

Les groupes ou acteurs collectifs utilisant le cyberespace pour agir sont de nature bien différente.

Il en résulte un usage varié en fonction des intentions de chacun. En premier lieu, ils utilisent les potentialités fédératives[24] du cyberespace et exploitent ses caractéristiques pour atteindre leur but. Se retrouvent dans cette catégorie, les groupes industriels, associatifs ou criminels.

[21]VENTRE Daniel, Cyberespace et acteurs du cyberconflit, Lavoisier, 2011, p103

[22] KEMPF Olivier, *Introduction à la cyberstratégie,* Paris, Economica, novembre 2012, p79

[23] La compétence technique de ceux-ci [les hackers] pourrait être mise au profit de la défense des intérêts cyber de la nation comme le rappelle Eric Filiol : « nous souffrons d'un manque de recherches ouvertes, alors qu'il y a un excellent potentiel en France. Il faut laisser ce potentiel s'exprimer. L'Etat ne peut plus payer de recherches parce que les budgets sont restreints. Il doit donc s'appuyer sur une communauté de hackers vivante et qui assez souvent est là pour aider. L'Etat doit comprendre que cette ressource existe et l'utiliser ». BAUD Michel, *Cyberguerre. En quête d'une stratégie*, Focus stratégique n°44, mai 2013, p34

[24] BOYER Bertrand *Cybertactique. Conduire la guerre numérique*, Bertrand Boyer, nuvis, janvier 2014, p32

Bertrand Boyer, dans son ouvrage *Cybertactique Conduire la guerre numérique*, établit une classification chronologique[25] qui permet d'affiner cette catégorie. Selon lui, ces acteurs collectifs se répartissent en deux ensembles : les acteurs mutants et les acteurs émergents. Les acteurs mutants (sociétés industrielles et commerciales, syndicats, médias, partis politiques, ONG) sont ceux qui voient leur nature évoluer suite au développement du cyberespace, les acteurs émergents (industries des nouvelles technologies de l'information et des télécommunications) sont eux apparus avec le cyberespace. Suivant leur lien avec le cyberespace, ils en sont peu ou complètement dépendants ce qui peut expliquer leurs postures stratégiques. Pour les différencier et apprécier cette posture stratégique, Olivier Kempf[26] avance les critères suivants : la solidité des liens, l'intention, la spécialisation cyber. La solidité des liens entre des membres varient selon les groupes et leur modalité d'appartenance. L'intention caractérise le but commun que partagent les membres. Enfin, la spécialisation cyber renseigne sur le positionnement du groupe vis-à-vis du cyberespace. « Ainsi un groupe aux liens très solides, avec une intention affirmée et une forte spécialisation cyber aura certainement plus de présence cyberstratégique qu'un autre qui demeure très enraciné dans le monde réel, ou qui a des objectifs flous ».

Connaître ces caractéristiques s'avère utile voire indispensable pour adopter son comportement et sa réponse face aux groupes utilisant peu ou fortement le cyberespace. En effet, les menaces pesant contre les Etats ne sont pas uniquement le fait d'autres Etats, mais le sont également de groupes souhaitant s'attaquer à l'autorité de ces derniers.

Les Etats et institutions supranationales

En dépit des travaux initiés par les Etats dans le domaine de l'informatique et des télécommunications notamment lors de la seconde guerre mondiale (création des premiers ordinateurs pour appuyer la cryptologie), il apparait que les Etats n'ont pas saisi dans un premier temps toutes les conséquences de l'évolution du cyberespace indue par les nouvelles

[25]Nous proposons une approche chronologique qui permet de distinguer trois catégories d'acteurs, ceux qui ont toujours eu un rôle dans les études géopolitiques, ceux dont le statut a changé du fait de l'apparition de ce nouveau territoire et enfin ceux qui sont apparus avec le cyberespace.
BOYER Bertrand, *ibid*, nuvis, janvier 2014, p30

[26]KEMPF Olivier, *Introduction à la cyberstratégie,* Paris, Economica, novembre 2012, p92

technologies de l'information et de la communication.[27]. Pour autant, les Etats sont, sous diverses formes, très présents dans le cyberespace.

Depuis l'invention du télégraphe de Chappe, les Etats utilisent les réseaux pour administrer leurs territoires et les citoyens. La maîtrise du cyberespace s'avère donc capitale pour conserver l'autorité nécessaire et constitue un enjeu vital. Il n'est ainsi pas étonnant pour un Etat centralisé comme la France d'observer que le premier opérateur des télécommunications (Orange) est l'émanation d'un service public dépendant directement d'un ministère[28]. L'interconnexion mondiale de l'ensemble des réseaux et l'absence de régulation internationale provoquent une remise en cause de l'autorité des Etats dans le cyberespace. Ce dernier est alors vu par les Etats comme une source de risques et de menaces, d'autant plus qu'il permet de mener des actions plus ou moins anonymement. Les Etats-Unis écrivent qu'à travers cet espace, des acteurs étatiques ou non-étatiques peuvent conduire des attaques sur leurs réseaux d'infrastructures critiques et voler leurs propriétés intellectuelles[29]. Au niveau supérieur aux Etats, les organisations et institutions internationales voire supranationales se saisissent également de cet enjeu, parce qu'elles sont également actrices du cyberespace[30] et qu'elles permettent de mettre en place des mesures de coordination et de contrôle mondiales. Cependant, ces mesures demeurent limitées, chaque Etat ayant son propre agenda et ne dispose des mêmes ressources pour réguler le cyberespace.

La posture des Etats dans le cyberespace possède un caractère stratégique, car il s'agit bien de l'opposition des volontés dans le cadre de la défense de ses propres intérêts.

[27] [Face au cyberespace] l'Etat a subi le choc initial et a perdu l'initiative
BOYER Bertrand, *Cybertactique. Conduire la guerre numérique*, Bertrand Boyer, nuvis, janvier 2014, p31

[28] Il s'agit du ministère des postes et télécommunications, héritier du ministère des postes et télégraphe.

[29] State and non-state actors plan to conduct disruptive and destructive cyberattacks on the networks of our critical infrastructure and steal US intellectual property to undercut our technological and military advantage. Department of Defense, *Department of Defense Cyberstrategy*, Washington, avril 2015, p5

[30] KEMPF Olivier, *Introduction à la cyberstratégie,* Paris, Economica, novembre 2012, p96

Pourquoi l'acteur militaire doit investir le cyberespace?

En dépit des frontières floues, le cyberespace constitue un nouvel espace à défendre

Car il représente un enjeu de premier ordre pour les Etats et les citoyens

Le cyberespace a pris une place importante dans la vie de chaque individu mais également dans l'organisation des sociétés modernes, comme l'illustre un rapport du parlement européen[31].

Chacun possède dorénavant un ou plusieurs systèmes lui permettant d'être connecté quasiment en permanence au cyberespace. Que ce soient les entreprises privées ou les administrations publiques, elles s'organisent toutes autour de systèmes d'information et de communication. De plus, il s'est également créé tout un écosystème entrepreneurial s'appuyant sur les développements du cyberespace, les firmes les plus connues du grand public dans ce domaine sont rassemblées sous l'acronyme GAFA : Google, Apple, Facebook, Amazon auxquelles s'ajoute aussi Microsoft. A l'opposé, des groupes criminels sont également à l'œuvre dans le cyberespace, profitant des opportunités offertes par ce milieu. C'est d'ailleurs pour faire face à cette menace représentée par ces groupes que les premières mesures de sécurité ont été développées[32]. Au fur et à mesure du développement des technologies et de la croissance des interconnexions, les risques se sont accentués et cette situation a provoqué une prise de conscience au niveau des Etats qui ont alors débuté la mise en place de stratégie visant à sécuriser les systèmes informatiques. Nous avons alors assisté dans un premier temps en France à l'implémentation d'une politique de sécurité de système d'information à vocation défensive avec la création en 2002 de la DCSSI[33]. Dans les armées, c'est également cet aspect défensif qui a été d'abord favorisé. Même si d'après Bertrand

[31] Internet est devenu au XXIème siècle un élément central de la vie quotidienne de ses 2,4 milliards d'utilisateurs dans le monde.
Rapport du Parlement européen, *Le droit d'accès à l'Internet*, Strasbourg, mars 2015, p5.

[32] Si les risques soulevés par la « cybercriminalité » sur l'économie avaient déjà été identifiés depuis longtemps, la perception d'un risque pesant plus particulièrement sur la sécurité des Etats est plus récente.
Rapport n°681 d'information fait au nom de la commission des affaires étrangères, de la défense et des forces armées sur la cyberdéfense par M. Jean-Marie Bockel, Sénat, juin 2012, p 11

[33] Direction Centrale de la Sécurité des Systèmes d'Information, précurseur de l'ANSSI, Agence Nationale de la Sécurité des Systèmes d'Information.

Boyer, le cyberespace possède intrinsèquement un caractère conflictuel[34], la prise en compte des enjeux symbolisés par cet espace a été différente selon les armées, à l'instar des exemples américains et français[35].
Dorénavant, la compréhension de ces enjeux fait que les armées modernes se sont emparées de la question cyber et nous voyons le retour d'une réelle stratégie dans ce domaine.

A l'instar des autres milieux, il constitue un espace de conflictualité

S'il peut être vu comme un moyen d'accès à l'information et de partage, le cyberespace est également propice à l'expression des conflits[36]. Et si cet espace reste immatériel, il n'est en pas moins le jeu des souverainetés des Etats.
En effet, bien qu'aucune autorité centrale ne gouverne directement l'internet, les principaux organismes de régulation et de normalisation demeurent localisés aux Etats-Unis[37]. La Chine a décidé de se doter de son propre réseau « Internet » disposant de passerelles avec le réseau Internet mondial, permettant ainsi aux autorités un contrôle plus fin d'une partie de son cyberespace. Une lutte larvée pour le contrôle et l'organisation d'Internet existe donc, chacun souhaitant imposant propre vision du cyberespace. Pour l'acteur militaire, ce nouvel espace de conflictualité offre l'opportunité d'agir sur les autres milieux[38] grâce à des cyberarmes[39].

---

[34]Le développement des autoroutes de l'information repose sur la volonté des pays développés de conserver la domination mondiale. Il s'agit d'un aspect souvent oublié, mais aux conséquences majeurs : internet, les autoroutes de l'information et le cyberespace possèdent, dès l'origine, les germes de conflits.
BOYER Bertrand, *Cybertactique. Conduire la guerre numérique*, nuvis, janvier 2014, p240

[35] Alors que le document de base de l'armée américaine date de 2006 (Joint Publication for Cyberdoctrine JP3-13), il faut en France attendre 2011 pour voir apparaître les premiers documents (Concept interarmées de cyberdéfense du 12 juillet 2011)
BOYER Bertrand, *ibid*, nuvis, janvier 2014, p96

[36] Ainsi, comme pour les espaces physiques, nous observons quotidiennement le jeu du droit et de la puissance, les rivalités autour de la définition des périmètres de souveraineté, les actes hostiles mais également des avancées positives qui répondent à une forme d'auto organisation comparable à des politiques d'aménagement du territoire. Dès lors aucune barrière ne nous interdit de penser une géopolitique du cyberespace.
BOYER Bertrand, *ibid*, nuvis, janvier 2014, p27

[37] […] la centralisation de la gestion des ressources techniques d'Internet par les Etats-Unis suscite une demande de transparence.
Les nouveaux enjeux de la gouvernance d'internet, Regards sur l'actualité n°327, La Documentation française, janvier 2007.

[38] BAUD Michel, *Cyberguerre. En quête d'une stratégie*, Focus stratégique n°44, mai 2013, p19

Quelques exemples récents démontrent l'utilité de l'usage des codes informatiques pour atteindre une cible. Il y a eu *Stuxnet* qui a pour effet de ralentir la production de produits fissibles par l'Iran afin de neutraliser son programme d'armement nucléaire, l'infection du réseau informatique de la Marine nationale par le ver *conficker* qui a obligé les avions de chasse « rafale » à rester au sol.

Ignorer le caractère conflictuel du cyberespace aurait des conséquences majeures sur les capacités militaires. Non seulement, l'acteur militaire serait vulnérable aux attaques lancées à partir de cet espace, mais aussi cet acteur se priverait de nouveaux moyens permettant d'atteindre également des buts de guerre.

A l'instar des autres milieux, sa maîtrise constitue un avantage

La maîtrise du cyberespace est désormais recherchée par les acteurs militaires.

Pour Daniel Ventre, le cyberespace est considéré comme un pivot dans notre monde globalisé dont la maîtrise demeure un enjeu majeur[40]. Au cours du XXème siècle, l'un des nouveaux enjeux des armées était et reste la domination de l'espace aérien. Nous assistons à une situation comparable avec le cyberespace. A travers le cyberespace, il est possible d'atteindre d'autres espaces dans la profondeur stratégique[41]. L'action de la force armée peut également être combinée aux actions dans le cyberespace pour s'attaquer à des objectifs stratégiques : ainsi, en septembre 2007, un raid aérien israélien réussit à détruire une installation nucléaire syrienne en désactivant la couverture radar de l'armée syrienne[42]. Si dans cet exemple, la force a été employée, la maîtrise du cyber peut aussi permettre à un Etat de parvenir à ses fins

---

[39]Une cyberarme pourrait être définie comme un élément logique (un code) servant à mettre le système d'information d'un adversaire, ou tout équipement qui en est doté (système d'arme, infrastructure critique) hors de combat.
BAUD Michel, *Cyberguerre. En quête d'une stratégie*, Michel Baud, Focus stratégique n°44, mai 2013, p13

[40]Le cyberespace peut être considéré comme un espace pivot d'un monde global, par référence au Heartland qui était le pivot de l'île mondiale. La domination du cyberespace, tout au moins sa maîtrise, est un enjeu majeur, au même titre que l'était celle du Heartland. L'enjeu est toujours le même : identifier, localiser, définir un zone, un espace, un territoire dont la domination assure la puissance sur le monde entier.
VENTRE Daniel, *Cyberespace et acteurs du cyberconflit*, Daniel Ventre, Lavoisier, 2011, p103

[41] BAUD Michel, *Cyberguerre. En quête d'une stratégie*, Focus stratégique n°44, mai 2013, p19

[42] HUYGHE François-Bernard, KEMPF Olivier, MAZZUCHI Nicolas, *Gagner les cyberconflits*, economica, septembre 2015, p124

sans avoir recours à la force conventionnelle[43], l'affaire *Stuxnet* précédemment évoquée en est l'illustration. Toutefois et contrairement à ce qui peut se passer dans les autres espaces communs[44], une maîtrise totale du cyberespace semble difficile voire irréalisable. Les obstacles liés à l'attribution des attaques, la persistance de l'effet de surprise et « l'étendue » du cyberespace rendent complexe son contrôle par les institutions étatiques. En revanche, comme le montre l'exemple précédent du raid aérien israélien, il reste possible de s'assurer de la maîtrise d'une partie du cyberespace pendant un intervalle temporel défini. La maîtrise du cyberespace, cette fois-ci au sens technique, s'avère nécessaire évidemment pour l'attaque mais également pour la défense.

Adopter uniquement un concept de défense passif et statique, telle une ligne Maginot numérique, serait nié la nature de la cybermenace, protéiforme et tout azimut. C'est pourquoi, il est préconisé de combiner défense passive et active, qui nécessite une connaissance des acteurs, des menaces et des techniques[45], donc une certaine maîtrise de l'environnement.

Les menaces existantes

Les principaux types d'attaque

C'est à compter de 1994 que la première évocation de menaces sur les systèmes informatiques apparait dans un Livre blanc sur la défense. Les éditions suivantes et, entre temps des rapports parlementaires, développeront davantage ces menaces.

Monsieur le Sénateur Roger Romani décrit ainsi dans son rapport[46] en 2008 les principaux modes de guerre informatique : « la guerre contre l'information, qui s'attaque à l'intégrité de systèmes informatiques pour en perturber ou en interrompre le fonctionnement ; la guerre pour l'information, qui vise à pénétrer les réseaux en vue de récupérer les informations qui y circulent ou y sont stockées ; la guerre par l'information, qui utilise le vecteur informatique

[43] CDEF, *Les forces terrestres et le cyberespace comme nouveau champ de bataille*, cahier du RETEX, mai 2014

[44] L'appareil militaire américain a, aujourd'hui, la maîtrise globale des « espaces communs » : la mer, le ciel, et l'espace. Celle-ci est comparable à la « suprématie navale » chère à Paul Kennedy. Ces « espaces communs » ne relèvent de la souveraineté d'aucun pays et constituent les voies de circulation et d'accès de notre monde. POSEN Barry R, *La maîtrise des espaces, fondement de l'hégémonie des Etats-Unis*, Politique étrangère n°1-2003, p42

[45] RAUFER Xavier (dir.), *La première cyberguerre mondiale*, MA éditions, juin 2015, p37

[46] ROMANI Roger, *Rapport d'information n°449, fait au nom de la commission des Affaires étrangères, de la défense et des forces armées sur la cyberdéfense*, Sénat, 2008

dans un but de propagande, de désinformation ou d'action politique ». Cette simple catégorisation souligne l'éventail de la menace auquel doit faire face le défenseur. Celui-ci ne peut se satisfaire de baser uniquement sa défense sur la sécurisation des systèmes informatiques, il doit être capable de se défendre sur les couches physique, logique et informationnelle. Sous ces trois modes de guerre informatique, nous trouvons des attaques[47] telles que les attaques par déni de service ou déni de service distribué qui visent à saturer les équipements informatiques de l'adversaire ou encore l'insertion de codes malveillants pour espionner ou saboter les réseaux ciblés. De même, l'attaque peut avoir lieu hors ou par le cyberespace. La neutralisation de serveurs ou de relais de télécommunications, peut se faire par bombardement, l'interception d'informations par le vol de support de données.
Les possibilités pour l'adversaire sont donc multiples.

Les cibles visées

Les cibles visées sont elles aussi multiples, il peut s'agir directement des systèmes d'informations opérationnels des armées, des systèmes de supervision et de régulation d'importance plus ou moins vitale, ou encore de personnages publics[48].
En même temps que le cyberespace s'est considérablement élargi, la sécurité générale s'est amoindrie[49]. Les choix pris par la plupart des utilisateurs du cyberespace, dans l'optique de toujours plus partager, plus rapidement des informations depuis n'importe quel lieu, rendent les systèmes informatiques davantage vulnérables. Un échange fluide d'information sur support informatique impose en effet des passerelles d'interconnexion entre les réseaux. Les réseaux n'ayant pas tout le même niveau de sécurité, cela fragilise l'ensemble. Pour autant, le cloisonnement des systèmes s'il réduit les risques d'être attaqué, n'en écarte pas toute possibilité, comme le démontre l'emploi de *Stuxnet*[50]. Si, défendre une frontière géographique

[47] ROMANI Roger, *ibid*, Sénat, 2008, p12

[48] Joint Chiefs of Staff, *The Joint Operating Environment*, Washington, juillet 2016, p34

[49] Un premier comptage concerne soit la prolifération des outils malveillants (les armes du cyber-attaquant) soit l'augmentation des failles exploitables. Ainsi un rapport récent [The Cyber-Crime Black-Market :Uncovered, http://press.pandasecurity.com/press-room/reports/] parmi d'autres, dénombre, en 2010, 60 millions de logiciels ou codes malveillants en circulation, pour seulement 92000 en 2005.
WOLF Philippe, VALLEE Luc, *Cyber-conflits, quelques clés de compréhension*, rapport de l'INHESJ, p787

[50] HUBERT Vanille, *Cyberguerre et nucléaire, le ver informatique Stuxnet*, Centre de doctrine d'emploi des forces, lettre du retex-recherche n°27, janvier 2016

représente déjà un défi pour tout pays, défendre l'intégralité des systèmes informatiques des acteurs principaux d'un pays (institutions régaliennes, fournisseurs de services eau, électricité, …) n'est pas à la portée de toute armée. La protection des cibles les plus sensibles passe donc par une phase d'identification et de sélection et repose d'abord sur les organisations humaines. Bien souvent, les agresseurs se basent sur l'ingénierie sociale[51] pour exploiter les failles potentielles des organismes qu'ils veulent attaquer. L'environnement des cibles doit donc être étudié dans le cadre de leur protection.

Discriminer la nature des cibles potentielles pour le défenseur n'est pas une activité neutre, car cet exercice permet d'établir une priorisation des cibles à défendre et peut fournir une aide à la détermination du niveau de réponse vis-à-vis d'une agression[52].

Le profil des attaquants

Là encore, la diversité règne car la menace voire l'attaque peut émaner d'un individu, d'un groupe de hackers pilotés ou non par une organisation criminelle, un Etat, etc. Même les alliés traditionnels peuvent dans ce milieu, le cyberespace, se comporter en tant qu'adversaire. L'exemple le plus connu nous a été livré par Edward Snowden, révélant le programme d'interception et d'écoute généralisé *Prism* de la National Security Agency (NSA), l'une des agences américaines du renseignement[53]. A la lecture de la littérature contemporaine dans le domaine, il semble toujours difficile de déterminer avec précision l'origine des attaques[54] ; ce qui profite évidemment à l'attaquant et l'encourage à mener des actions offensives. L'absence d'une réelle et surtout efficace coopération internationale ainsi que d'instances et de normes

[51] L'ingénierie sociale (ou social engineering en anglais) est une forme d'acquisition déloyale d'information et d'escroquerie, utilisée en informatique pour obtenir d'autrui, un bien, un service ou des informations clefs. Cette pratique exploite les failles humaines et sociales de la structure cible, à laquelle est lié le système informatique visé. Utilisant ses connaissances, son charisme, l'imposture ou le culot, l'attaquant abuse de la confiance, de l'ignorance ou de la crédulité des personnes possédant ce qu'il tente d'obtenir.
Source :https://fr.wikipedia.org/wiki/Ingénierie_sociale_sécurité_de_l'information

[52] BAUD Michel, *Cyberguerre. En quête d'une stratégie*, Focus stratégique n°44, mai 2013, p14

[53] GREENWALD G, MACASKILL E, *NSA Prism program taps in to user of Apple, Google and others*, The Guardian, 7 juin 2013

[54] L'origine géographique ne peut pas toujours être établie avec certitude et le fait de localiser les ordinateurs d'où sont parties les attaques ne signifie pas que ceux-ci aient été utilisés avec l'accord de leurs propriétaires légitimes ou l'assentiment de l'Etat en question.
APARGIAN Nicolas, *La cybersécurité*, puf, août 2015, p18

de régulation[55] ne peut qu'inciter les attaquants à poursuivre leurs actions dans le cyberespace d'autant plus que les outils pour opérer malicieusement se sont généralisés et sont aisément accessibles. L'autre élément, qui complexifie l'identification de l'attaquant, est la coalescence, définie comme « la réunion d'acteurs disséminés et de nature parfois différente en vue d'une action conjuguée »[56].

Devant cette multiplicité de profils, il devient alors complexe d'établir une frontière rectiligne permettant de distinguer ce qui relève de la cybersécurité et de la cyberdéfense. Pourtant, cette distinction s'avère essentielle pour adapter la riposte aux différents types d'attaque et développer une stratégie prenant en compte le cyberespace.

Stratégie française et américaine

La stratégie française

Le traitement de la question de la sécurité des systèmes d'information n'est pas récent en France[57], en revanche, son appropriation par les plus hautes sphères de l'appareil d'Etat fut plus longue[58]. S'il est fait mention dans le livre blanc sur la défense de 1994 des menaces qui « pèsent sur nos systèmes informatiques (intrusion>comme sur nos installations de production d'énergie ou l'ensemble des réseaux de communication) »[59], la première stratégie de

[55] APARGIAN Nicolas, *ibid*, puf, août 2015, p19

[56] Selon ce principe de coalescence, des acteurs (individus, voir pré-collectivisés mais non institués) s'assemblent, hors de toute structure établie, pour mener des actions groupés. […] Il s'effectue donc des alliances de circonstance qui peuvent se diriger contre tel ou tel objectif, en général une puissance (soit un Etat, une institution, soit une entreprise privée de bonne taille) ce qui permet de se placer temporairement, dans un rapport de force symétrique, le temps de l'attaque.
KEMPF Olivier *(dir.), Stratégies dans le cyberespace*, L'esprit du Livre, septembre 2011, p184

[57] Si le débat a eu du mal à être formalisé, on ne peut négliger la présence française sur les questions de cyberdéfense dès l'origine du concept. […] Dès1997, Jean Guisnel propose une étude de l'impact d'internet sur les questions de renseignement...[...] La sécurité des systèmes d'information devient progressivement "cybersécurité" et l'on observe entre 2009 et 2011 une véritable inflation de "cyber".
BOYER Bertrand, *Cybertactique. Conduire la guerre numérique*, nuvis, janvier 2014, p99

[58] Alors que les documents de base de l'armée américaine date de 2006 (Joint Publication for Cyberdoctrine JP 3-13), il faut en France attendre 2011 pour voir apparaître les premiers documents (Concept interarmées de cyberdéfense du 12 juillet 2011). Ce retard relatif est en partie explicable par les hésitations à assumer l'usage du terme "offensif".
BOYER Bertrand, *ibid*, p99

[59] *Livre blanc sur la défense 1994*, p23

cybersécurité française date de 2011[60] à l'instar du premier concept interarmées de cyberdéfense. Le dernier document fixant au plus niveau la stratégie de la France dans le cyberespace a été rendu publique en octobre 2015. Intitulé stratégie nationale pour la sécurité du numérique, il a été approuvé par le premier ministre, responsable de la défense nationale selon la Constitution de la 5ème république. Cette stratégie se veut globale, elle s'adresse donc à l'ensemble des acteurs du numérique (ministères, administrations, collectivités territoriales, entreprises et citoyens) et précise la position de l'Etat sur la scène internationale. Faisant le constat amer de la dangerosité de la menace et des nombreux défis posés par de nouveaux acteurs tels les géants de l'internet (alphabet/google, amazon,…), elle fixe à l'Etat cinq objectifs stratégiques[61] :

- garantir la liberté d'expression et d'action de la France et assurer la sécurité de ses infrastructures critiques en cas d'attaque informatique majeure ;

- protéger la vie numérique des citoyens et des entreprises et lutter contre la cybercriminalité;

- assurer la sensibilisation et la formation nécessaire à la sécurité du numérique ;

- favoriser le développement d'un écosystème favorable à la confiance dans le numérique ;

- promouvoir la coopération entre Etats-membres de l'Union dans un sens favorable à l'émergence d'une autonomie stratégique numérique européenne, garante sur le long terme d'un cyberespace plus sûr et respectueux de nos valeurs.

Avec cette stratégie, l'Etat français cherche avant tout à conserver son autonomie d'appréciation et de décision dans le cyberespace comme il l'a fait dans le domaine du renseignement après la 1ère guerre du Golfe en 1991[62]. C'était, d'ailleurs, déjà, l'un des quatre objectifs de la stratégie sur la défense et la sécurité des systèmes d'information[63] publiée en

[60] Secrétariat général de la défense et de la sécurité nationale*, Stratégie nationale pour la sécurité du numérique*, octobre 2015, p7

[61] Secrétariat général de la défense et de la sécurité nationale, *ibid,* octobre 2015, p9

[62] *Livre blanc sur la défense 1994*, p87

[63] La stratégie sur la défense et la sécurité des systèmes d'information repose sur quatre objectifs :
-faire de la France une puissance mondiale de cyberdéfense tout en conservant son autonomie ;
-garantir sa liberté de décision par la protection de l'information de souveraineté ;

2011 par l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information). La lecture des livres blancs sur la défense et la sécurité nationale de 2008 et 2013 met en exergue la prise en compte des nouvelles menaces issues du cyberespace et l'évolution de la posture française dans l'intervalle. Auparavant principalement axée sur la défensive[64], le dernier changement majeur de la stratégie française réside sur la reconnaissance de la lutte informatique offensive comme réponse possible à une cyberattaque[65]. Les attaques dans le cyberespace pouvant prendre des formes différentes avec des atteintes plus ou moins sérieuses, la stratégie nationale « repose sur le principe d'une approche globale fondée sur […] une capacité de réponse gouvernementale globale et ajustée face à des agressions de nature et d'une ampleur variées faisant en premier lieu appel à l'ensemble des moyens diplomatiques, juridiques ou policiers, sans s'interdire l'emploi gradué de moyens relevant du ministère de la Défense, si les intérêts stratégiques nationaux étaient menacés »[66]. En déclarant sa volonté et en présentant ses capacités, l'Etat français adopte une attitude dissuasive, qui ne serait cependant s'entendre au sens classique de la dissuasion nucléaire[67].

Accusant un certain retard dans la prise en compte des enjeux de souveraineté dans le cyberespace[68], la France souhaite rester une référence et exprimer sa puissance dans le domaine.

-renforcer la cybersécurité des infrastructures vitales nationales ;
-assurer la sécurité dans le cyberespace.
Agence nationale de la Sécurité des Système d'Information, *Stratégie sur la défense et la sécurité des systèmes d'information*, février 2011

[64] Comme l'indique son titre, Défense et sécurité des systèmes d'information, la stratégie de la France ne se concentre officiellement que sur le volet défensif : « le gouvernement a décidé de renforcer significativement les capacités nationales en matière de cyberdéfense ».
BAUD Michel, *Cyberguerre. En quête d'une stratégie*, Focus stratégique n°44, mai 2013, p24

[65] La France a récemment présenté une position décomplexée vis-à-vis de la lutte informatique offensive à l'occasion de la publication du livre blanc 2013, dans lequel elle affirme que « la capacité informatique offensive enrichit la palette des options possibles à la disposition de l'Etat ».
CDEF, *cahier du RETEX*, mai 2014, p214

[66] *Livre blanc sur la sécurité et la défense nationale 2013*

[67] Les ambiguïtés de la cyberdissuasion constratent durement avec la clarté de la dissuasion nucléaire.
LIBICKI Martin, *Cyberdeterrence and cyberwar*, Rand Corporation, 2009, p16

[68] Le livre blanc de 2008 sur la défense et la sécurité nationale a permis une réelle prise en compte des faiblesses de la France dans ce domaine, faiblesses qui ont été mises en exergue dans le rapport Romani de 2008 qui estime que la « France n'est ni bien préparée, ni bien organisée » pour faire face aux cybermenaces».
BAUD Michel, *Cyberguerre. En quête d'une stratégie*, Focus stratégique n°44, mai 2013, p29

La stratégie américaine

Les Etats-Unis occupent une place particulière dans le cyberespace, ils en sont les principaux architectes. A ce titre, ils en possèdent une maîtrise décisive et ont très tôt développé une stratégie dans ce domaine et ont massivement investi pour le développement d'une capacité cyber militaire.

Dans les différents documents émis par la défense américaine ou encore la présidence, nous retrouvons une caractérisation de la menace cyber commune, faisant le constat de la faiblesse des Etats-Unis face aux cyberattaques, qui elles s'amplifient et s'améliorent, faiblesse d'autant plus saillante que la pénétration du numérique dans la société américaine concerne tous les secteurs d'activité[69]. La finalité de la stratégie américaine demeure la domination du cyberespace, qui leur permettra de conserver un avantage technologique, économique et militaire sur les autres nations[70]. En juillet 2011, est ainsi publiée par la Maison blanche une stratégie pour opérer dans le cyberespace[71] dans laquelle est précisée que « le département de défense doit s'assurer d'avoir les capacités nécessaires pour opérer efficacement dans tous les domaines Air, Terre, Mer, Espace et Cyberespace ». Dans cette stratégie, le département de la défense n'est pas le seul intervenant, et les Etats-Unis comptent sur la mobilisation de tous les acteurs majeurs du cyberespace pour assurer leur sécurité. A ce titre, les géants de l'Internet, dont la plupart sont des entreprises américaines collaborent avec les services de renseignement américains[72]. C'est la directive présidentielle PPD 20[73] qui définit les périmètres et missions de chaque acteur. Dans cette directive sont distinguées la défense des réseaux (*network defense*) et opérations offensives et défensives dans le cyberespace (*offensive and defensive cyberspace operations*). Concernant la défense des réseaux, chaque département (département de la défense, département d'état) en est responsable. Quant aux

[69] Department of Defense, *The Department of Defense Cyber Strategy*, Washington, avril 2015, p1

[70] C'est l'un des axes clés de la stratégie américaine dans le cyberespace : les Etats-Unis ont été à l'origine du développement d'Internet, ils doivent non seulement maintenir mais accentuer le fossé technologique avec leurs adversaires en imaginant et en construisant les réseaux de demain.
BONNEMAISON Aymeric, DOSSE Stéphane, *Attention : Cyber ! Vers le combat cyber-électronique*, Economica, décembre 2013, p137

[71] President of the United States of America, *Strategy for operating in Cyberspace*, Washington, juillet 2011

[72] ERHEL Corinne, de la RAUDIERE Laure, *Rapport d'information sur le développement de l'économie numérique*, Assemblée nationale, mai 2014, p104

[73] VENTRE Daniel, Cyber Operations in DOD Policy and Plans : Issues for Congress. Congressional Research Service report. Note de lecture, janvier 2015

opérations offensives, le cadre en est défini par un « Executive order » émanant du département de la défense. La PPD 20 précise enfin que la réponse à une cyberattaque terroriste ou un acte de cyberguerre ne peut être autorisée que par le président. La publication récente d'un document intitulé "*Joint Operating Environment 2035. The Joint Force in a Contested and Disordered World*"[74] nous offre un aperçu de la stratégie que les Etats-Unis poursuivent dans le domaine cyber. Il s'agira pour les Etats-Unis de défendre leur cyberespace souverain et de protéger l'utilisation du cyberespace non-souverain. A l'instar des conflits pour la reconnaissance d'un territoire ou d'une souveraineté par le passé, le cyberespace fera également l'objet de dispute du même ordre.

Le cyberespace occupe donc une place primordiale dans la stratégie américaine, sa maîtrise constitue un enjeu majeur au même titre que la maîtrise des autres espaces.

Comment l'acteur militaire peut intervenir dans le cyberespace?

Organisation française

Doctrine militaire

En 2010, l'Association Nationale des Auditeurs Jeunes de l'Institut des Hautes Etudes de Défense Nationale (ANAJ-IHEDN) publie, dans un rapport intitulé « Prospectives des doctrines françaises en matière de cyberdéfense »[75], que la doctrine française est à l'époque embryonnaire et s'appuie sur plusieurs textes dont le livre blanc sur la défense et la sécurité nationale de 2008 (LBDSN 2008). Dans ce document cadre figure la nécessité de se doter, pour la défense nationale d'une défense en profondeur, d'une protection intrinsèque des systèmes, d'une surveillance permanente et d'une capacité de réaction rapide et d'action offensive. Faisant écho à ce livre blanc, la loi de programmation militaire 2009-928 du 29 juillet 2009 prévoit que « la défense informatique combinera protection des systèmes, surveillance, réaction rapide et action offensive de rétorsion ». Toutefois, il est encore délicat de parler d'une réelle capacité de lutte informatique offensive à cette date, en effet bien que mentionnée dans le projet de loi de programmation 2003-2008, cette capacité n'est toujours

[74] Department of Defense, *Joint Operating Environment 2035. The Joint Force in a Contested and Disordered World*, juillet 2016

[75] *Prospectives des doctrines françaises en matière de cyberdéfense*, ANAJ-IHEDN, 2010

pas développée[76]. Même si elle n'existe pas, son cadre d'emploi est déjà précisé dans le livre blanc : respect du principe de riposte proportionnelle et atteinte en priorité des moyens opérationnels de l'adversaire. D'après le rapport du sénateur Jean-Marie Bockel[77], dans les années 2010-2011, le ministère de la Défense s'est réorganisé afin de s'adapter à une stratégie de cyberdéfense en profondeur, précédemment évoqué dans le LBDSN 2008. Aussi, cette nouvelle organisation, décrite dans une instruction ministérielle de janvier 2012 fait la distinction entre la protection et la défense des systèmes d'information, la protection pouvant s'entendre comme la planification des actions à moyen et long terme et la défense comme la réaction en temps réel. Enfin ce même rapport indique que « le ministère de la défense et les armées se sont dotés d'un concept et d'une doctrine interarmées de cyberdéfense, documents adoptés respectivement en juillet 2011 et en janvier 2012 », documents non rendus publics, et conclut que « le ministère de la défense a su adapter son organisation en matière de sécurité et de défense des systèmes d'information, de manière à ce que cette dimension soit pleinement prise en compte dans la chaîne opérationnelle ». Cette conclusion partielle signifiant dès lors que le domaine cyber est désormais pris en compte dans la conception, la planification et l'exécution des opérations militaires et donc non seulement comme un ensemble de mesures de sécurité techniques et organisationnelles. Cela marque en France une étape majeure dans la montée en puissance des armées dans le cyberespace.

La position des forces armées et du ministère de la défense français a fait l'objet d'une réactualisation lors de la divulgation du pacte cyberdéfense[78] par le ministre de la défense le 7 février 2014. Ce pacte a présenté le plan de montée en puissance de la filière cyber au sein des armées françaises et du monde de la défense. Il comprend cinquante mesures reparties en six axes de développement:

- Axe 1 : durcir le niveau de sécurité des systèmes d'information et les moyens de défense et d'intervention du ministère et des grands partenaires de confiance ;

- Axe 2 : préparer l'avenir en intensifiant l'effort de recherche tant technique et académique qu'opérationnel, tout en soutenant la base industrielle ;

- Axe 3 : renforcer les ressources humaines dédiées à la cyberdéfense et construire les parcours professionnels associés ;

[76] Projet de loi de programmation militaire 2009-2014

[77] *Rapport n°681d'information fait au nom de la commission des affaires étrangères, de la défense et des forces armées sur la cyberdéfense par M. Jean-Marie Bockel*, Sénat, juin 2012

[78] Ministère de la défense, *Pacte cyberdéfense*, février 2014

- Axe 4 : développer le pôle d'excellence en cyberdéfense en Bretagne au profit du ministère de la défense et de la communauté nationale de cyberdéfense ;

- Axe 5 : cultiver un réseau de partenaires étrangers, tant en Europe qu'au sein de l'OTAN et dans les zones d'intérêt stratégique ;

- Axe 6 : favoriser l'émergence d'une communauté nationale de cyberdéfense en s'appuyant sur un cercle de partenaires et les réseaux de la réserve.

Ce pacte exprime une vision globale vis-à-vis des enjeux liés à la question cyber et vise pour la France à conserver voire reprendre son rang dans le domaine. Il vise à renforcer l'écosystème cyberdéfense national dans les sphères académiques, professionnels civils et militaires.

Suivant la présentation de ce pacte, le dernier jalon majeur dans le développement de la doctrine française est le discours du ministre de la défense, Jean-Yves Le Drian, du 12 décembre 2016, prononcé à Bruz lors de sa visite de la Direction générale de l'armement-Maîtrise de l'information[79]. Dans son discours, le ministre, avant d'évoquer la nécessité d'une doctrine française, revient rapidement sur le concept de dissuasion en écartant d'emblée toutes similitudes entre dissuasion cyber et dissuasion nucléaire. D'après lui, il ne peut y avoir de dissuasion conventionnelle ni cyber « estimant que jamais un armement classique n'exercerait l'effet radical de dissuasion propre au nucléaire ». Cette distinction avec d'autres conceptions partagées par des partenaires de la France faite, le ministre justifie le développement d'une doctrine et d'une stratégie cyber de défense car dorénavant pour dominer un adversaire, il faut également rechercher et obtenir la supériorité dans l'espace cyber. De par le caractère transverse de cet espace, cette doctrine dépasse le seul cadre ministériel et doit s'inscrire dans une stratégie d'ensemble à définir au plus haut niveau. Elle repose sur quatre axes : l'axe des missions, l'axe juridique, l'axe de la coopération internationale, et l'axe des moyens. Reprenant les trois types de catégories des missions conventionnelles de l'appareil de défense, la fonction cyberdéfense se voit confier au même titre les missions de renseignement, les missions de protection/défense et les missions de riposte et neutralisation. Le renseignement dans le domaine cyber a pour objectifs d'identifier les failles, de détecter les actions hostiles, d'attribuer les attaques, de contribuer à préparer, planifier et soutenir les actions offensives. De même que l'arme cyber participe à l'élaboration du renseignement global, le renseignement d'origine humaine conserve toute sa

[79] LE DRIAN Jean-Yves, *Discours du ministre de la Défense le lundi 12 décembre 2016 prononcé à l'occasion de la visite de la Direction générale de l'armement-Maîtrise de l'information*, consultable sur le site 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

pertinence et peut fournir des informations clés pour la conduite d'opérations cyber. Au chapitre de la mission de protection/défense, le périmètre de cette mission s'étend à l'ensemble des systèmes du ministère de la Défense tant sur le territoire national que déployés sur les théâtres d'opérations extérieures et en coordination avec l'ANSSI aux opérateurs d'infrastructures vitales. La protection des systèmes du ministère doit même pouvoir disposer d'outils de protection immédiate éventuellement automatisés. Pour la dernière mission, de riposte et neutralisation, il s'agit de pouvoir offrir au président de la République un large éventail de réponses possibles, cyber ou non, en cas d'attaque caractérisé. Afin de pouvoir remplir cette mission, les capacités cyber doivent permettre de s'introduire dans les systèmes adverses pour y causer des dommages, des interruptions de service ou des neutralisations temporaires ou définitives. Sur l'axe juridique, le ministre souligne que la responsabilité des Etats laissant transiter des actes internationalement illicites pourrait être engagée et faire l'objet de contre-mesures et s'appuie pour se justifier sur l'interprétation que le droit international s'applique également au domaine cyber. « Ainsi, une attaque informatique majeure, eu égard aux dommages qu'elle causerait, pourrait constituer une agression armée au sens de l'article 51 de la charte des Nations Unies et justifier ainsi l'évocation de la légitime défense. » Cette règle s'appliquerait d'ailleurs que l'agression soit le fait d'un Etat ou d'un groupe, sans précision cependant sur la nature de ce groupe. La coopération, le troisième axe, a pour but de faire progresser l'ensemble des partenaires et alliés à travers le renforcement de leurs capacités, les échanges d'information et la coordination spécifique lors d'actions en coalition. Enfin, le dernier axe, celui des moyens, insiste sur les investissements financiers, matériels et humains consentis pour mettre à niveau la cyberdéfense militaire et civile du ministère. Au terme de la loi de programmation militaire 2014-2019, ce sont environ 3200 personnes qui participeront à la mission cyber soit plus du double par rapport à 2012. A cet effectif se rajoute celui des réserves, qui ont fait l'objet d'un recrutement assez ciblé vers les experts du domaine en entreprise et les étudiants d'école d'ingénieurs, constituant la réserve de cyberdéfense. Pour soutenir cette montée en puissance, l'investissement financier consenti sur la période 2014-2019 devrait atteindre un milliard d'euros. L'une des annonces clés de ce discours est la création d'un nouveau commandement au sein des armées : la création du commandement CYBER, le CYBERCOM. Le rôle de ce commandement sera de mener les opérations militaires dans l'espace numérique. Cette création marque une étape importante dans l'évolution de la doctrine militaire française, qui voit le « CYBER » gagner en autonomie par rapport aux autres armées et services. L'année 2017 verra donc, au sein du

ministère de la défense et des armées, une réorganisation complète de la chaîne CYBER actuelle.

Structure

Domaine transverse par excellence, le cyberespace a d'abord été considéré dans les armées françaises comme une fonction opérationnelle venant appuyer les opérations. Dorénavant, il lui est concédé une certaine part d'autonomie avec la reconnaissance que des opérations militaires peuvent se dérouler intégralement dans le cyberespace en autonomie. Pour prendre en compte cette évolution de la doctrine, il a fallu adapter les organisations et les chaînes de commandement. La structure mise en place vise à permettre le bon fonctionnement de la cyberdéfense militaire tel que défini par le pacte de cyberdéfense[80]. Sous les ordres du chef d'état-major des armées, un officier général CYBER est placé à la tête d'une chaîne de commandement opérationnel dédié à la cyberdéfense. Responsable de la défense des systèmes d'information pour l'ensemble du ministère, cet officier général coordonne et assure la conduite des opérations de lutte informatique défensive. Désormais avec la création, en janvier 2017 du CYBERCOM[81], ce même officier général, l'OG CYBER, devient le commandeur des opérations militaires dans l'espace numérique. En pleine montée en puissance, le commandement CYBER sera composé, à court terme, d'un véritable état-major et aura autorité sur toutes les unités opérationnelles spécialisées dans la cyberdéfense du ministère, appartenant à toutes les armées, directions et services. Quatre pôles le structurent :

- un pôle protection qui reposera sur les personnels de la DIRISI (Direction Interarmées des Réseaux d'Infrastructure et des Systèmes d'Information) en charge de la sécurisation des réseaux ;

[80] La cyberdéfense militaire regroupe l'ensemble des actions défensives ou offensives conduites dans le cyberespace pour garantir le bon fonctionnement du ministère de la Défense et l'efficacité de l'action des forces armées en préparation ou dans la planification et la conduite des opérations.
Ministère de la défense, *Pacte cyberdéfense*, février 2014, p4

[81] LE DRIAN Jean-Yves, *Discours du ministre de la Défense le lundi 12 décembre 2016 prononcé à l'occasion de la visite de la Direction générale de l'armement-Maîtrise de l'information*, consultable sur le site 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

- un pôle défensif intégrant le CALID (Centre d'Analyse en Lutte Informatique Défensive) qui assure une capacité permanente de détection, d'analyse et de réponse aux cyberattaques ;

- un pôle « d'action numérique » couvrant les missions offensives ou de renseignement. A terme des unités de « combat informatique » devraient être créées pour remplir les missions offensives ;

- un pôle chargé de la réserve.

Nous assistons en quelque sorte à l'avènement d'une nouvelle composante d'armée, cependant elle reste toutefois fortement liée aux autres armées. Cela s'explique en partie par sa relative jeunesse et les moyens disponibles tant humains que financiers. Son développement n'en est qu'à ses balbutiements et les engagements futurs valideront ou non la pertinence de ce modèle.

Relation avec les partenaires civils, étrangers

Le ministère de la Défense n'est pas le seul acteur majeur du cyberespace en France. Depuis la modification du code de la Défense en 2013, c'est le premier ministre qui conduit la politique de cybersécurité et définit les règles pour le contrôle de la sécurité des systèmes d'information. De plus, inclus dans le décret de création de l'ANSSI en 2011[82], le comité stratégique de la sécurité des systèmes d'information coordonne et fait appliquer les mesures concernant la sécurité des systèmes d'information. Ce comité interministériel sous la supervision du SGDSN comprend le chef d'état-major des armées, le secrétaire général du ministère de l'intérieur, le secrétaire général du ministère des affaires étrangères, le directeur de la DGA, le directeur de la Direction Générale de la Sécurité Extérieure (DGSE), celui de la Direction Générale des Systèmes d'Information et de Communication (DGSIC), celui de la Direction Interministérielle des Systèmes d'Information et de Communication de l'Etat, celui pour la Direction Interministérielle pour la Modernisation de l'Action Publique, de la Direction Générale de la Sécurité Intérieure (DGSI) et le directeur de l'ANSSI. Cette longue énumération a le mérite de mettre en perspectives la prise en compte globale de la cybersécurité par l'Etat français. Si le SGDSN est responsable d'assister le premier ministre

[82] *Décret n°2009-834 du 7 juillet 2009 portant création d'un service à compétence nationale dénommé « Agence nationale de la sécurité des systèmes d'information »*

dans la définition de la politique de cybersécurité ; l'ANSSI, agence subordonnée au SGDSN, coordonne entre tous les acteurs interministériels et privés l'effort national de cybersécurité. Cette agence clé veille notamment à la sécurité informatique des infrastructures vitales de l'Etat à travers le Centre Opérationnel de la Sécurité des Systèmes d'Information (COSSI). A ce niveau existe également une passerelle d'échange avec le ministère de la Défense, en effet le COSSI est co-localisé avec le CALID pour améliorer le partage d'information et la coordination face aux menaces et attaques.

Le secteur public n'est pas le seul partenaire de la défense dans le cyberespace puisque des entreprises privées, qu'elles soient françaises ou étrangères, sont connectées avec les armées françaises à différent titre. Les fournisseurs d'équipement informatique en font évidemment partie et dorénavant quasiment tous les fabricants de systèmes d'armes. Ensuite, il existe un tissu de petites et moyennes entreprises développant des compétences dans la sécurité informatique. C'est ce tissu que compte d'ailleurs développer le ministre de la défense à travers son pacte cyberdéfense[83] pour d'une part, permettre à la France de conserver une certaine indépendance dans le domaine et d'autre part, participer au vivier de la réserve cyber.

Comme évoqué précédemment, la coopération internationale occupe une place importante dans la stratégie de cyberdéfense française. Cette coopération est développée à plusieurs niveaux, soit dans le cadre d'accords bilatéraux avec d'autres pays. Ce cadre semble être techniquement le plus fructueux car deux pays seront plus à même d'échanger de l'information que dans un cadre multilatéral[84]. Ensuite la France faisant partie de l'Union européenne et l'Organisation du Traité de l'Atlantique Nord, elle participe naturellement à l'élaboration des politiques de cybersécurité et cyberdéfense de ces organisations et en retour est influencé par les autres membres. Ainsi depuis 2013, la France fait partie des nations sponsors du Centre d'excellence pour la cyberdéfense de l'OTAN à Tallin en Estonie[85].

A l'instar du caractère transverse du cyberespace, la cyberdéfense ne peut être assuré seule par les forces armées françaises. En France, il existe donc un partage de compétences entre les

[83] Le pôle d'excellence cyber, implanté en Bretagne avec une portée nationale et un objectif de rayonnement international, se structure autour de deux composantes. La première est consacrée à la formation initiale, la formation continue et l'enseignement supérieur. La seconde concerne la recherche, garante d'un enseignement supérieur de qualité, et le développement d'un tissu industriel, avec une attention particulière portée aux PME/ETI innovantes.
Ministère de la défense, *Pacte cyberdéfense*, février 2014, p7

[84] Les évolutions de la cybersécurité : contraintes, facteurs, variables, Daniel Ventre, Direction Générale des Relations Internationales et de la Stratégie, juin 2015

[85] RAUFER Xavier (dir.), *La première cyberguerre mondiale*, MA éditions, juin 2015, p45

différentes entités publiques. Le secteur privé a également son rôle à jouer encadré par les autorités civiles.

Organisation américaine

Doctrine militaire

Pionnier dans le cyberespace, les Etats-Unis publient dès 2006 leur première stratégie militaire des opérations dans le cyberespace, *the National Military Strategy for Cyberspace Operations*[86]. Dans ce document, il est mis en avant le rôle des forces armées dans la protection des intérêts américains par la conduite d'opérations militaires dans le cyberespace. Cinq ans plus tard, dans un document de portée supérieure intitulé stratégie nationale militaire des Etats-Unis d'Amérique de 2011, sont reconnus le caractère conflictuel du cyberespace et la nécessité pour les Etats-Unis de renforcer leur posture dissuasive dans l'espace aérien, spatial et cyber en possédant la capacité de combattre dans un environnement dégradé et d'améliorer leur capacité à attribuer et à mettre en échec les attaques sur les systèmes ou les infrastructures[87]. En 2013, l'état-major des armées, le Joint Staff, diffuse la doctrine interarmées des opérations cyber[88], la *Joint Publication 3-12 Cyber Operations* qui vise à intégrer davantage les cyberopérations dans les opérations militaires. Elle explicite clairement la chaîne de commandement des opérations cyber afin de permettre aux différents commandeurs des forces une meilleure intégration et synchronisation dans les opérations militaires. En termes d'opération cyber, les armées américaines les classent de la façon suivante :

- les *DoDIN (Deparment of Defense Information Networks Operations)*: ces opérations regroupent les actions de conception, configuration, supervision et sécurisation des systèmes d'information et de communications ;

- les *Defensive Cyber Operations (DCO) :* opérations destinées à défendre le cyberespace du *DoD*, elles répondent à toute activité non autorisée ou alerte/menace allant à l'encontre des *DoDIN ;*

[86] The Joint Chief of Staff, *The National Military Strategy for Cyberspace Operations*, Washington, 2006

[87] U.S. Department of Defense, *National Military Strategy of the United States of America 2011: Redefining America's Military Leadership*, Washington, 2011

[88] The Joint Chief of Staff, *Joint Publication 3-12 Cyber Operations*, Washington, 2013

- les *Offensive Cyber Operations (OCO) :* opérations visant à projeter de la puissance par et dans le cyberespace contre tout ennemi ou acteur hostile en ciblant leurs activités et leurs capacités, elles exigent les mêmes *Executive Order* que les opérations dans les domaines physiques.

Le même document indique qu'en dépit d'une centralisation due à l'interconnexion des systèmes, des délégations pour conduire des opérations cyber sont possibles pour les commandeurs. Il précise également que chaque opération aura une procédure spécifique incluant des actions pré approuvées afin de répondre à la vitesse du combat dans le cyberespace.

L'approche actuelle du département de la défense a été redéfinie dans la stratégie cyber de 2015[89], où sont préconisées cinq initiatives stratégiques :

- Former et entretenir des forces et des capacités pour conduire les opérations dans le cyberespace ;

- Défendre les réseaux du département de la Défense, sécuriser ses données et réduire les risques des missions du département ;

- Etre prêt à défendre le sol américain et les intérêts vitaux face à des attaques cyber d'une importance significative ;

- Etablir et entretenir des options cyber viable et planifier leur utilisation pour contrôler l'escalade des conflits et modeler l'environnement des conflits à tous niveaux ;

- Etablir et entretenir des alliances internationales robustes et des partenariats pour dissuader les menaces partagées et augmenter la sécurité et la stabilité internationales.

A travers l'étude des différents documents, il apparait que les Etats-Unis ont acquis une certaine maturité dans la prise en compte du cyberespace. Les forces armées américaines disposent d'un corpus doctrinaire élargi où la place du cyber est assez bien décrite.

Structure

Pour assurer l'application de cette doctrine militaire, les Etats-Unis se sont dotés en 2010 d'un état-major spécialisé, le *Cyber Command*, aussi dénommé *CYBERCOM*[90]. Cet état-major est subordonné au *Strategic Command (USSTRATCOM).* Le *CYBERCOM* est co-localisé avec l'état-major de l'agence de sécurité nationale (*National Security Agency*, *NSA)*,

[89] U.S. Department of Defense, Department of Defense Cyber Strategy, Washington, 2015

[90] U.S. Department of Defense, US Cyber Command Fact sheet, Washington, 2010

l'une des agences de la communauté du renseignement, portée historiquement sur le renseignement d'origine électromagnétique. Cette co-localisation n'est pas anodine puisque le commandeur du *CYBERCOM* est également le directeur de la *NSA.* La mission principale du CYBERCOM est le commandement et le contrôle des opérations dans l'espace cyber, ce qui inclut leur synchronisation, planification et exécution. Il assure la défense et la protection des réseaux du département de la défense, appuie les missions militaires et se prépare sur ordre à conduire des opérations militaires « large spectre » dans le cyberespace. Les cinq priorités de cet état-major sont de former une force cyber entraîné et prête, mettre en place les outils de supervision de la situation dans le cyberespace, de créer des capacités de commandement et des concepts opérationnels pour les opérations, établir un réseau interarmées défendable, et s'assurer que le commandeur dispose des politiques et de l'autorité adéquates pour lui permettre d'exécuter l'ensemble des opérations dans l'espace cyber[91]. Sous le commandement du *CYBERCOM*, chaque composante des armées américaines a créé son propre état-major cyber : l'*ARMY CYBER COMMAND*, l'*AIR FORCE CYBER COMMAND*, le *FLEET CYBER COMMAND* et le *MARINE CORPS FORCES CYBERSPACE COMMAND.* Ces commandements disposent d'unités cyber à l'échelon tactique. Ces unités destinées à mener des opérations dans le cyberespace sont de type différent[92] :

- *The Cyber National Mission Force :* élément national axé sur la lutte contre les menaces affectant le cyberespace national de niveau stratégique ;

- *The Cyber Combat Mission Force :* rattachées aux états-majors cyber de composante et chargées de conduire des opérations offensives une fois approuvées et autorisées par les autorités compétentes (Niveau secrétaire de la défense) ;

- *The Cyber Support Teams :* fournissent des développeurs, analystes, programmeurs, linguistes et ingénieurs en appui des opérations offensives ;

- *The Cyber Protection Teams :* mènent des opérations défensives, DoDIN en se coordonnant avec l'agence des systèmes d'information de la Défense *(Defense Information Systems Agency ,DISA).*

Enfin dans chaque grand commandement régional sont créés des *JCC (Joint Cyberspace Center)* pour permettre une intégration totale des cyberopérations dans les opérations militaires.

[91] Ibid
[92] U.S. Joint Staff Joint Force Development, *Cross-Domain Synergy in Joint Operations*, 2016, p54

S'il est difficile de se rendre compte des résultats obtenus par les armées américaines en termes d'opérations cyber, leur organisation démontre un investissement important et une prise en compte à tous les niveaux de la menace.

Relations avec les partenaires civils, étrangers

La politique en matière de cybersécurité et de cyberdéfense émane de la présidence des Etats-Unis. Pour ce faire, le président dispose depuis 2009 d'un conseiller spécial responsable de la coordination de la cybersécurité. Ce conseiller, le *« Cyber Security Coordinator »*, co-préside, avec le conseil de la sécurité intérieur (*Homeland Security Council*), le comité de la politique inter-agences des infrastructures d'information et de communication. Ce comité de coordination de haut-niveau fait partie du conseil de la sécurité nationale, instance où se décide la politique nationale et internationale du gouvernement fédéral. Il existe une répartition assez claire des rôles entre les différents départements, comprendre ministères, ainsi, c'est le département de la sécurité intérieure (*Department of Homeland Security, DHS)* qui est le premier responsable de la cybersécurité à l'intérieur des frontières nationales. Ce département a en charge notamment le renforcement de la sécurité et de la résilience des infrastructures critiques et l'appui aux agences civiles fédérales. Au cœur du *DHS*, le centre national d'intégration de la cybersécurité et des communications (*National Cybersecurity and Communications Integration Center, NCCIC)* est chargé d'effectuer l'estimation de la situation cyber sur le territoire américain et d'en assurer son partage avec les multiples agences et le secteur privé. Le département d'état (*Department of State, DoS)* est quant à lui responsable de la communication et la coordination de la politique présidentielle de cybersécurité au niveau international. Le département de la justice (*Department of Justice, DoJ)* fait appliquer les lois relatives à la cybersécurité et conduit les enquêtes et poursuit les infractions et crimes commis sous sa juridiction. Il dispose pour cela d'une section « crimes informatiques et propriété intellectuelle » (*Computer Crime and Intellectual Property Section*). Malgré l'absence de frontière dans le cyberespace, la distinction entre défense et sécurité nationale semble bien établie aux Etats-Unis, toutefois devant la nécessité de partager l'information entre tous les acteurs, une loi importante a été votée dans un passé récent : la loi sur la partage des informations de cybersécurité (*Cybersecurity Information Sharing act, 2015).*De plus, en février 2015, l'office du direction du renseignement national (*Office of the Director of National Intelligence*), qui regroupe et coordonne les 17 agences civiles et

militaires de la communauté du renseignement, a créé le centre d'intégration du renseignement de la menace cyber *(Cyber Threat Intelligence Integration Center, CTIIC).* Son but est d'être un centre de partage entre le *NCCIC*, le *CYBERCOM*, les différentes entités gouvernementales traitant du cyberespace et également le secteur privé américain.

Les liens entre la défense et les acteurs privés sont nombreux aux Etats-Unis, les armées américaines faisant recours à des sociétés privées pour les appuyer. Le cyber ne fait pas exception. La *NSA* compte environ 64000 sous-traitants et, autre type de relation avec le monde privé, elle fournit aux entreprises américaines des informations relevant de l'espionnage économique[93]. De surcroit, il revient au département de la défense de participer à la réponse en cas d'attaque sur un membre de la base industrielle de défense américaine.

L'organisation de la cybersécurité et de la cyberdéfense aux Etats-Unis est donc partagée en acteurs civils et militaires. Pour en assurer la coordination entre les agences, des nombreuses passerelles ont été créées. La distinction entre la chaîne civile et militaire semble toutefois bien établie, les armées se consacrant à la défense de leurs propres réseaux et aux opérations militaires dans le cyberespace.

Similitudes et différences majeures

Il n'est pas rare de lire que dans la montée en puissance de sa filière cyber, la France suit l'exemple américain, pourtant les deux modèles se différencient sur quelques points. Tout d'abord, en ce qui concerne les ressemblances, il semble que les armées françaises suivent la voie ouverte par leurs homologues américains en ayant dans un premier temps développé une approche prioritairement défensive. En 2010, à la création du *CYBERCOM*, les missions de ce commandement sont axées sur les opérations défensives visant à protéger les réseaux d'information du département de la Défense et à s'assurer la liberté d'action des Etats-Unis dans le cyberespace[94]. Trois ans plus tard, à l'occasion d'une audition devant le Sénat américain, le général Alexander témoigne de la nouvelle orientation de la stratégie américaine dans le cyberespace et indique que les Etats-Unis disposent également d'unités offensives

[93] KEMPF Hervé, *Les Etats-Unis et le cyberespace*, Conflits hors série n°4, automne 2016

[94] *U.S. Department of Defense*, U.S. Cyber Command fact sheet, Washington, le 25 mai 2010.

dans ce milieu[95]. Le cheminement suivi par la France, avec quelques années de décalage, poursuit sensiblement la même voie. En effet, la France partage avec les Etats-Unis la vision du caractère conflictuel du cyberespace et n'envisage par la défense des intérêts nationaux dans cet espace sans le développement de capacités offensives[96]. Une nouvelle étape attestant de cette démarche commune a été franchie lors de la création du commandement cyber français, début 2017. De même, l'un des principaux défis est partagé par les deux pays, il s'agit du recrutement, de la formation et de la fidélisation du personnel nécessaire, effort qui dépasse le seul monde de la défense et doit concerner l'ensemble des composantes des pays. Si l'approche du cyberespace française et américaine comporte de nombreux points de similitude, il apparait également des différences notables. C'est un truisme que d'écrire que les Etats-Unis disposent de davantage de moyens humains, financiers et matériels que la France. Cela est également vrai dans le cyberespace. Il a été vu lors des chapitres précédents les structures civiles et militaires des deux états, le nombre important d'acteurs côté américains ne peut que frapper. En plus des différentes structures, le personnel œuvrant à ces missions aux Etats-Unis atteint environ 6200 militaires[97], civils de la défense et de société privé alors qu'il atteindra 2600 personnes en France à l'horizon 2019[98]. Au-delà du seul aspect quantitatif, deux autres caractéristiques différencient modèle français et américains, il s'agit des liens entre la cyberdéfense et le renseignement et de la propriété dissuasive de la cyberdéfense. Aux Etats-Unis, renseignement et cyberdéfense sont intégrés, la *NSA* et le *CYBERCOM* répondent au même chef et le *Cyber Threat Intelligence Integration Center*, formation dépendant du directeur national du renseignement, assure le partage de l'information entre toutes les agences de renseignement civile et militaire et le *CYBERCOM*.

[95] « Auditionné par le Sénat américain, le général Keith B. Alexander, commandant du Cyber Command, décrit la mission des 13 unités cyber offensives chargées de la dissuasion face aux cyberattaques destructrices dont peuvent être victimes les Etats-Unis: "Laissez-moi être clair, ces unités de défense nationale ne sont pas des unités défensives, ce sont des unités offensives que le département de la défense peut utiliser pour défendre le pays si nous sommes attaqués dans le cyberespace". »
BAUD Michel, *Cyberguerre. En quête d'une stratégie*, Michel Baud, Focus stratégique n°44, mai 2013, p29

[96] La France développera sa posture sur la base d'une organisation de cyberdéfense étroitement intégrée aux forces, disposant de capacités défensives et offensives pour préparer ou accompagner les opérations militaires. *Livre blanc sur la défense et la sécurité nationale 2013*, p94

[97] U.S. department of defense, *The Department of Defense CyberStrategy fact sheet*, Washington, april 2015

LE DRIAN Jean-Yves, *Discours du ministre de la Défense le lundi 12 décembre 2016 prononcé à l'occasion de la visite de la Direction générale de l'armement-Maîtrise de l'information*, consultable sur le site 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

En France, une séparation nette demeure entre le renseignement et la cyberdéfense[99], le Centre de Recherche et d'Analyse du Cyberespace fait partie de la Direction du Renseignement Militaire et les autres services de renseignement français disposent de leurs propres spécialistes cyber utilisés pour la sécurité de leur service ou la recherche de renseignement. Enfin, si les Etats-Unis considèrent que se doter d'une cyberdéfense crédible permettra de dissuader certains adversaires de s'attaquer aux Etats-Unis à travers le cyberespace, le ministre de la défense français a clairement invalidé ce concept dans le cadre du cyberespace, comme vu supra.

La France et les Etats-Unis ont donc entrepris de militariser leur défense dans le cyberespace pour dans un premier temps, protéger leur propre appareil militaire, et par la suite, assurer la défense de leurs intérêts. Des spécificités subsistent de part et d'autre, s'expliquant par les moyens disponibles et les choix organisationnels préexistants (place du renseignement notamment).

[99] *Audition de l'amiral Arnaud Coustillière, directeur de projet chargé de la coordination générale des actions du ministère de la Défense dans le domaine de la cyberdéfense*, assemblée nationale, Paris, 28 juin 2016

Conclusion :

L'évolution de la posture des forces armées dans le cyberespace résulte de plusieurs tendances. La première est le besoin de protection des armées pour leurs propres systèmes d'information et de communication. Ce besoin n'est pas récent, il est inscrit dans la culture militaire du secret et se poursuit dans le temps. La seconde tendance est la multiplication des menaces et la prise de conscience des risques liés au numérique et à l'interconnexion généralisée des systèmes. Notre dépendance à la technologie constitue désormais une telle source de fragilité, qu'une atteinte majeure sur les systèmes informatiques pourrait bouleverser la vie de la Nation. Les stratèges et les politiques ayant reconnu l'aspect conflictuel du cyberespace, ils ont alors décidé d'en confier la défense à l'acteur militaire, œuvrant déjà dans les autres espaces terrestre, maritime, aérien et spatial. Nous assistons depuis les deux dernières décennies à la réorganisation des armées pour prendre en compte ce nouveau champ de bataille à l'instar de ce qu'a connu l'armée en France au début de l'aviation. Si jusqu'à présent, il n'existe pas encore d'armée du cyberespace disposant d'une pleine autonomie vis-à-vis des autres composantes, nous pouvons en observer les prémisses aux Etats-Unis et en France. Quel que soit la forme que prendra la cyberdéfense à terme, l'enjeu reste de taille puisqu'il s'agit encore et toujours d'assurer l'indépendance de la Nation.

Enfin, il s'agit pour la France et ses armées d'adopter leur propre voie en cyberdéfense en gardant à l'esprit l'avertissement du général Beaufre dans son Introduction à la stratégie : « cependant, cet intense mouvement d'idées pénètre à peine en Europe, où l'on se contente en général après quelques lectures distraites d'adopter le vocabulaire et le matériel américains parce que l'on croit encore sans le dire à la suprématie du matériel sur les idées »[100]. Or le cyberespace poursuit continuellement son élargissement et sa mutation avec l'arrivée de nouvelles technologies reliant davantage l'homme à cet espace, il importe donc d'en comprendre son fonctionnement et ses dynamiques par la pensée.

[100]BEAUFRE André, *Introduction à la stratégie*, Hachette, Paris,1998

Sources et bibliographie :

Sources françaises :

AGENCE NATIONALE DE LA SECURITE DES SYSTEMES D'INFORMATION, *Stratégie sur la défense et la sécurité des systèmes d'information*, février 2011

ARMEE DE TERRE, Centre de Doctrine d'Emploi des Forces, *Les forces terrestres et le cyberespace comme nouveau champ de bataille*, cahier du RETEX, mai 2014

ASSEMBLEE NATIONALE, *Rapport d'information sur le développement de l'économie numérique, Corinne Erhel et Laure de la Raudière*, mai 2014

ASSEMBLEE NATIONALE, *Audition de l'amiral Arnaud Coustillière, directeur de projet chargé de la coordination générale des actions du ministère de la Défense dans le domaine de la cyberdéfense, assemblée nationale*, Paris, juin 2016

Décret n°2009-834 du 7 juillet 2009 portant création d'un service à compétence nationale dénommé « Agence nationale de la sécurité des systèmes d'information »

HUBERT Vanille, *Cyberguerre et nucléaire, le ver informatique Stuxnet*, Centre de doctrine d'emploi des forces, lettre du retex-recherche n°27, janvier 2016

Livre blanc sur la sécurité et la défense nationale, la documentation française, avril 2013

LOI n° 2009-928 du 29 juillet 2009 relative à la programmation militaire pour les années 2009 à 2014 et portant diverses dispositions concernant la défense

LOI n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale

MINISTERE DE LA DEFENSE, *Discours du ministre de la Défense le lundi 12 décembre 2016 prononcé à l'occasion de la visite de la Direction générale de l'armement-Maîtrise de l'information, consultable sur le site http:/www.defense.gouv.fr/ministre/prises-de-parole-du-ministre*

MINISTERE DE LA DEFENSE, *Pacte cyberdéfense*, février 2014

SENAT, *Rapport d'information n°449, fait au nom de la commission des Affaires étrangères, de la défense et des forces armées sur la cyberdéfense*, Sénat, 2008

SENAT, *Rapport d'information n°681 fait au nom de la commission des affaires étrangères, de la défense et des forces armées sur la cyberdéfense par M. Jean-Marie Bockel*, juin 2012

Sources américaines :

Department of Defense, *Department of Defense Cyberstrategy*, Washington, avril 2015

Department of Defense, *Joint Operating Environment 2035. The Joint Force in a Contested and Disordered World*, juillet 2016

Department of Defense, *Strategy for operating in Cyberspace*, juillet 2011

Department of Defense, *US Cyber Command Fact sheet*, Washington, 2010

Joint Chief of Staff, *Joint Publication 3.12*, Washington, février 2013

Joint Chief of Staff, The Joint Operating Environment, juillet 2016

Joint Staff Joint Force Development, *Cross-Domain Synergy in Joint Operations*, 2016

Bibliographie :

ANAJ-IHEDN, *Prospectives des doctrines françaises en matière de cyberdéfense*, 2010

ARPAGIAN Nicolas, *La cybersécurité*, puf, août 2015

BAUD Michel, *Cyberguerre. En quête d'une stratégie*,Focus stratégique n°44, mai 2013

BONNEMAISON Aymeric, DOSSE Stéphane, *Attention : Cyber ! Vers le combat cyber-électronique*, Economica, décembre 2013

BOYER Bertrand, Cybertactique. Conduire la guerre numérique, nuvis, janvier 2014

GREENWALD G, MACASKIL E, *NSA Prism program taps in to user of Apple, Google and others*, The Guardian, 7 juin 2013

HUYGHE François-Bernard, KEMPF Olivier, MAZZUCHI Nicolas, *Gagner les cyberconflits*, economica, septembre 2015

KEMPF Hervé, *Les Etats-Unis et le cyberespace*, Conflits hors série n°4, automne 2016

KEMPF Olivier, *Introduction à la cyberstratégie,* Paris, Economica, novembre 2012

KEMPF Olivier, DOSSE Stéphane (dir), *Stratégies dans le cyberespace*, L'esprit du Livre, septembre 2011.

LIBICKI Martin, *Cyberdeterrence and cyberwar*, Rand Corporation, 2009

PARLEMENT EUROPEEN, *Rapport sur le droit d'accès à l'Internet*, mars 2015

POSEN Barry R, *La maîtrise des espaces, fondement de l'hégémonie des Etats-Unis*, Politique étrangère n°1-2003

RAUFER Xavier (dir.), *La première cyberguerre mondiale*, MA éditions, juin 2015

SCHREIR Fred, *The report on Cyberwarfare*, DCAF, 2012

VENTRE Daniel, *Cyberespace et acteurs du cyberconflit*, Lavoisier, 2011

VENTRE Daniel, *Cyber Operations in DOD Policy and Plans : Issues for Congress. Congressional Research Service report*, janvier 2015

WOLFF Philippe, VALLEE Luc, *Cyber-conflits, quelques clés de compréhension*, rapport de l'INHESJ